ID: 1385428
Sample Name:
3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe
Cookbook: default.jbs
Time: 09:36:08
Date: 02/02/2024
Version: 39.0.0 Ruby

Table of Contents

Table of Contents 2
Windows Analysis Report 3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 6
Dropped Files 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 6
System Summary 6
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
Compliance 7
Networking 7
System Summary 7
Data Obfuscation 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 12
World Map of Contacted IPs 14
Public IPs 14
General Information 14
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\Config.Msi\49a7b8.rbs 16
C:\Program Files (x86)\Remote Utilities - Host\EULA.rtf 16
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\MessageBox.exe 16
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\VPDAgent.exe 17
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\emf2pdf.dll 17
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\fwproc.exe 17
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\pdfout.dll 18
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\printer.ico 18
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\progressbar.exe 18
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\properties.exe 19
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\rupd.lng 19
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\srvinst.exe 19
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\vpd_sdk.dll 20
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\vpdisp.exe 20
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\msvcp120.dll 20
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\msvcr120.dll 21
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\ntprint.inf 21
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\printer.ico 21
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupd.gpd 22
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupd.ini 22
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupd.lng 22
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupdpm.dll 23
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupdui.dll 23
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\setupdrv.exe 23
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\stdnames_vpd.gpd 24
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unidrv_rupd.dll 24
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unidrv_rupd.hlp 24
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unidrvui_rupd.dll 25
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unires_vpd.dll 25
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\vccorlib120.dll 25
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\msvcp120.dll 26
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\msvcr120.dll 26
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\ntprint.inf 26
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\printer.ico 27
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\rupd.gpd 27
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\rupd.ini 27
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\rupd.lng 28
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\rupdpm.dll 28
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\rupdui.dll 28
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\setupdrv.exe 29
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\stdnames_vpd.gpd 29

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\unidrv_rupd.dll 29
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\unidrv_rupd.hlp 29
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\unidrvui_rupd.dll 30
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\unires_vpd.dll 30
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\vccorlib120.dll 30
C:\Program Files (x86)\Remote Utilities - Host\eventmsg.dll 31
C:\Program Files (x86)\Remote Utilities - Host\libeay32.dll 31
C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe 31
C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe 32
C:\Program Files (x86)\Remote Utilities - Host\ssleay32.dll 32
C:\Program Files (x86)\Remote Utilities - Host\vp8decoder.dll 32
C:\Program Files (x86)\Remote Utilities - Host\vp8encoder.dll 33
C:\Program Files (x86)\Remote Utilities - Host\webmmux.dll 33
C:\Program Files (x86)\Remote Utilities - Host\webmvorbisdecoder.dll 33
C:\Program Files (x86)\Remote Utilities - Host\webmvorbisencoder.dll 34
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html 34
C:\ProgramData\Remote Utilities\install.log 34
C:\ProgramData\Remote Utilities\msi\70220_{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\Exel.msi 35
C:\Users\user\AppData\Local\Temp\Exel.msi 35
C:\Windows\Installer\49a7b6.msi 35
C:\Windows\Installer\49a7b9.msi 36
C:\Windows\Installer\MSIAB6F.tmp 36
C:\Windows\Installer\MSIACD8.tmp 36
C:\Windows\Installer\SourceHash{3FF12DDA-38DA-466F-B4E3-6775ACEF5538} 37
C:\Windows\Installer\inprogressinstallinfo.ipi 37
C:\Windows\Installer\{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\ARPPRODUCTICON.exe 37
C:\Windows\Installer\{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\UNINST_Uninstall_R_3B1E3C8B7D0945898DA82CEEED02F0C7.exe 38
C:\Windows\Installer\{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\en_server_settings_E3BFC76BE38F4CF79D2ED7163B7DECEE.exe 38
C:\Windows\Installer\{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\en_server_start_85DB64512C79429FA70AC6C0611579DD.exe 38
C:\Windows\Installer\{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\en_server_stop_B603677802D142C98E7A415B72132E14.exe 38
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log 39
C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\26C212D9399727259664BDFCA073966E_C5856A5EB1E3B74AE8014850A678CDBF 39
C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\3EC49180A59F0C351C30F112AD97CFA5_ED80F76A55EEDF047A88FD3F37D62FA3 39
C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\26C212D9399727259664BDFCA073966E_C5856A5EB1E3B74AE8014850A678CDBF 40
C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3EC49180A59F0C351C30F112AD97CFA5_ED80F76A55EEDF047A88FD3F37D62FA3
C:\Windows\Temp\~DF10BD94535F44088B.TMP 4040
C:\Windows\Temp\~DF43AE85119F93081A.TMP 41
C:\Windows\Temp\~DF46A59DA49B45DF44.TMP 41
C:\Windows\Temp\~DF529C0FE4C5A9CE4B.TMP 41
C:\Windows\Temp\~DF70B43A60818B563C.TMP 41
C:\Windows\Temp\~DF8E23FC32B87CAA71.TMP 42
C:\Windows\Temp\~DF9FE2B93D9F6F7365.TMP 42
C:\Windows\Temp\~DFB588C3675999CB76.TMP 42
C:\Windows\Temp\~DFCE78CABB386C66F3.TMP 43
C:\Windows\Temp\~DFD5F4580B380072C8.TMP 43
C:\Windows\Temp\~DFDE25689DD43B2CB0.TMP 43
C:\Windows\Temp\~DFE4BF60F9C7AF91F3.TMP 44
Static File Info 44
General 44
File Icon 44
Static PE Info 44
General 44
Entrypoint Preview 45
Rich Headers 46
Data Directories 46
Sections 47
Resources 47
Imports 48
Network Behavior 48
Network Port Distribution 48
TCP Packets 48
UDP Packets 50
DNS Queries 50
DNS Answers 50
Statistics 51
Behavior 51
System Behavior 51
Analysis Process: 3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exePID: 7316, Parent PID: 2580 51
General 51
File Activities 52
Analysis Process: msiexec.exePID: 7416, Parent PID: 7316 52
General 52
File Activities 52
Analysis Process: msiexec.exePID: 7448, Parent PID: 620 52
General 52
File Activities 52
File Written 52
File Read 53
Registry Activities 53
Analysis Process: msiexec.exePID: 7528, Parent PID: 7448 53
General 53
Analysis Process: rfusclient.exePID: 7600, Parent PID: 7448 53
General 53
File Activities 54
File Created 54
File Written 54
File Read 55
Analysis Process: rutserv.exePID: 7640, Parent PID: 7448 55
General 55
File Activities 55
File Created 55
File Written 56
File Read 56
Registry Activities 56
Key Created 56
Analysis Process: rutserv.exePID: 7676, Parent PID: 7448 57
General 57
File Activities 57
File Created 57
File Read 57
Analysis Process: rutserv.exePID: 7772, Parent PID: 7448 57
General 57
File Activities 58
File Created 58
File Read 58

Analysis Process: rutserv.exePID: 7876, Parent PID: 620 58
General 58
File Activities 58
File Created 58
File Written 60
File Read 65
Registry Activities 65
Key Created 65
Key Value Created 65
Key Value Modified 75
Analysis Process: rutserv.exePID: 8008, Parent PID: 7876 94
General 94
Analysis Process: rfusclient.exePID: 8048, Parent PID: 7876 95
General 95
Analysis Process: rfusclient.exePID: 8068, Parent PID: 7876 95
General 95
Analysis Process: rfusclient.exePID: 5016, Parent PID: 8048 95
General 95
Disassembly 96

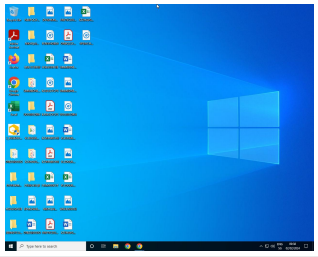
Windows Analysis Report

3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe

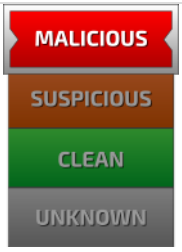
Overview

General Information

Sample name:	3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exerenamed because original name is a hash value
Original sample name:	3_.pdf.exe
Analysis ID:	1385428
MD5:	075d6c122274…
SHA1:	6f54d70f39fa28..
SHA256:	92192af947017..
Tags:	exe RemoteUtilities rurat
Infos:	YARA SIGMA



Detection



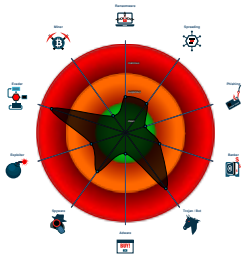
RMSRemoteAdmin, Remote Utilities

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Remote Utilities RAT
- Detected unpacking (overwrites its o…
- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double…
- Connects to many ports of the same…
- Initial sample is a PE file and has a…
- Query firmware table information (lik…
- Tries to detect sandboxes and other…
- Uses an obfuscated file name to hid…
- AV process strings found (often use…
- Checks for available system drives …

Classification



Process Tree

- **System is w10x64**
- 3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe (PID: 7316 cmdline: C:\Users\user\Desktop\3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe MD5: 075D6C122274CB9226521D3CD298F2F2)
  - msiexec.exe (PID: 7416 cmdline: "C:\Windows\System32\msiexec.exe" /i Exel.msi /qn MD5: E5DA170027542E25EDE42FC54C929077)
- msiexec.exe (PID: 7448 cmdline: C:\Windows\system32\msiexec.exe /V MD5: E5DA170027542E25EDE42FC54C929077)
  - msiexec.exe (PID: 7528 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 494BECA00E3009394CA5F2713F238EA9 MD5: 9D09DC1EDA745A5F87553048E57620CF)
  - rfusclient.exe (PID: 7600 cmdline: C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe" -msi_copy "C:\Users\user\AppData\Local\Temp\Exel.msi MD5: 6AAE165F3B1575DB887A0370CFC80083)
  - rutserv.exe (PID: 7640 cmdline: "C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" /silentinstall MD5: 652C2A693B333504A3879460D0AF7224)
  - rutserv.exe (PID: 7676 cmdline: "C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" /firewall MD5: 652C2A693B333504A3879460D0AF7224)
  - rutserv.exe (PID: 7772 cmdline: "C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" /start MD5: 652C2A693B333504A3879460D0AF7224)
- rutserv.exe (PID: 7876 cmdline: "C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" -service MD5: 652C2A693B333504A3879460D0AF7224)
  - rutserv.exe (PID: 8008 cmdline: "C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" -firewall MD5: 652C2A693B333504A3879460D0AF7224)
  - rfusclient.exe (PID: 8048 cmdline: C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe MD5: 6AAE165F3B1575DB887A0370CFC80083)
    - rfusclient.exe (PID: 5016 cmdline: "C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe" /tray MD5: 6AAE165F3B1575DB887A0370CFC80083)
  - rfusclient.exe (PID: 8068 cmdline: "C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe" /tray MD5: 6AAE165F3B1575DB887A0370CFC80083)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe	JoeSecurity_RMS RemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe	MALWARE_Win_ RemoteUtilitiesRA T	RemoteUtilitiesRA T RAT payload	ditekSHen	• 0x39d3a4:$s1: rman_message • 0x405be0:$s3: rms_host_ • 0x40657c:$s3: rms_host_ • 0x7a410c:$s4: rman_av_capture_settings • 0x3a76cc:$s7: _rms_log.txt • 0x45d27c:$s8: rms_internet_id_settings
C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe	JoeSecurity_RMS RemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe	MALWARE_Win_ RemoteUtilitiesRA T	RemoteUtilitiesRA T RAT payload	ditekSHen	• 0x3a02f0:$s1: rman_message • 0x431f3c:$s3: rms_host_ • 0x4328e0:$s3: rms_host_ • 0x7d1f30:$s4: rman_av_capture_settings • 0x83a260:$s5: rman_registry_key • 0x83a2ac:$s5: rman_registry_key • 0x4e5a1c:$s6: rms_system_information • 0x2e6274:$s7: _rms_log.txt • 0x4a5efc:$s8: rms_internet_id_settings

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.1747218595.0000000001803000.00000002.00000001.01000000.0000000A.sdmp	JoeSecurity_RMS RemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
00000009.00000003.1896822360.000000000890F000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RMS RemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
00000005.00000000.1747218595.0000000001739000.00000002.00000001.01000000.0000000A.sdmp	JoeSecurity_RMS RemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
00000004.00000000.1716230830.0000000001091000.00000002.00000001.01000000.00000009.sdmp	JoeSecurity_RMS RemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
Process Memory Space: rfusclient.exe PID: 7600	JoeSecurity_RMS RemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.rfusclient.exe.650000.0.unpack	JoeSecurity_RMS RemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
4.0.rfusclient.exe.650000.0.unpack	MALWARE_Win_ RemoteUtilitiesRA T	RemoteUtilitiesRA T RAT payload	ditekSHen	• 0x39d3a4:$s1: rman_message • 0x405be0:$s3: rms_host_ • 0x40657c:$s3: rms_host_ • 0x7a410c:$s4: rman_av_capture_settings • 0x3a76cc:$s7: _rms_log.txt • 0x45d27c:$s8: rms_internet_id_settings

Sigma Signatures

System Summary

Sigma detected: Suspicious Double Extension File Execution

Sigma detected: Suspicious Outbound SMTP Connections

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Connects to many ports of the same IP (likely port scanning)

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Hooking and other Techniques for Hiding and Protection

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Remote Access Functionality

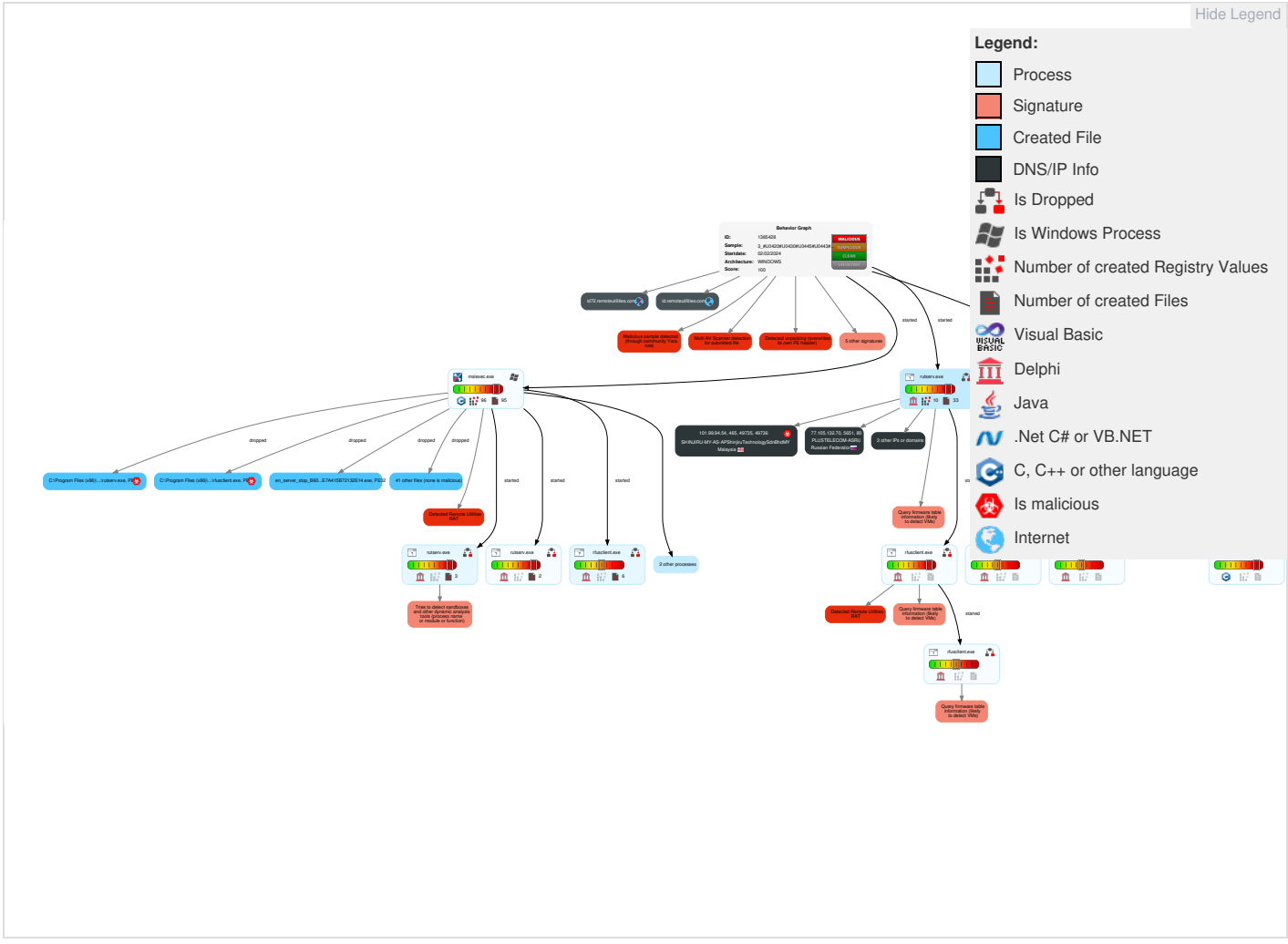
Detected Remote Utilities RAT

Mitre Att&ck Matrix

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	1 Replication Through Removable Media	1 Native API	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	OS Credential Dumping	2 System Time Discovery	Remote Services	1 1 Archive Collected Data	2 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	2 Service Execution	3 Windows Service	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 1 Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	3 Windows Service	1 4 Obfuscated Files or Information	Security Account Manager	4 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Remote Access Software	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	1 2 Process Injection	1 2 Software Packing	NTDS	5 6 System Information Discovery	Distributed Component Object Model	Input Capture	1 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 5 1 Security Software Discovery	SSH	Keylogging	1 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 File Deletion	Cached Domain Credentials	1 1 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 2 1 Masquerading	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	1 Modify Registry	Proc Filesystem	1 Application Window Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	1 1 1 Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	Network Sniffing	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	1 2 Process Injection	Network Sniffing	Network Service Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement

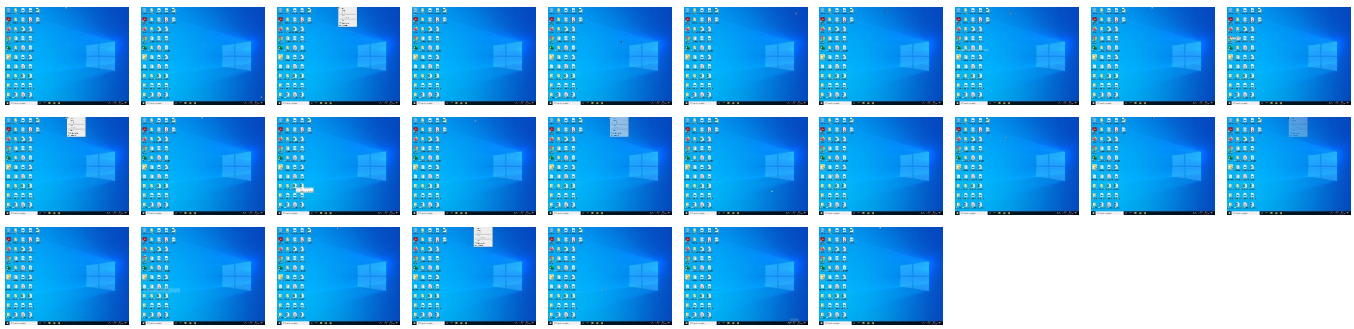
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe	28%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\MessageBox.exe	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\MessageBox.exe	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\VPDAgent.exe	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\VPDAgent.exe	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\emf2pdf.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\emf2pdf.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\fwproc.exe	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\fwproc.exe	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\pdfout.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\pdfout.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\progressbar.exe	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\progressbar.exe	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\properties.exe	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\properties.exe	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\srvinst.exe	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\srvinst.exe	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\vpd_sdk.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\vpd_sdk.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\vpdisp.exe	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\common\vpdisp.exe	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\msvcp120.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\msvcp120.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\msvcr120.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\msvcr120.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupdpm.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupdpm.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupdui.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupdui.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\setupdrv.exe	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\setupdrv.exe	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unidrv_rupd.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unidrv_rupd.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unidrvui_rupd.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unidrvui_rupd.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unires_vpd.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unires_vpd.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\vccorlib120.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\vccorlib120.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\msvcp120.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\msvcp120.dll	0%	Virustotal		Browse
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\msvcr120.dll	0%	ReversingLabs		
C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\msvcr120.dll	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
fp2e7a.wpc.phicdn.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.indyproject.org/	0%	URL Reputation	safe	
http://www.indyproject.org/	0%	URL Reputation	safe	
http://www.flexerasoftware.com0	0%	URL Reputation	safe	
http://update.remoteutilities.net/upgrade_beta.ini	0%	Avira URL Cloud	safe	
http://update.remoteutilities.net/upgrade.ini	0%	Virustotal		Browse
http://update.remoteutilities.net/upgrade.ini	0%	Avira URL Cloud	safe	
http://madExcept.comU	0%	Avira URL Cloud	safe	
http://update.remoteutilities.net/upgrade_beta.ini	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
id.remoteutilities.com	64.20.61.146	true	false		high
fp2e7a.wpc.phicdn.net	192.229.211.108	true	false	• 0%, Virustotal, Browse	unknown
id72.remoteutilities.com	unknown	unknown	false		high

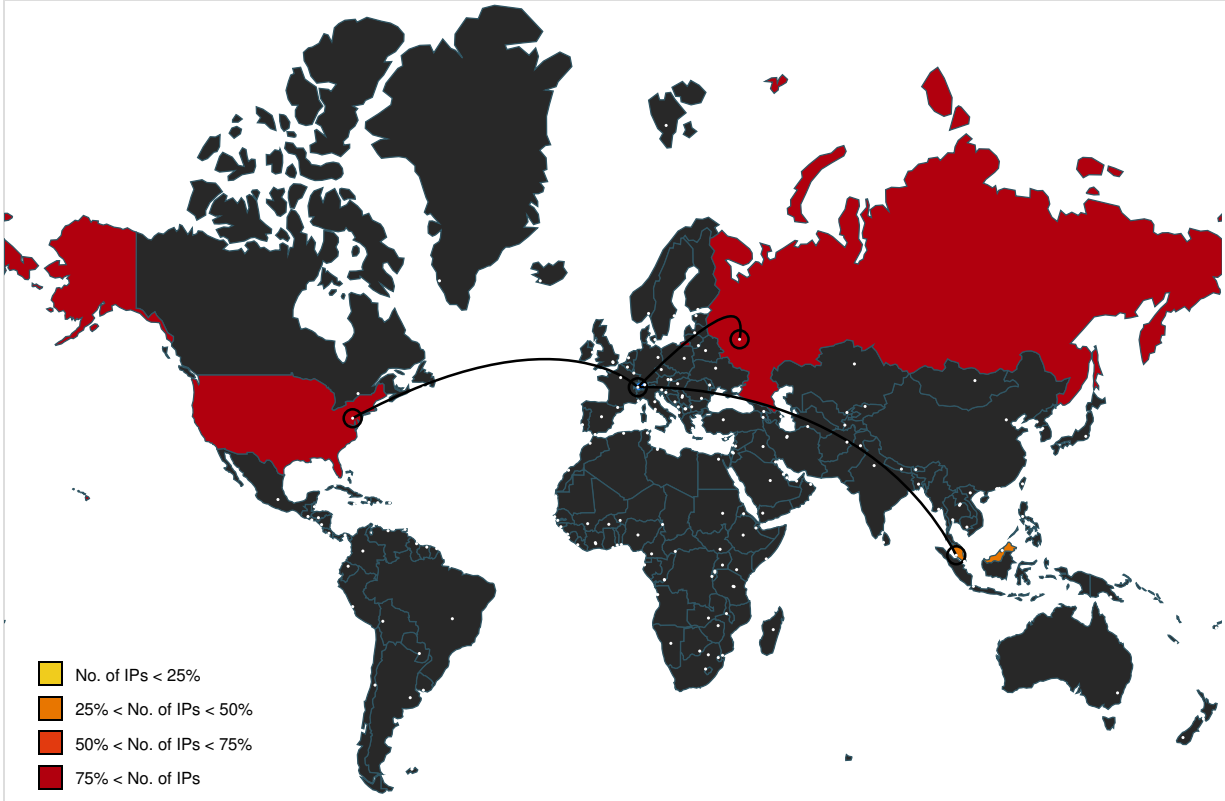
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.openssl.org/support/faq.html.....rbwb.rndC:HOMERANDFILEPRNG	rutserv.exe, 00000005.00000002.177682461 0.00000000110EA000.00000002.00000001.010 00000.0000000B.sdmp	false		high
http://https://www.remoteutilities.com/support/docs/e	rutserv.exe, 00000009.00000002.297787330 6.0000000005720000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/support/docs/	rutserv.exe, 00000009.00000002.290959424 2.000000000269A000.00000004.00001000.000 20000.00000000.sdmp, rutserv.exe, 000000 09.00000002.2977873306.0000000005720000. 00000004.00001000.00020000.00000000.sdmp, rutserv.exe, 00000009.00000002.2971300777.000000 0004F70000.00000004.00001000.00020000.00 000000.sdmp	false		high
http://https://www.remoteutilities.com/tell-me-more.phpities.com/tell-me-more.phpet	rutserv.exe, 00000009.00000002.290959424 2.00000000026C8000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://www.openssl.org/V	rutserv.exe, 00000005.00000002.177793797 7.0000000012053000.00000002.00000001.010 00000.0000000C.sdmp, rutserv.exe, 000000 05.00000002.1777313937.000000001114B000. 00000002.00000001.01000000.0000000B.sdmp	false		high
http://https://www.remoteutilities.com/support/docs/s0	rutserv.exe, 00000009.00000002.297787330 6.0000000005720000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://madExcept.comU	rfusclient.exe, 00000004.00000000.171476 9466.0000000000651000.00000020.00000001. 01000000.00000009.sdmp, rutserv.exe, 000 00005.00000000.1736259820.00000000003410 00.00000020.00000001.01000000.0000000A.sdmp, rutserv.exe, 00000009.00000003.1849563793.000 000007B8C0000.00000004.00001000.00020000 .00000000.sdmp, rutserv.exe, 00000009.00 000003.1859762685.000000007CCF0000.00000 004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.remoteutilities.com/support/docs/o0	rutserv.exe, 00000009.00000002.297787330 6.0000000005720000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/support/docs/rt/docs/r	rutserv.exe, 00000009.00000002.297787330 6.0000000005720000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	rfusclient.exe, 00000004.00000000.171476 9466.0000000000651000.00000020.00000001. 01000000.00000009.sdmp, rutserv.exe, 000 00005.00000000.1736259820.00000000003410 00.00000020.00000001.01000000.0000000A.sdmp, rutserv.exe, 00000009.00000003.1849563793.000 000007B8C0000.00000004.00001000.00020000 .00000000.sdmp, rutserv.exe, 00000009.00 000003.1859762685.000000007CCF0000.00000 004.00001000.00020000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/tell-me-more.phpet	rutserv.exe, 00000009.00000002.290959424 2.00000000026C8000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://www.indyproject.org/	rfusclient.exe, 00000004.00000003.172844 6387.00000000033EC000.00000004.00001000. 00020000.00000000.sdmp, rfusclient.exe, 00000004.0 0000000.1714769466.0000000000E4E000.0000 0020.00000001.01000000.00000009.sdmp, ru tserv.exe, 00000005.00000000.1736259820. 000000000122A000.00000020.00000001.01000 000.0000000A.sdmp, rutserv.exe, 00000009 .00000002.2909594242.0000000002675000.00 000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.remoteutilities.com/support/docs/0	rutserv.exe, 00000009.00000002.297787330 6.0000000005720000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/tell-me-more.phpB	rutserv.exe, 00000009.00000002.297787330 6.0000000005720000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://www.symauth.com/cps0(	3_#U0420#U0430#U0445#U0443#U043d#U043e#U 043a.pdf.exe, 00000000.00000003.16577194 55.000001A6A21A0000.00000004.00000020.00 020000.00000000.sdmp, 3_#U0420#U0430#U04 45#U0443#U043d#U043e#U043a.pdf.exe, 0000 0000.00000003.1657719455.000001A6A216200 0.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://rmansys.ru/internet-id/	rutserv.exe, 00000005.00000000.174721859 5.0000000001803000.00000002.00000001.010 00000.0000000A.sdmp, rutserv.exe, 000000 05.00000000.1747218595.0000000001739000. 00000002.00000001.01000000.0000000A.sdmp	false		high
http://https://www.remoteutilities.com/tell-me-more.php...	rutserv.exe, 00000009.00000002.290959424 2.00000000026C8000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://www.openssl.org/support/faq.html	rutserv.exe, 00000005.00000002.177682461 0.00000000110EA000.00000002.00000001.010 00000.0000000B.sdmp	false		high
http://https://www.remoteutilities.com/index.php?src=app?src=app	rutserv.exe, 00000009.00000002.297787330 6.0000000005720000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/index.php?src=appx.php?src=app0	rutserv.exe, 00000009.00000002.297130077 7.0000000004F70000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://update.remoteutilities.net/upgrade.ini	rutserv.exe, 00000005.00000000.173625982 0.0000000000341000.00000020.00000001.010 00000.0000000A.sdmp, rutserv.exe, 000000 09.00000003.1869888513.000000007E7E0000. 00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.remoteutilities.com/tell-me-more.php1	rutserv.exe, 00000009.00000002.290959424 2.00000000026C8000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/tell-me-more.php.	rutserv.exe, 00000009.00000002.290959424 2.00000000026C8000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd	rfusclient.exe, 00000004.00000000.171623 0830.0000000001091000.00000002.00000001. 01000000.00000009.sdmp, rutserv.exe, 000 00005.00000000.1747218595.0000000018030 00.00000002.00000001.01000000.0000000A.sdmp, rutserv.exe, 00000009.00000003.1896822360.000 000000890F000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://www.symauth.com/rpa00	3_#U0420#U0430#U0445#U0443#U043d#U043e#U 043a.pdf.exe, 00000000.00000003.16577194 55.000001A6A21A0000.00000004.00000020.00 020000.00000000.sdmp, 3_#U0420#U0430#U04 45#U0443#U043d#U043e#U043a.pdf.exe, 0000 0000.00000003.1657719455.000001A6A216200 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/index.php?src=app	rutserv.exe, 00000009.00000002.297130077 7.0000000004F70000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/support/docs/t0	rutserv.exe, 00000009.00000002.297787330 6.0000000005720000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/tell-me-more.phpes.	rutserv.exe, 00000009.00000002.290959424 2.00000000026C8000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/support/docs/connecting-over-the-internet/	rutserv.exe, 00000009.00000002.297130077 7.000000000503E000.00000004.00001000.000 20000.00000000.sdmp, rutserv.exe, 000000 09.00000002.2971300777.0000000004F70000. 00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/support/docs/rt/docs/	rutserv.exe, 00000009.00000002.290959424 2.000000000269A000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/tell-me-more.php	rutserv.exe, 00000009.00000002.290959424 2.00000000026C8000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://update.remoteutilities.net/upgrade_beta.ini	rutserv.exe, 00000005.00000000.173625982 0.0000000000341000.00000020.00000001.010 00000.0000000A.sdmp, rutserv.exe, 000000 09.00000003.1869888513.000000007E7E0000. 00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.remoteutilities.com/tell-me-more.phpdo?	rutserv.exe, 00000009.00000002.290959424 2.00000000026C8000.00000004.00001000.000 20000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/tell-me-more.phpken	rutserv.exe, 00000009.00000002.290959424 2.00000000026C8000.00000004.00001000.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.flexerasoftware.com0	3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe, 00000000.00000003.1657719455.000001A6A21A0000.00000004.00000020.00020000.00000000.sdmp, 3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe, 00000000.00000003.1657719455.000001A6A2162000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.inkscape.org/namespaces/inkscape	rfusclient.exe, 00000004.00000000.171623083 0.0000000001091000.00000002.00000001.01000000.00000009.sdmp, rutserv.exe, 00000005.00000000.1747218595.0000000001803000.00000002.00000001.01000000.0000000A.sdmp, rutserv.exe, 00000009.00000003.1896822360.000000000890F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/support/docs/a0	rutserv.exe, 00000009.00000002.2977873306.0000000005720000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/support/docs	rutserv.exe, 00000009.00000002.2909594242.000000000269A000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.remoteutilities.com/tell-me-more.phpities.com/tell-me-more.phpum	rutserv.exe, 00000009.00000002.2909594242.00000000026C8000.00000004.00001000.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.105.132.70	unknown	Russian Federation		42031	PLUSTELECOM-ASRU	false
64.20.61.146	id.remoteutilities.com	United States		19318	IS-AS-1US	false
185.70.104.90	unknown	Russian Federation		49335	NCONNECT-ASRU	false
66.23.226.254	unknown	United States		19318	IS-AS-1US	false
101.99.94.54	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	true

General Information

Joe Sandbox version:	39.0.0 Ruby
Analysis ID:	1385428
Start date and time:	2024-02-02 09:36:08 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 9m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exerenamed because original name is a hash value
Original Sample Name:	3_.pdf.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@23/88@2/5
EGA Information:	• Successful, ratio: 83.3%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 192.229.211.108
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ocsp.edge.digicert.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtCreateKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:37:16	API Interceptor	466522x Sleep call for process: rutserv.exe modified
09:37:24	API Interceptor	105497x Sleep call for process: rfusclient.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Config.Msi\49a7b8.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	32359
Entropy (8bit):	5.221077217292647
Encrypted:	false
SSDEEP:	768:fltototxA6rSrBjp1kyUXGiM01HuEClQcQpeQn6mPaUaqBt6M+pG57:YGsBjpKyUXGeHuEClQcQkQ6mPaUaqBtD
MD5:	68206233254021EE853F27ADA734D571
SHA1:	E39BBFE2F243F5DA81FF44D7F3F7F4304635A8D6
SHA-256:	70B973BF6109792A708B02D6EE011540F39C6EE73B4C7E2FBA20B23E9D4D8E7D
SHA-512:	4E6FAD6664F3D6FC8DF295BE51C5D07286EBF591AA849E57C39D781879F7D4C4EC111FB727DA2BABCD2D21B2E9E6ED286D2D08D1C350263E37E6BF0434468 9F
Malicious:	false
Preview:	...@IXOS.@.....@.LBX.@.....@.....@.....@.....@.....@.....&.{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}..Remote Utilities - Host..Exel.msi.@.....@.....@.....@.....A RPPRODUCTICON.exe..&.{BFB6CB81-8A2D-41FC-A737-5CF8EB370093}.....@.....@.....@.....@.....@.....@.....@.....@.....Remote Utilities - Host.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{26EAB54E-4659-47E8-86F9-4CB74 F7E03BE}&.{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}.@.....&.{596F4636-5D51-49F5-B3B4-F3C366E9DC23}&.{3FF12DDA-38DA-466F-B4E3-6775ACE F5538}.@.....&.{596F4636-5D51-49F5-B3B4-F3C366E9DC23}&.{00000000-0000-0000-0000-000000000000}.@.....&.{3244CDE6-6414-4399-B0D5-424562747210}&. {3FF12DDA-38DA-466F-B4E3-6775ACEF5538}.@.....&.{197F692B-7CCA-4D79-85A5-ED04202D08D0}&.{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}.@.....&. {E79AC184-AD38-4B26-89D0-75B7CEA19FA2}&.{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}.@.....&.{BDFF180E-29DE-4951-A6

C:\Program Files (x86)\Remote Utilities - Host\EULA.rtf

Process:	C:\Windows\System32\msiexec.exe
File Type:	Rich Text Format data, version 1, ANSI, code page 1252
Category:	dropped
Size (bytes):	15975
Entropy (8bit):	4.971311456641861
Encrypted:	false
SSDEEP:	384:Akc9TI9T+FCnjK71n5yqmOxSCH/Cu37gFpBukSVb5R:AkcuoCnjK7Rh5Cu3U/W
MD5:	9B0E600EB09E7A86199F7BA245D1CD2B
SHA1:	E3E52B3E04B08E59AAE74300F7D30C3D0AA27148
SHA-256:	879180116B82210292648709982F405EAE84B05E6F2FF324A6A5CC7CD512D3E7
SHA-512:	DD1622474C48ECF5C95E7585FB30B5279CF45DFC893325311758838B05F73499F536F7CADAF529AA4FA5AE0808E30A455465829DB7D13F2EE2E7D9B7BD12E17E
Malicious:	false
Preview:	{\rtf1\ansi\ansicpg1252\cocoartf2638.\cocoatextscaling0\cocoaplatform0{\fonttbl\f0\fswiss\fcharset0 ArialMT;\f1\ftech\fcharset77 Symbol;}.{\colortbl;\red255\green255\blue 255;\red51\green51\blue51;}.{*\expandedcolortbl;;\csgenericrgb\c20000\c20000\c20000;}.{*\listtable{\list\listtemplateid1\listhybrid{\listlevel\levelnfc23\levelnfcn23\le veljc0\leveljcn0\levelfollow0\levelstartat1\levelspace360\levelindent0{*\levelmarker \{disc\}}{\leveltext\leveltemplateid1\'01\uc0\u8226 ;}{\levelnumbers;}\fi-360\li720\lin720 } {\listname ;}\listid1}.{\list\listtemplateid2\listhybrid{\listlevel\levelnfc23\levelnfcn23\leveljc0\leveljcn0\levelfollow0\levelstartat1\levelspace360\levelindent0{*\levelmarker \{d isc\}}{\leveltext\leveltemplateid101\'01\uc0\u8226 ;}{\levelnumbers;}\fi-360\li720\lin720 }{\listname ;}\listid2}}.{*\listoverridetable{\listoverride\listid1\listoverridecount0\ls1} {\listoverride\listid2\listoverridecount0\ls2}}.{\info.{\author Marat}}\margl1440\margr1440\vieww12540\viewh15120\view

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\MessageBox.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	16352
Entropy (8bit):	6.54052527746532
Encrypted:	false
SSDEEP:	192:IxgSABvdm4Yy3EA39QKH5EDZSZuc2+huLdALWwsUJZscF8Bd1LPK6CYHB5K:Ix0FmW3EaHiDZSZwJdLSZsHLPK6jHG
MD5:	73E40D762BA0B67027B8A489E5161821
SHA1:	F4D9B83EC23C6226C20C39F1B996894992707124
SHA-256:	37E3F9B5D5B95A47EB44E72E1E587C553BCAB7981DFF5D108FDE86B702E1A858
SHA-512:	8F9FC3533433AF5B44B1E19B377D184FCA51A95B6289B9D80628998802FB1ACEC488F22FFC563E1CC413DFD8FFEF2E097E882C29029BC29CFA11F9434A8DF00
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3.j.]Oj.]Oj.]Og..Oh.]Og..Oh.]Og..Oy.]Og..Oh.]Oc..Oc.]Oj.\OY.]O..Ok.]Og..Ok.]O..Ok.]ORichj.]O.....PE..L.....S..... ....@.....`.....k....@.....".x....@.....!...P..|....!..8. .....!..@..... .....text...2..... ..`.rdata..... .....@..@.data.....0.....@....rsrc.....@..... @..@.reloc..|....P.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\VPDAgent.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2674656
Entropy (8bit):	6.865564996943119
Encrypted:	false
SSDEEP:	49152:dE8JxHX5r9sDQl7wDSMSFxvQ/qpyr0k0ha5XLDaDMPNw2x8pWTUKA76AeFG:dE8XHX5riUl7wDP6vQ/qpyr0kR5XLWD/
MD5:	D47B1FBDAE6406EC50110A3C59F685F4
SHA1:	B242609CB05CA8F5BFD08306274D10AC6E22E20C
SHA-256:	B03A3AD0C77DD9FD4DE0CB1FF938074ACCFBB8AC413524B1158DFA5014A26CE2
SHA-512:	E2601392D9615138B32F33295CBACF1C54A7DDD04FF4BE70800190CC55F1FD6EE8A8400913E103FC74C0C57D18B1A94B81E9E5EC9AE9182BA03D413B87DD7E E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....zz..zz..zz.M...zz.+...zz.+...zz.+...zz.+...zz.f...zz..zz..zz.f..Oxz ..z{..{z.....zz.f...zz..(...zz..z...zz.f...zz.Rich.zz.....PE..L..../.\.....5u.....@.....)....9)...@.....<.&.....'.H.....(..!...'..n. .....0:&.@.....text...5..... ..`.rdata.....@..@.data...<.....&..d....&.....@....rsrc...H.....'.....8'..... .....@..@.reloc...n....'..p...>'.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\emf2pdf.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1111520
Entropy (8bit):	6.491611255996076
Encrypted:	false
SSDEEP:	24576:UqSQS800orApz53PI2GVqH7kpf/V57GGcP6T5m+moXafzz:SQSX0oAtkpf/bfcyTTmoozz
MD5:	829AB21444204D50C64B805FE7897433
SHA1:	8540A93A2376B4B3EA447830775FFA69AB089A63
SHA-256:	2FE3D65C4CB5CB2DBB73AA0C05392230F7B52A7482C80A531B2E4C7DC42C16D9
SHA-512:	E5FF3639B275B6849FF0E974E4A921ED9461B4257684F088E651D32080C07F09394B19FB75E5EAA69C250CFAA682F6E3740CD0BA65F16B0FFBD81F01183FF2A8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....[.:..:..:....l.:....n.7:....o.:..d..:..d...:..d..:..u.V.:..?d...:..?d..:..?d..:.. :..T:..?d..:..?d..:...:db.:..?d..:...Rich.:.....PE..L.....\.....!.....@.....|....&..d.....!.....l.....p .....@.....text..... .@..@.rsrc.....d.....@..@.reloc...l.....n...f.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\fwproc.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	23520
Entropy (8bit):	6.440740836511924
Encrypted:	false
SSDEEP:	384:Bb57Gk7g+iy218DTK9jkrtpgjKMp+fZSZwJdLSZsHLPK6jHvCg:h/218DTVrtsKMsBpPKgP1
MD5:	99B4B661886B0E7B480FEA0847ABD1B0
SHA1:	397EBD9B25DB33B20E5FECA257BDFA69424D8693
SHA-256:	0168F614579F7EFDE386DF3C6F63A3804DBB5EC37ED954859B4CEE3D82065617
SHA-512:	9F150CDA46349401984BA11F3E88FD379A36006CC403AD78DF02A6BFE4D9EC49043A343A49B7349C19D2391ED84D9B27E6BCF374322E76F4EA6E237852A9715
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9Gf.}&.I}&.I}&.I;w.I|&.I;w.In&.I;w.Iy&.I;w.Iy&.It^.Ix&.I}&.I?&.I..I|&.Ip t.I|&.I}&.I|&.I..I|&.IRich}&.I.....PE..L..../.\.....8.....e".....0....@.....@.....49..d....`..@.....:...!...p.....@1..8..... .....5..@.....0.....text...k..... ..`.rdata..:....0.....@..@.data.....@.....@....rsrc...@....`.....0.....@..@.reloc .....p.....6.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\pdfout.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4006368
Entropy (8bit):	6.80959441986422
Encrypted:	false
SSDEEP:	98304:ZbR+lDT6t58JcKdTG57M06POn9rvBAUZLM8FA8:5R+lDOt5kgFvVwmr
MD5:	545F1581B2486E834B8FA676A5F7A8EA
SHA1:	2AB6F0B7D1FC4CE98CAE89B0DC04D7972CC67D77
SHA-256:	21E0FEBE30F53D63985ACA992A1BCF2B6853B6B23808BD910C4EE54979B271EE
SHA-512:	1DF88C03CB89845C484767897FA6CAD1C6412B10C67363E597BFC80BD0798F99D2C47A84FAF6A07B721D81CA0F3D0D5A7F3F7BDD2B179819A468F9DDA07F586
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....3.....3.....3.....fP8.....,.....,..... .,...Z...,.....).....Rich.....PE..L.....\.....!....b"..0.....".....=.....>...@.....pA:.....p:.d....;.....=..!...;.$....6.p..... .....6.....p.6.@.....".d.....text...9a".....b"..... ..`.rdata..(....."....f".....@..@.data.....:.j...f:.....@....gfids.....;.....:.....@..@.tls. .....;.....:.....@....rsrc.....;.....:.....@..@.reloc..$....;.. ....:.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\printer.ico

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows icon resource - 6 icons, 32x32, 4 bits/pixel, 16x16, 4 bits/pixel
Category:	dropped
Size (bytes):	10134
Entropy (8bit):	5.364629779133003
Encrypted:	false
SSDEEP:	96:75LkqDCmLVf89uqywWrvNCB4isySOc3AOv2B+YT1/44tuU+3:1OmLVf4dErvNCB5tSOc3AY2BP944g
MD5:	6F70BD62A17EC5B677EC1129F594EE6F
SHA1:	4FB95EB83A99C0DA62919C34886B0A3667F3911E
SHA-256:	FC8570D50C1773A1B34AA4E31143FD0776E26FF032EE3EEB6DB8BFAB42B4A846
SHA-512:	615A7E8738B2CF1BC47C8D5FC1357C1299080D0BAA1E54129D0DEBDB6BA60CD366364BE0BDAFDABCBA60F16544B0516A50B4B0182E8BCF01F59171003CE9B244
Malicious:	false
Preview:	....f.....(...N... .....v.....h..... .... .h....#..(... ...@..... x.....wx.....ww.....ww.x.....ww.xx.....ww.wxx.....w.wwxx.....wwwxx.....xwwwxx.....xwwwx.....xwww..x.....xww.wx.x.....xw.wwwx.x.... ...x.w|.x.x.x.....z.x.ww..x.....x.x.ww....x.....x..w....x.x.....x.....p.x.....x.....x.....p.....p..... .....?.....?.....(..... ..... .x.....w.....w.x.....wx.....wwx.....w

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\progressbar.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	40416

Entropy (8bit):	6.363657503806742
Encrypted:	false
SSDEEP:	384:ZkzqOI138e1y6JMKxTrAogoAoaP7+qFXYiLxjdQMUQ9LSk3E0gTSsn2TkhI3K0Tz:ZLqokSaddQMUNk3EXSsn2Tk4j3pPKgz
MD5:	65BE96DA02367532D8ED15F1300850CF
SHA1:	A8105BB2B6759450726539831AB646209C3EA51C
SHA-256:	5ABD11523B355CEF76D32DF24D9E82ED148B1A6DC3CA7C2FD7197FFED45D74E3
SHA-512:	F336974A176120AD7453144548CD01CFFF71F91CCE6E146F99F1ACFA488A57CBBDC436DACA54F1FD04254E48BD86C54C90D990A33761BF1C4874621C31C513E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b..b..b..3...b..3+..b..3*..b..3...b.Z....b...X..b..b..b.Z....b..0.. .b..b\..b.Z....b.Rich.b.....PE..L..../.\.....D...8.....I.....`....@.....~....@.....s.....|...!.....b..8..... .j..@.....`.....text....C.....D..... ..`.rdata.....`.. ...H.....@..@.data.....h.....@....rsrc.....I.....@..@.reloc.....t .....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\properties.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	180192
Entropy (8bit):	5.245276621355164
Encrypted:	false
SSDEEP:	1536:zvQtL1VQPsuMC7Wsb5o5/mXOMzZ52NyoGCIfb0wk7UAjKQpmArUaDZqxw+:E/i97Wao5eDaNvGCIj0w+mArBZk
MD5:	1589EAD8B5B00AE5E574FA6F005256C4
SHA1:	894D1EB249155F9383870F754B745321EA924473
SHA-256:	6D4939FD651AF68DB82784425A2B6805F1169376B5CA9C5821E5C8CFB81C549C
SHA-512:	86252A061E102E87933CEFA53F31F1AD459A91AB555D1847F10583D9096542E2912AA7230E90DCFB3ED8EA5E8F2D232AC81C203E943DBF2E690AC8D500EB24A F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.....X.1....X.....X.3....X.....m.....}....D3.....D.....5.....y ....D0....Rich.....PE..L..../.\.....\.....8.....p....@.....0.....@.....,5.....`..V.....!.....z..8..... .....@.....0..,.....text....[.....\..... ..`.rdata..(E...p...F...`.....@..@.data....l.....@....idata...$...0...&.....@..@.rsrc...V....`..... .....@..@.reloc.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\rupd.lng

Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	98650
Entropy (8bit):	4.192473934109759
Encrypted:	false
SSDEEP:	768:5rENOwVRq6rZmor3CmRxhESLGZ0s1JP2PY6rZlshvwmE2uJJ6rZqDJK1YRo6rZGx:S9miFao0WDn
MD5:	1614E6CDF119FD284D476F7E6723B3AD
SHA1:	3FF9164C9E5FC47169CC1C6EECA22AAB099F2EA3
SHA-256:	C8DF350F95FFEEED30060092DC8666EADCE040A4DDCB98E7A9293F87D19387A8
SHA-512:	8FBCB156B2F9637BC15FA71758A361CB2500F5A19875EE6BE2B52FC3171C38353A6CDC623E36777D052E0B319C7AF934D2D1DBE92E69666C9B9AD749610BA47 1
Malicious:	false
Preview:	..[.E.n.g.l.i.s.h.].....L.a.n.g.I.D.=.1.0.3.3.....;. .l.o.o.k. .f.o.r. .l.a.n.g.u.a.g.e. .i.d.e.n.t.i.f.i.e.r.s. .i.n. .M.S.D.N. .-. .'.T.a.b.l.e. .o.f. .L.a.n.g.u.a.g.e. .I.d.e.n.t.i.f.i.e.r.s.'. .t.o.p.i.c... .....;. .S.T.A.N.D.A.R.D. .D.I.A.L.O.G. .B.U.T.T.O.N.S.:.....1.=.O.K.....2.=.C.a.n.c.e.l.....;. .P.R.I.N.T.I.N.G. .P.R.E.F.E.R.E.N.C.E.S.:.....;. .C.o.m.m.o.n. .s.t.r.i.n.g.s... ..;. .b.i.t.s. .p.e.r. .p.i.x.e.l.....5.0.0.0. .=. .1. .b.i.t. .-. .b.l.a.c.k. .a.n.d. .w.h.i.t.e.....5.0.0.1. .=. .4. .b.i.t.s. .-. .1.6. .c.o.l.o.r.s.....5.0.0.2. .=. .8. .b.i.t.s. .-. .2.5.6. .c.o.l.o.r.s... ..5.0.0.3. .=. .2.4. .b.i.t.s. .-. .t.r.u.e. .c.o.l.o.r.....;. .C.o.m.p.r.e.s.s.i.o.n.....5.0.0.4. .=. .N.o.n.e.....5.0.0.5. .=. .A.u.t.o.m.a.t.i.c.....5.0.0.6. .=. .C.C.I.T.T. .m.o.d.i.f.i.e.d. . H.u.f.f.m.a.n. .R.L.E.....5.0.0.7. .=. .C.C.I.T.T. .G.r.o.u.p. .3. .f.a.x. .e.n.c.o.d.i.n.g.....5.0.0.8. .=. .C.C.I.T.T. .G.r.o.u.p. .4. .f.a.x. .e.n.c.o.d.i.n.g.....5.0.0.9. .=. .L.e.m.p.e.

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\srvinst.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	53728
Entropy (8bit):	6.5571910635788635

Encrypted:	false
SSDEEP:	768:jqfYiEXOtlk4SgVg1pQtfVuTsxxSzELKoZeepPKg3:ZiEXYq2g1pC9uToxkiZ/x1
MD5:	A810FC0F499E254375FB1FA9116E2CCF
SHA1:	CBD73834170A05A8D47846B255E02A2C7778C06A
SHA-256:	966EF76FE3476D530B1B97A6F40947ED14ADA378F13E44ECFE774EDC998CD0B0
SHA-512:	59D0855636E25C0F41A5401184C7CA16082A25FF72CAAD2D2C183E3977FBF60AE50C2E6A9F686681F1F19067225BB68C6FB3AEA808E7E5982C49B08E2095A669
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...3..3..3..uO..1..uO.. ..uO,.7..uO..6..3..S..:fb.4.....1..>L*.2..3.f.2 .../.2..Rich3.....PE..L.../.\.....v...:.....Ez.....@.....@.....x.....@.....!.....8..... ...@.....|.....text....u.....v..... ..`.rdata...!.....".z.....@..@.data.....@....rsrc...@.....@..@.reloc..... .....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\vpd_sdk.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2772960
Entropy (8bit):	6.917269583439067
Encrypted:	false
SSDEEP:	49152:QuZqJvz7GHYFVw8vfMVDpaLGtH3uSvQ/qpyr0kiU6HoCPLG5gzyUxChReb0:QuZqJvz7GHGVfvfMVDNNxvQ/qpyr0kpn
MD5:	E608CE332F016026E3D3B62E606192CA
SHA1:	0A5FB826AC299D4D086AF8BF1391184A15976571
SHA-256:	57AB69CBCB0DA76BD70D897514AEAE6858F52BD391B955D5C3A980A19F1DDE58
SHA-512:	53E4E647D43910D15158EF61445A77F80D72F7A63001C220D8A53853DCF04918B8495323051803 47A230D70E61992C034C48CEE2DAB8247BEE113FEB5AF1ACAF
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.&.1fH.1fH.1fH....8fH.w7..<fH.w7..<fH.w7..5fH.w7..6fH.8..$fH. 1fI.^gH.1fH.&fH.....dH.....fH.....,fH.....0fH.<4..0fH.....0fH.Rich1fH.....PE..L...,.[.....!.....j.....#..... .....*.....*...@.....p.'.:..T.(. .....).....*..!....).8|..0. .8.....8'.@..... .h.....text..... ..`.rdata...-.... ....@..@.data.....@(..~...0(.....@....rsr c.....).....(.....@..@.reloc..8|....)..~....(.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\common\vpdisp.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2992096
Entropy (8bit):	6.789893578257523
Encrypted:	false
SSDEEP:	49152:kN1BAW/tsUJX4JIHl3LhI2NnmTYH2RXoSrB/KYtvQ/qpyr0kyaTGjEawEP1vsB9u:kN1BaFY3FI29mTYH2JRwovQ/qpyr0ksD
MD5:	45D5F1B29B1B40B232D662DACF07D0DC
SHA1:	822E821E261B385FA7300530AA633A2E0C7D7914
SHA-256:	F224CDCDE4A049C4F471CC2C50E75FB55E4C0A540FEA4AD24A4C57E97DE48780
SHA-512:	1ADBB3D83107DCDE018EC41902FEF7C5E3AF3D6A7BC11AA6C71D23FB23F02ED36E9D6317631523D7B837FD19D934C0DCE73345B5DF0E82C2BE4B0A831C6A8 282
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....8.....!..L.!This program cannot be run in DOS mode....$.....j...j...j..V.u..j...;m..j...;R..j...;o..j...;S..j....!..j..}.o..j...j...j..}.R.3h..}.S. .j..._4...j...j..Ah..}.W..j..}.n..j...8i..j...j%..j..}.I..j..Rich.j.....PE..L.../.\.....!.....!.....".."...@.....-.....@.....+.+.....+.....,@..... .....-..!.....C.....x+.@.....".....text...g.!.....!..... ..`.rdata..T.....".....".....@..@.data....~.....,..N....+.....@....rsrc...@.. ...,.....<,.....@..@.reloc...C.....,..D...B,.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\msvcp120.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	660128
Entropy (8bit):	6.339798513733826

Encrypted:	false
SSDEEP:	12288:N2fus43uu43Ry4GHlT4xH2K+M+/i+WSpY+7YOzCaK9A3gS2EKZm+GWodEEwnyh:muJzCaK9AB2EKZm+GWodEEwnyh
MD5:	46060C35F697281BC5E7337AEE3722B1
SHA1:	D0164C041707F297A73ABB9EA854111953E99CF1
SHA-256:	2ABF0AAB5A3C5AE9424B64E9D19D9D6D4AEBC67814D7E92E4927B9798FEF2848
SHA-512:	2CF2ED4D45C79A6E6CEBFA3D332710A97F5CF0251DC194EEC8C54EA0CB85762FD19822610021CCD6A6904E80AFAE1590A83AF1FA45152F28CA56D862A3473FA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;..h..h..h..[h..h..h..h..Mh..hIAWh..h..Oh..h..qh..h..ph..h..uh..h..Lh ..h..Kh..h..Nh..hRich..h.....PE..d.....OR.....".....@.....`.....a....`.....pU.. ....2..<....@.....G.....>...P.....X.... .....p.....P.....text....>.....@..... ..`.rdata.....P.....D.....@..@.data.....P...8...B.....@....pdata...G.....H...z..... @..@.rsrc.....@.....@..@.reloc.....P.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\msvcr120.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	963232
Entropy (8bit):	6.634408584960502
Encrypted:	false
SSDEEP:	24576:FkZ+EUPoH5KTcAxt/qvRQdxQxO61kCS9mmWymzVPD:FkMAlM8ixQI5C6wl
MD5:	9C861C079DD81762B6C54E37597B7712
SHA1:	62CB65A1D79E2C5ADA0C7BFC04C18693567C90D0
SHA-256:	AD32240BB1DE55C3F5FCAC8789F583A17057F9D14914C538C2A7A5AD346B341C
SHA-512:	3AA770D6FBA8590FDCF5D263CB2B3D2FAE859E29D31AD482FBFBD700BCD602A013AC2568475999EF9FB06AE666D203D97F42181EC7344CBA023A8534FB13AC B7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Ck..".."..".."..D..."..".."...s..$ ...s.."...s.."...s.. "...s.."...s.."...s.."..Ric h."..... .....PE..d.....OR.....".....h..:.....)..... .....]....`.....@...(.....@...s...t...>.....8...p..... .....2..p.....text....g.....h..... ..`.rdata...8.....:...l.....@..@.data...hu.....D.....@....pdata...s...@...t.....@..@.rsrc..... ....^.....@..@.reloc..8.....b.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\ntprint.inf

Process:	C:\Windows\System32\msiexec.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	9698
Entropy (8bit):	3.8395767056459316
Encrypted:	false
SSDEEP:	192:jxUPudWfG9sPEd5yVplXhzPGeQ6cGIDGzBs+2o5WcicJXoNaTXy:jyxFeGIDIFXoNT
MD5:	6476F7217D9D6372361B9E49D701FB99
SHA1:	E1155AB2ACC8A9C9B3C83D1E98F816B84B5E7E25
SHA-256:	6135D3C9956A00C22615E53D66085DABBE2FBB93DF7B0CDF5C4F7F7B3829F58B
SHA-512:	B27ABD8ED640A72424B662AE5C529CDDA845497DC8BD6B67B0B44AE9CDD5E849F627E1735108B2DF09DD6EF83AD1DE6FAA1AD7A6727B5D7A7985F92A92CA0 779
Malicious:	false
Preview:	.....;. .N.T.P.R.I.N.T...I.N.F. .(.f.o.r. .W.i.n.d.o.w.s. .S.e.r.v.e.r. .2.0.0.3. .f.a.m.i.l.y.).....;.....;. .L.i.s.t. .o.f. .s.u.p.p.o.r.t.e.d. .p.r.i.n.t.e.r.s.,. .m.a.n.u.f.a.c.t.u.r.e.r.s.....;... .....[.V.e.r.s.i.o.n.].....S.i.g.n.a.t.u.r.e.=.".$.W.i.n.d.o.w.s. .N.T.$."....P.r.o.v.i.d.e.r.=.".M.i.c.r.o.s.o.f.t."....C.l.a.s.s.G.U.I.D.={.4.D.3.6.E.9.7.9.-.E.3.2.5.-.1.1.C.E.-.B.F.C.1.- .0.8.0.0.2.B.E.1.0.3.1.8.}.....C.l.a.s.s.=.P.r.i.n.t.e.r.....C.a.t.a.l.o.g.F.i.l.e.=.n.t.p.r.i.n.t...c.a.t.....D.r.i.v.e.r.I.s.o.l.a.t.i.o.n.=.2.....D.r.i.v.e.r.V.e.r.=.0.6./.2.1./.2.0.0.6.,.6...1. ..7.6.0.0...1.6.3.8.5.....[.M.a.n.u.f.a.c.t.u.r.e.r.].....".M.i.c.r.o.s.o.f.t.".=.M.i.c.r.o.s.o.f.t.,.N.T.a.m.d.6.4.....[.M.i.c.r.o.s.o.f.t...N.T.a.m.d.6.4.].....".{.D.2.0.E.A.3.7.2.-.D.D.3.5.- .4.9.5.0.-.9.E.D.8.-.A.6.3.3.5.A.F.E.7.9.F.0.}.". .=. .{.D.2.0.E.A.3.7.2.-.D.D.3.5.-.4.9.5.0.-.9.E.D.8.-.A.6.3.3.5.A.F.E.7.9.F.0.}.,. .{.D.2.0.E.A.3.7.2.-.D.D.3.5.-.4.9.5.0.-.9.E.D.8.- .A.6.3.3.5.A.F.

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\printer.ico

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows icon resource - 6 icons, 32x32, 4 bits/pixel, 16x16, 4 bits/pixel
Category:	dropped
Size (bytes):	10134

Entropy (8bit):	5.364629779133003
Encrypted:	false
SSDEEP:	96:75LkqDCmLVf89uqywWrvNCB4isySOc3AOv2B+YT1/44tuU+3:1OmLVf4dErvNCB5tSOc3AY2BP944g
MD5:	6F70BD62A17EC5B677EC1129F594EE6F
SHA1:	4FB95EB83A99C0DA62919C34886B0A3667F3911E
SHA-256:	FC8570D50C1773A1B34AA4E31143FD0776E26FF032EE3EEB6DB8BFAB42B4A846
SHA-512:	615A7E8738B2CF1BC47C8D5FC1357C1299080D0BAA1E54129D0DEBDB6BA60CD366364BE0BDAFDABCBA60F16544B0516A50B4B0182E8BCF01F59171003CE9B244
Malicious:	false
Preview:	....f.....(...N... .....v.....h..... .... .h....#..(... ...@.....x.....wx.....ww.....ww.x.....ww.xx.....ww.wxx.....w.wwxx.....wwwxx.....xwwwxx.....xwwwx.....xwww..x.....xww.wx.x.....xw.wwwx.x....x.w|.x.x.x.....z.x.ww..x.....x.x.ww....x.....x..w....x.x.....x.....p.x.....x.....x.....p.....p.....?.....?.....(..... ..... .x.....w.....w.x.....wx.....wwx.....w

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupd.gpd

Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	17415
Entropy (8bit):	4.618177193109944
Encrypted:	false
SSDEEP:	384:U1EQCr2g2t2g2F2s2J2m2p2z2ZOgoNJUTlZah25Dy:3oLILwfcV86ZO3eTlZzy
MD5:	8EE7FD65170ED9BD408E0C821171B62A
SHA1:	9D14A87A049C3B576CEC4B28210F0C95B94E08E0
SHA-256:	EE1E4D9869188CC3FA518C445ECF071845E5BD8BE56767A9F7F7DD3ACE294BA5
SHA-512:	5740AB3545D2217BA2156C58BA9AF6681D73116AB5DFBEAA5AB615D9CD0C77716C25865E67188E9D7892B340776755D4CBB1A3E98FAEAF8B6BB4B2CCA00D8AE6
Malicious:	false
Preview:	*GPDSpecVersion: "1.0"..*GPDFileVersion: "1.0"..*GPDFileName: "***.GPD"..*Include: "STDNAMES_VPD.GPD"..*ModelName: "*****"..*MasterUnits: PAIR(40800, 117600)..*ResourceDLL: "UNIRES_VPD.DLL"..*PrinterType: PAGE..*MaxCopies: 99....*Feature: Orientation..{.. *rcNameID: =ORIENTATION_DISPLAY.. *DefaultOption: PORTRAIT.. *Option: PORTRAIT.. {.. *rcNameID: =PORTRAIT_DISPLAY.. *Command: CmdSelect.. {.. *Order: DOC_SETUP.6.. *Cmd: "".. }.. }.. *Option: LANDSCAPE_CC270.. {.. *rcNameID: =LANDSCAPE_DISPLAY.. *Command: CmdSelect.. {.. *Order: DOC_SETUP.6.. *Cmd: "".. }.. }..}..*Feature: InputBin..{.. *rcNameID: =PAPER_SOURCE_DISPLAY.. *DefaultOption: AUTO...*Option: AUTO.. {.. *rcNameID: =AUTO_DISPLAY.. *Command: CmdSelect.. {.. *Order: DOC_SETUP.9.. *Cmd: "".. }.. }.. *Option: CASSETTE.. {.. *rcNameID:

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupd.ini

Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.479503224130279
Encrypted:	false
SSDEEP:	3:z8ANyq3jlZc:z8cy2wc
MD5:	610DFCD7FF61B76DAAC9DDC3CDAA64A9
SHA1:	343A63A7E2B0617F30B94E15E236DF7892FE722D
SHA-256:	7BA0ACE1E899C38CB5E8BF303868C0AB4B9890D536009CF21C958B114888DFA3
SHA-512:	D8095398ACC9DE610E42EAB655145BBACB09AE2D460906F9B490E48947EA802795C00CBFA3C674CDCC344D8A64FD63961D2D4A8999E0F0BADAFD3E367FE8B495
Malicious:	false
Preview:	[OEMFiles] ..OEMConfigFile1=rupdui.dll ..

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupd.lng

Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	98650
Entropy (8bit):	4.192473934109759
Encrypted:	false
SSDEEP:	768:5rENOwVRq6rZmor3CmRxhESLGZ0s1JP2PY6rZIshvwmE2uJJ6rZqDJK1YRo6rZGx:S9miFao0WDn
MD5:	1614E6CDF119FD284D476F7E6723B3AD
SHA1:	3FF9164C9E5FC47169CC1C6EECA22AAB099F2EA3

SHA-256:	C8DF350F95FFEEED30060092DC8666EADCE040A4DDCB98E7A9293F87D19387A8
SHA-512:	8FBCB156B2F9637BC15FA71758A361CB2500F5A19875EE6BE2B52FC3171C38353A6CDC623E36777D052E0B319C7AF934D2D1DBE92E69666C9B9AD749610BA47 1
Malicious:	false
Preview:	..[.E.n.g.l.i.s.h.].....L.a.n.g.I.D.=.1.0.3.3.....;. .l.o.o.k. .f.o.r. .l.a.n.g.u.a.g.e. .i.d.e.n.t.i.f.i.e.r.s. .i.n. .M.S.D.N. .-. .'.T.a.b.l.e. .o.f. .L.a.n.g.u.a.g.e. .I.d.e.n.t.i.f.i.e.r.s.'. .t.o.p.i.c... .....;. .S.T.A.N.D.A.R.D. .D.I.A.L.O.G. .B.U.T.T.O.N.S.:.....1.=.O.K.....2.=.C.a.n.c.e.l.....;. .P.R.I.N.T.I.N.G. .P.R.E.F.E.R.E.N.C.E.S.:.....;. .C.o.m.m.o.n. .s.t.r.i.n.g.s... ..;. .b.i.t.s. .p.e.r. .p.i.x.e.l.....5.0.0.0. .=. .1. .b.i.t. .-. .b.l.a.c.k. .a.n.d. .w.h.i.t.e.....5.0.0.1. .=. .4. .b.i.t.s. .-. .1.6. .c.o.l.o.r.s.....5.0.0.2. .=. .8. .b.i.t.s. .-. .2.5.6. .c.o.l.o.r.s... ..5.0.0.3. .=. .2.4. .b.i.t.s. .-. .t.r.u.e. .c.o.l.o.r.....;. .C.o.m.p.r.e.s.s.i.o.n.....5.0.0.4. .=. .N.o.n.e.....5.0.0.5. .=. .A.u.t.o.m.a.t.i.c.....5.0.0.6. .=. .C.C.I.T.T. .m.o.d.i.f.i.e.d. . H.u.f.f.m.a.n. .R.L.E.....5.0.0.7. .=. .C.C.I.T.T. .G.r.o.u.p. .3. .f.a.x. .e.n.c.o.d.i.n.g.....5.0.0.8. .=. .C.C.I.T.T. .G.r.o.u.p. .4. .f.a.x. .e.n.c.o.d.i.n.g.....5.0.0.9. .=. .L.e.m.p.e.

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupdpm.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36320
Entropy (8bit):	6.363095921735073
Encrypted:	false
SSDEEP:	768:/ek2AuDHuROuyVrGWngM328PAh8bWgs5fLutlfpPKgPH:foebh8bRs5zutJx5
MD5:	DA9CC6631ECEDCF3819332552F1EB449
SHA1:	161B227A23E87E4D7A7F59CF12AB87CB8D5D41A9
SHA-256:	363C85F73AD85F041BBAFB141B8EF1B7BD7A1268DA6B39F96D81582303C9ABE3
SHA-512:	29262D594D4112577F60CAB26698731381FB19BC0AF28BAAF1A2F07951617FE71F8BC7AF30E330F7A936BC3531CF9BCC58B00C0AA86B8C28AB558DA845E62EE 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p.....i'.....i1.....i6.....z....i!.....i .....i;.....i&..... i#.....Rich.....PE..d...O0.\....." .....V.....P.....@.....d..W....[.....`....I...!..... ..... .....text...GU.....V..... ..`.data...4....p.....Z.....@....pdata..`.....b.....@..@.rsrc.....f.....@..@.reloc.....j..... ...@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\rupdui.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	204768
Entropy (8bit):	5.825387232540853
Encrypted:	false
SSDEEP:	3072:pZN5YrUYklih2FJ5tmN8DNWcpQOw9Tsk1n1WOA6uBgmW:pZNhfxh2FTpWO2T/1WOA6uc
MD5:	75C636087E541A9524752F1DF66AAB99
SHA1:	C33E55AF6F92D48BE994F1999193CCD9F1C586BE
SHA-256:	EA37728ABE1401F32F01C113701EAA447380B65E58934AB0360113CA86CA1FF6
SHA-512:	9A871DF80660DA09F7297D69ECAADAC13F03DDCD298F5300E83C194A394EEC990743FCE5B6B3554BC0123CE96D1F3D5F124344B7E5247D282D540D853BC11C D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....dD....\....c....^....b.....R.....5Zf...5Zb...5Z_....X.....5Z].. .Rich.....PE..d...80.\....." .....~.....`.....@H..I....H.....(.....<.....!..... ..p.....text...=..... ..`.rdata.....@..@.data...ph...`.....@.....@....pdata..<.....X.....@..@.rsrc...(.....n.. .....@..@.reloc.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\setupdrv.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	102880
Entropy (8bit):	6.071756563190581
Encrypted:	false
SSDEEP:	1536:PFqz35CEMCZFwsbn60NhoBGO9otLJx39aHXI0OYWusz+xn:9wJ3MGimnrhoAOkNa3I0OYWtzu
MD5:	D0F22AFD5EAD9FFF432BE5746F2F989A
SHA1:	D83187AAAFD3BE638457E79961E54F22AFAD81F3

SHA-256:	C57FC5CFD1FA1241849AB423B49CE04D2EC361D2972204A2A9D7039D7100A8D7
SHA-512:	F2B0B06FB47775DFA448034953B4E5B97770F384978112FBAA7F1F1EF2EB37875634F963DB2E9515B4678DF63E314FBCE26D1A6A958C3DBC5C57E1CD32593D3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C..".."..".+.I.."...st.."...sK.."...sv.."...sJ.."...Z8.."..."...."....N.."...pp .."..."<.."....u.."..Rich."..PE..d...H0.\....."....@.....`.....[.....|.....p...!.....8..... .....8..p.....P.....text...=..... ..`.rdata..&g.....h.....@..@.data.....p.....V.....@....pdata.....X.....@..@.rsrc..... .....d.....@..@.reloc.....n.....@..B.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\stdnames_vpd.gpd

Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	14366
Entropy (8bit):	4.1817849062232195
Encrypted:	false
SSDEEP:	192:NjThm8JC986ITRCzEzEpYNwtd29u7ZTl8hF:yFzOnS7z0
MD5:	7162D8977515A446D2C1E139DA59DED5
SHA1:	952F696C463B8410B1FA93A3B2B6DAE416A81867
SHA-256:	2835A439C6AE22074BC3372491CB71E6C2B72D0C87AE3EEE6065C6CAADF1E5C8
SHA-512:	508F7CA3D4BC298534AB058F182755851051684F8D53306011F03875804C95E427428BD425DD13633EEC79748BB64E78AAD43E75B70CC5A3F0F4E6696DBB6D8E
Malicious:	false
Preview:	*%%% Copyright (c) 1997-1999 Microsoft Corporation..*%%% value macros for standard feature names and standard option names..*%%% used in older Unidrv 's.....*CodePage: 1252 *% Windows 3.1 US (ANSI) code page....*Feature: RESDLL..{.. *Name: "resource dll files".. *ConcealFromUI?: TRUE.... *Option: UniresDLL.. {.. *Name: "unires_vpd.dll".. }..}....*Macros: StdFeatureNames..{.. ORIENTATION_DISPLAY: RESDLL.UniresDLL.11100.. PAPER_SIZE_DISPLAY: RESDLL.UniresDLL.11101.. PAPER_SOURCE_DISPLAY: RESDLL.UniresDLL.11102.. RESOLUTION_DISPLAY: RESDLL.UniresDLL.11103.. MEDIA_TYPE_DISPLAY: RESDLL.UniresDLL.11104.. TEXT_QUALITY_DISPLAY: RESDLL.UniresDLL.11105.. COLOR_PRINTING_MODE_DISPLAY: RESDLL.UniresDLL.11106.. PRINTER_MEMORY_DISPLAY: RESDLL.UniresDLL.11107.. TWO_SIDED_PRINTING_DISPLAY: RESDLL.UniresDLL.11108.. PAGE_PROTECTION_

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unidrv_rupd.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	487904
Entropy (8bit):	6.3408335931113395
Encrypted:	false
SSDEEP:	6144:EgjhSyqP1a/eVqxFxNCAiG3XyJ/2TxbfsEkhy+0F+K8lJrZdwwSvm:EglSTPaRxFdLXyJ/ebEEkx0rqJduw
MD5:	CF36C1CFF0210B423921398E8AEF1C59
SHA1:	85F694BAC2B4E2D724542AB518C7BF6C5361AD3E
SHA-256:	45230CA1752B1FD2901708A45E7CC6F1370F65C495D30B08D9F1CE4C8BEAF6FA
SHA-512:	925067AD750F6A01FA0C31DBD876088BB65C36AB8C0889A3A52F0D452154D2BE8284E1077BA1553E06DEAE2181F437E077F13D5FAFD8AD5A3F6C9FC417CB774F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&.....7.....W.... .....0.....!.....:...d.....'....".....Rich..... .....PE..d...w.[J....." .....8.....d.....t.....@.....4.....x....p.....@...(...P...!.....!..8.....0... .....text...O..... ..`.rdata.....0.....@..@.data...x.... .....@....pdata...(...@...*.....@..@.rsrc.....p.....B..... ...@..@.reloc.....F.....@..B..[J@...+.[JK.....[JU.....[Jb...+.[JK.....[Jo.....[Jy.....msvcrt.dll.NTDLL.DLL.WINSPOOL.DRV.KERNEL32.dll.ole32.dll.GDI32.dll... .....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unidrv_rupd.hlp

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows 3.1 help, Tue Apr 17 13:11:56 2001, 21225 bytes
Category:	dropped
Size (bytes):	21225
Entropy (8bit):	3.9923245636306675
Encrypted:	false
SSDEEP:	192:g8qo9MqLEGX9WkaNWvbAsmrEGckkwy95/HLQdu:g8rMqLwkW8AsqEHkkwy7N
MD5:	6798F64959C913673BD66CD4E47F4A65
SHA1:	C50FAA64C8267AC7106401E69DA5C15FC3F2034C

SHA-256:	0C02B226BE4E7397F8C98799E58B0A512515E462CCDAAC04EDC10E3E1091C011
SHA-512:	8D208306B6D0F892A2F16F8070A89D8EDB968589896CB70CF46F43BF4BEFB7C4CA6A278C35FE8A2685CC784505EFB77C32B0AABF80D13BCC0D10A39AE8AFB5 5A
Malicious:	false
Preview:	?_.....R..r...i.....(),.aabo.utadvanc.edAllows.andareas.assigned.availabl.ebebookl.etc-.hang.e..racter@Clickc. o.de..sColo.rc.0..scon.taindefa.ultdepth.directlyi.0o r..sh..PD.isplaysd.ocument.P.sdraftse.n, ex..nal.featuref.ilesfl.....PrFor..m..-.to-trayf.romgraph$ic.@sh@.to.neH.@dhig.herlfima.gesininE..atio..sta.ll.@..itLe.t..Listsl. o..*.nualm.em..meta..2mS.tM!...enhoto..Oy.w.o.per\.ngop.timizh ...@.nsor..p.....spa3.Pri.ntp.0..ed.0..0er.@-spe.cific.@s1 .m.q..ityQ.0.relaB.RET.k.ghseese.l..edsets.oft Somes0ourc}.P ed.S.@sb.'.poo...gsuchsu.pporttak.est..tha...eT..'.oTo...TrueType...l.usevie@wWhenw. e.1.rw..hwil.lyouyour.;bynewof.fs/...&....;)....z4.....N .....|CF0.lR..|CF1..R..|CF2..R..|CF4..R..|CF5..R..|CONTEXT..)..|CTXOMAP.. ..|FONT.. ..|Petra..2..|PhrImage.....|PhrIndex.....|SYSTEM.2...|TOPIC.....|TTLBTREE..!..|Topic Id.=J.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unidrvui_rupd.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	892896
Entropy (8bit):	6.044545103599267
Encrypted:	false
SSDEEP:	12288:hpvsrQZu8F/bY6Pgx2B8UNG2Ql20gcwtH2qMP23so7:JZ5F/bYogxJUB9cwtHFMD0
MD5:	D77628FCE2A09AD76889E3300150F99C
SHA1:	2280483371D679437901EDBCDEC0D11F057AF5E8
SHA-256:	9E1BE3FFE0AB8B8D3B6AA964AA9F752E850304A212BCE124C50AB08F1259CC0B
SHA-512:	BB8A28BB61321E5B414E1BC2C9267D38E2676AC1BE8DF27A9A747CB7F7CFE97C1DBFF6C723DC958BE594BE38312172DAF7243B47C25AF2C1D377EA76C423A A7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y'..I...I...I..`...I..`...I...H.R.I..`...I..`...I..`...I..`...I...7...I..`...I..`...I.Rich. .I.....PE..d.....[J....." ....$...V.....v.....G.....@...../..{.... ...../...~...!.....`..... .....0.....text...["....$..... ..`.data....5...@...0...(.....@....pdata.../.....0...X.....@..@.rsrc.....@..@.reloc..0.....j.....@ ..B..[J`...+.[Jk...5.[Ju.....[J.....[J.....[J....+.[Jk.....[J.....[J.....[J.....[J.....msvcrt.dll.NTDLL.DLL.RPCRT4.dll.ole32.dll.USER32.dll.KERNEL32.dll.VERSION.dll.WIN SPOOL.DRV.GDI32.dll.OLEAUT32.dll.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\unires_vpd.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	771040
Entropy (8bit):	5.631799273811714
Encrypted:	false
SSDEEP:	12288:rkozBEoNh3bBPc/s4430ye84TF1dbua5TVhRre3kf8lKHgikinLC:dzBEGbL4Np84TQazCSiRC
MD5:	2AC9DA11C87F558D785924C5E814A6C2
SHA1:	6EDF8B0224B9D2F666E2DB4E093703508DABF512
SHA-256:	4CC04BFD8ED79191FAF1520B3ABA80B45E2EEB653D7C48A960CD18A59C04E001
SHA-512:	C4DA961C9C6A3AB586B8FDAFDF8D4C59A48D902E4300925B28E275DF1168E6FC1C2D51E4EB1E07429401090ABB4FD97AC7AC96E78DE50EBAC887B6007C1F4 D3A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u..E...E...E...LI..D...LI..D...RichE.....PE..d.....[J....." .. ..@.....@.....0.....!.....rsrc..... .....@..@.....0...8.....P.....@.....r.....s...x...t...8...u.....v.....w...0...x.....y.....(.....X..... (.....h.....P..... .....8.....P.....h.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x64\vccorlib120.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	356528
Entropy (8bit):	5.917051105867173
Encrypted:	false
SSDEEP:	6144:0g5dgFfqaKFJyHrByeUIRAHq0KzS9OAgfVgYCDlSv:0OdcUIRAHqAeX0a
MD5:	BDD8AE768DBF3E6C65D741CB3880B8A7

SHA1:	91B01FD48A586822C1D81CA80B950F8639CCE78C
SHA-256:	602ADD77CBD807D02306DE1D0179CB71A908EECB11677116FC206A7E714AB6D6
SHA-512:	7840554A66F033E556CF02772B8B3749C593657CA254E0F2DBD93B05F4600E11BA821EBA8FC038115C038B5E5AF2F8D2CF0A5AE1F1362E813CF0B5041BBBFF9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c...'.@.'.@.'.@....!.@.a...#.@.....&.@.a...%.@.a...*.@.a.../.@..P.. .@.'.A.T.@.a...6.@.a...&.@.a...&.@.a...&.@.Rich'.@.....PE..d...}.OR....." .....n.....L.....`.....>...D.....P....." ...2...>...`.....`...p.....text....l.....n..... ..`.rdata.....r.....@..@.data...x...`.....F.....@....pdata..."......$.... .....@..@minATL.....@.....@..@.rsrc.....P.....@..@.reloc.....`.....@..B.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\msvcp120.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	455328
Entropy (8bit):	6.698367093574994
Encrypted:	false
SSDEEP:	12288:uZ/8wcqw2oe+Z3VrfwfNOOoWhUgiW6QR7t5ss3Ooc8DHkC2e77/:W/8wVwHZFTwFOOos3Ooc8DHkC2e77/
MD5:	FD5CABBE52272BD76007B68186EBAF00
SHA1:	EFD1E306C1092C17F6944CC6BF9A1BFAD4D14613
SHA-256:	87C42CA155473E4E71857D03497C8CBC28FA8FF7F2C8D72E8A1F39B71078F608
SHA-512:	1563C8257D85274267089CD4AEAC0884A2A300FF17F84BDB64D567300543AA9CD57101D8408D0077B01A600DDF2E804F7890902C2590AF103D2C53FF03D9E4A5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o...+.N+.N+.N.3wN).N+.N..Nm.aN(.Nm.cN#.Nm.]N..Nm.\Ne .Nm.YN-.Nm.`N*.Nm.gN*.Nm.bN*.NRich+.N.....PE..L....|OR....."!.....0.....x....@.....W..L...<...<..... .....>.....D.....K..@.....<.....text...<..... ..`.data....^...0...0... .....@....idata.....P.....@..@.rsrc..... j.....@..@.reloc...D.....F...n.....@..B.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\msvcr120.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	970912
Entropy (8bit):	6.9649735952029515
Encrypted:	false
SSDEEP:	12288:LBmFyjLAOQaYkxGXPfY7eiWWcpOKnpTVOIxhK765qlRRb6x4pI23IbJQV:dmFyjLF847eiWWcoGZVOIxh/WxIAlbGV
MD5:	034CCADC1C073E4216E9466B720F9849
SHA1:	F19E9D8317161EDC7D3E963CC0FC46BD5E4A55A1
SHA-256:	86E39B5995AF0E042FCDAA85FE2AEFD7C9DDC7AD65E6327BD5E7058BC3AB615F
SHA-512:	5F11EF92D936669EE834A5CEF5C7D0E7703BF05D03DC4F09B9DCFE048D7D5ADFAAB6A9C7F42E8080A5E9AAD44A35F39F3940D5CCA20623D9CAFE373C63557 F7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S9...XIA.XIA.XIA..A.XIA.XmA.XIAQ..A.ZIAQ..AvXIAQ..A!XIAQ..A.XI AQ..A.XIAQ..A.XIAQ..A.XIARich.XIA.....PE..L....|OR.....!.....D..... .....@.....`.....R..(....p.....>.....d]..@...8..... .....H...@.....P.....text..... ..`.data...4e.....V.....@....idata.....P.....@....rsrc.....p.....0.....@..@. reloc..d].....^...4.....@..B.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\ntprint.inf

Process:	C:\Windows\System32\msiexec.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	9698
Entropy (8bit):	3.8395767056459316
Encrypted:	false
SSDEEP:	192:jxUPudWfG9sPEd5yVplXhzPGeQ6cGIDGzBs+2o5WcicJXoNaTXy:jyxFeGIDIFXoNT
MD5:	6476F7217D9D6372361B9E49D701FB99

SHA1:	E1155AB2ACC8A9C9B3C83D1E98F816B84B5E7E25
SHA-256:	6135D3C9956A00C22615E53D66085DABBE2FBB93DF7B0CDF5C4F7F7B3829F58B
SHA-512:	B27ABD8ED640A72424B662AE5C529CDDA845497DC8BD6B67B0B44AE9CDD5E849F627E1735108B2DF09DD6EF83AD1DE6FAA1AD7A6727B5D7A7985F92A92CA 779
Malicious:	false
Preview:	.....;. .N.T.P.R.I.N.T...I.N.F. .(.f.o.r. .W.i.n.d.o.w.s. .S.e.r.v.e.r. .2.0.0.3. .f.a.m.i.l.y.).....;....;. .L.i.s.t. .o.f. .s.u.p.p.o.r.t.e.d. .p.r.i.n.t.e.r.s.,. .m.a.n.u.f.a.c.t.u.r.e.r.s.....;... .....[.V.e.r.s.i.o.n.].....S.i.g.n.a.t.u.r.e.=.".$.W.i.n.d.o.w.s. .N.T.$."".....P.r.o.v.i.d.e.r.=.".M.i.c.r.o.s.o.f.t.".....C.l.a.s.s.G.U.I.D.=.{.4.D.3.6.E.9.7.9.-.E.3.2.5.-.1.1.C.E.-.B.F.C.1.- .0.8.0.0.2.B.E.1.0.3.1.8.}.....C.l.a.s.s.=.P.r.i.n.t.e.r.....C.a.t.a.l.o.g.F.i.l.e.=.n.t.p.r.i.n.t...c.a.t.....D.r.i.v.e.r.I.s.o.l.a.t.i.o.n.=.2.....D.r.i.v.e.r.V.e.r.=.0.6./.2.1./.2.0.0.6.,.6...1. ..7.6.0.0...1.6.3.8.5.....[.M.a.n.u.f.a.c.t.u.r.e.r.].....".M.i.c.r.o.s.o.f.t.".=.M.i.c.r.o.s.o.f.t.,.N.T.a.m.d.6.4.....[.M.i.c.r.o.s.o.f.t...N.T.a.m.d.6.4.].....".{.D.2.0.E.A.3.7.2.-.D.D.3.5.- .4.9.5.0.-.9.E.D.8.-.A.6.3.3.5.A.F.E.7.9.F.0.}.". .=. .{.D.2.0.E.A.3.7.2.-.D.D.3.5.-.4.9.5.0.-.9.E.D.8.-.A.6.3.3.5.A.F.E.7.9.F.0.}.,. .{.D.2.0.E.A.3.7.2.-.D.D.3.5.-.4.9.5.0.-.9.E.D.8.- .A.6.3.3.5.A.F.

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\printer.ico

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows icon resource - 6 icons, 32x32, 4 bits/pixel, 16x16, 4 bits/pixel
Category:	dropped
Size (bytes):	10134
Entropy (8bit):	5.364629779133003
Encrypted:	false
SSDEEP:	96:75LkqDCmLVf89uqywWrvNCB4isySOc3AOv2B+YT1/44tuU+3:1OmLVf4dErvNCB5tSOc3AY2BP944g
MD5:	6F70BD62A17EC5B677EC1129F594EE6F
SHA1:	4FB95EB83A99C0DA62919C34886B0A3667F3911E
SHA-256:	FC8570D50C1773A1B34AA4E31143FD0776E26FF032EE3EEB6DB8BFAB42B4A846
SHA-512:	615A7E8738B2CF1BC47C8D5FC1357C1299080D0BAA1E54129D0DEBDB6BA60CD366364BE0BDAFDABCBA60F16544B0516A50B4B0182E8BCF01F59171003CE9B 244
Malicious:	false
Preview:	....f.....(...N... .....v.....h..... .... .h....#..(... ...@..... x.....wx.....ww.....ww.x.....ww.xx.....ww.wxx.....w.wwxx.....wwwxx.....xwwwx.....xwwwx.....xwww..x.....xww.wx.x.....xw.wwwx.x.... ...x.w|.x.x.x.....z.x.ww..x.....x.x.ww....x.....x..w....x.x.....x.....p.x.....x.....x.....p.....p..... .....?.....?.....(..... ..... .x.....w.....w.x.....wx.....wwx.....w

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\rupd.gpd

Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	17415
Entropy (8bit):	4.618177193109944
Encrypted:	false
SSDEEP:	384:U1EQCr2g2t2g2F2s2J2m2p2z2ZOgoNJUTIZah25Dy:3oLILwfcV86ZO3eTIZzy
MD5:	8EE7FD65170ED9BD408E0C821171B62A
SHA1:	9D14A87A049C3B576CEC4B28210F0C95B94E08E0
SHA-256:	EE1E4D9869188CC3FA518C445ECF071845E5BD8BE56767A9F7F7DD3ACE294BA5
SHA-512:	5740AB3545D2217BA2156C58BA9AF6681D73116AB5DFBEAA5AB615D9CD0C77716C25865E67188E9D7892B340776755D4CBB1A3E98FAEAF8B6BB4B2CCA00D8A E6
Malicious:	false
Preview:	*GPDSpecVersion: "1.0"..*GPDFileVersion: "1.0"..*GPDFileName: "***.GPD"..*Include: "STDNAMES_VPD.GPD"..*ModelName: "*****"..*MasterUnits: PAIR(40800, 1 17600)..*ResourceDLL: "UNIRES_VPD.DLL"..*PrinterType: PAGE..*MaxCopies: 99....*Feature: Orientation..{.. *rcNameID: =ORIENTATION_DISPLAY.. *Defa ultOption: PORTRAIT.. *Option: PORTRAIT.. {.. *rcNameID: =PORTRAIT_DISPLAY.. *Command: CmdSelect.. {.. *Order: DOC_SETUP.6.. *Cmd: "".. }.. }.. *Option: LANDSCAPE_CC270.. {.. *rcNameID: =LANDSCAPE_DISPLAY.. *Command: CmdSelect.. {.. *Order: DO C_SETUP.6.. *Cmd: "".. }.. }..}..*Feature: InputBin..{.. *rcNameID: =PAPER_SOURCE_DISPLAY.. *DefaultOption: AUTO...*Option: AUTO.. {.. *rcNameID: =AUTO_DISPLAY.. *Command: CmdSelect.. {.. *Order: DOC_SETUP.9.. *Cmd: "".. }.. }.. *Option: CASSETTE.. {.. * rcNameID:

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\rupd.ini

Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.479503224130279
Encrypted:	false
SSDEEP:	3:z8ANyq3jIZc:z8cy2wc
MD5:	610DFCD7FF61B76DAAC9DDC3CDAA64A9
SHA1:	343A63A7E2B0617F30B94E15E236DF7892FE722D

SHA-256:	7BA0ACE1E899C38CB5E8BF303868C0AB4B9890D536009CF21C958B114888DFA3
SHA-512:	D8095398ACC9DE610E42EAB655145BBACB09AE2D460906F9B490E48947EA802795C00CBFA3C674CDCC344D8A64FD63961D2D4A8999E0F0BADAFD3E367FE8B495
Malicious:	false
Preview:	[OEMFiles] ..OEMConfigFile1=rupdui.dll ..

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\rupd.lng

Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	98650
Entropy (8bit):	4.192473934109759
Encrypted:	false
SSDEEP:	768:5rENOwVRq6rZmor3CmRxhESLGZ0s1JP2PY6rZIshvwmE2uJJ6rZqDJK1YRo6rZGx:S9miFao0WDn
MD5:	1614E6CDF119FD284D476F7E6723B3AD
SHA1:	3FF9164C9E5FC47169CC1C6EECA22AAB099F2EA3
SHA-256:	C8DF350F95FFEEED30060092DC8666EADCE040A4DDCB98E7A9293F87D19387A8
SHA-512:	8FBCB156B2F9637BC15FA71758A361CB2500F5A19875EE6BE2B52FC3171C38353A6CDC623E36777D052E0B319C7AF934D2D1DBE92E69666C9B9AD749610BA471
Malicious:	false
Preview:	..[.E.n.g.l.i.s.h.].....L.a.n.g.I.D.=.1.0.3.3.....;. .l.o.o.k. .f.o.r. .l.a.n.g.u.a.g.e. .i.d.e.n.t.i.f.i.e.r.s. .i.n. .M.S.D.N. .-. .'.T.a.b.l.e. .o.f. .L.a.n.g.u.a.g.e. .I.d.e.n.t.i.f.i.e.r.s.'. .t.o.p.i.c.....;. .S.T.A.N.D.A.R.D. .D.I.A.L.O.G. .B.U.T.T.O.N.S.:.....1.=.O.K.....2.=.C.a.n.c.e.l.....;. .P.R.I.N.T.I.N.G. .P.R.E.F.E.R.E.N.C.E.S.:.....;. .C.o.m.m.o.n. .s.t.r.i.n.g.s.....;. .b.i.t.s. .p.e.r. .p.i.x.e.l.....5.0.0.0. .=. .1. .b.i.t. .-. .b.l.a.c.k. .a.n.d. .w.h.i.t.e.....5.0.0.1. .=. .4. .b.i.t.s. .-. .1.6. .c.o.l.o.r.s.....5.0.0.2. .=. .8. .b.i.t.s. .-. .2.5.6. .c.o.l.o.r.s.....5.0.0.3. .=. .2.4. .b.i.t.s. .-. .t.r.u.e. .c.o.l.o.r.....;. .C.o.m.p.r.e.s.s.i.o.n.....5.0.0.4. .=. .N.o.n.e.....5.0.0.5. .=. .A.u.t.o.m.a.t.i.c.....5.0.0.6. .=. .C.C.I.T.T. .m.o.d.i.f.i.e.d. .H.u.f.f.m.a.n. .R.L.E.....5.0.0.7. .=. .C.C.I.T.T. .G.r.o.u.p. .3. .f.a.x. .e.n.c.o.d.i.n.g.....5.0.0.8. .=. .C.C.I.T.T. .G.r.o.u.p. .4. .f.a.x. .e.n.c.o.d.i.n.g.....5.0.0.9. .=. .L.e.m.p.e.

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\rupdpm.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	34272
Entropy (8bit):	6.279189104394536
Encrypted:	false
SSDEEP:	384:sPE2+V5RqtDLvnmQ67I+Ud26uiGKjjAVAjXzjrMishb8pL4g2t4Qh5ZSZwJdLSZb:s2gnH6sDGuB3jrRpLr2t4QhvpPKgCv
MD5:	52B7FE7D8EB30DB65D821F513C99532A
SHA1:	2D29A4B71DA3992352AFD2C49E0234C93DD993AC
SHA-256:	49898528597E2423086D53F9639068AF46D060EB2ABDFEEE7D28CE069CF86F91
SHA-512:	7EF81871AF993327792EBFE5920E464120F9088E9E55971ABE04B77FA4E75365B24898954B27972A6A74DA622CD1088094E3952E5939CB844AC9A063DF3BD703
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....pZ.Y4;..4;..4;...4...:;..=C'.<;..=C6.9;..4;...;..=C!.7;..=C .5;..=C1.q;.....5;..=C&.5;..=C#.5;..Rich4;.....PE..L...L0.\.....!.....F.....D.....`.....Uz....@.....U..W....M.....p.....d...!.....@...@.....t.....text....E.....F..... .`.data...\....`.....J.....@....rsrc.....p.....P.....@..@.reloc.....T.....@..B.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\rupdui.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	160224
Entropy (8bit):	6.183469966253267
Encrypted:	false
SSDEEP:	3072:TYmfMb3REEgw5ojOfC0ZV1AxNjwE0cqR4n2AMNR0wmlmo+W+DAeU:Xfso0ZV12Njwhcqy2AMNxwzEA1
MD5:	91EF01D7DFB11B218B67DB346562161F
SHA1:	F27B8A35BA7630C6AA26E21872CA1EE706642D1B
SHA-256:	48BA5C22A72132A140A881A62B20CE778DDB1B6E495BCD23FAAFC43FB01FB3B1
SHA-512:	FE3AC0AF8822780CA36F1BB9A9E1F5E4168E61415E4CCE8CC20F8E402D9E5EA9F53E5B2F0680C65213D81C04A3193BF2D85C0BAF3256009549D01319B18D924
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\.q.\.q.\.q..h..].q...._.q.....P.q.....X.q.....T.q.U...].q.\.p..q.U...K.q..V..V.q..V..D.q..V..].q.Q...].q.\...].q..V..].q.Rich\.q.....PE..L....0.\.....!.....L...N.....0.....`.....^....@.....I.....(.....P...!.....@ .....Xz..@.....`.....text....J.....L..... ..`.rdata..DC...`...D...P.....@..@.data....\.....@....rsrc...(.....@..@.reloc..@ .....".....@..B.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\setupdrv.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	88032
Entropy (8bit):	6.425120133434353
Encrypted:	false
SSDEEP:	1536:Df1NQO+vd2nRnm4Mxcdn/2hYN7ZOdrkgUzinLnx9oxGcZ:Jo2nRmxcFe5xNUz8D8
MD5:	243C54EF85CA15238782BE036632E0C5
SHA1:	93358BA47E32F9B7513ACD2A27E3F86C9F037497
SHA-256:	00ED874B46999FC5E48F145B9DF3792EA7204FFF3DB28EE035BAF2EFB8DD9902
SHA-512:	C9EE7E75F4BBB5934D1A0344375C68AE8B2A229857E7A3B0D1AED0A7CFFCD074F4D502B7D1B13928E793FE69A6ACC056D3CF98011FABE3B21E513D2E9D943B2D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G..&...&...&....^..&...wF..&...wy..&...wD..&...wx..&...^...&...&..0&..$.|..&...tB..&...&...&..$.G..&..Rich.&.....PE..L...C0.\.....n.....@.....p.....@.....t.....@..|.....6...!...P.....8.....`...@.....text..... ..`.rdata...F.....H.....@..@.data...p....0.....@....rsrc.....@.....@..@.relo c.....P..... .....@..B.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\stdnames_vpd.gpd

Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	14366
Entropy (8bit):	4.1817849062232195
Encrypted:	false
SSDEEP:	192:NjThm8JC986ITRCzEzEpYNwtd29u7ZTl8hF:yFzOnS7z0
MD5:	7162D8977515A446D2C1E139DA59DED5
SHA1:	952F696C463B8410B1FA93A3B2B6DAE416A81867
SHA-256:	2835A439C6AE22074BC3372491CB71E6C2B72D0C87AE3EEE6065C6CAADF1E5C8
SHA-512:	508F7CA3D4BC298534AB058F182755851051684F8D53306011F03875804C95E427428BD425DD13633EEC79748BB64E78AAD43E75B70CC5A3F0F4E6696DBB6D8E
Malicious:	false
Preview:	*%%% Copyright (c) 1997-1999 Microsoft Corporation..*%%% value macros for standard feature names and standard option names..*%%% used in older Unidrv 's.....*CodePage: 1252 *% Windows 3.1 US (ANSI) code page....*Feature: RESDLL..{.. *Name: "resource dll files".. *ConcealFromUI?: TRUE.... *Option: UniresDLL.. {.. *Name: "unires_vpd.dll".. }..}....*Macros: StdFeatureNames..{.. ORIENTATION_DISPLAY: RESDLL.UniresDLL.11100.. PAPER_SIZE_DISPLAY: RESDLL.UniresDLL.11101.. PAPER_SOURCE_DISPLAY: RESDLL.UniresDLL.11102.. RESOLUTION_DISPLAY: RESDLL.UniresDLL.11103.. MEDIA_TYPE_DISPLAY: RESDLL.UniresDLL.11104.. TEXT_QUALITY_DISPLAY: RESDLL.UniresDLL.11105.. COLOR_PRINTING_MODE_DISPLAY: RESDLL.UniresDLL.11106.. PRINTER_MEMORY_DISPLAY: RESDLL.UniresDLL.11107.. TWO_SIDED_PRINTING_DISPLAY: RESDLL.UniresDLL.11108.. PAGE_PROTECTION_

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\unidrv_rupd.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	383968
Entropy (8bit):	6.6511922978509315
Encrypted:	false
SSDEEP:	6144:9plBo/TK5C+psQzJzCSX6hjg+4GRr3CoA7f3j5G+hinZ5P31uGX7Zum8oyk7lAT8:Z0/djgEUhWnJ2UlxqOttoICvPn/318SW
MD5:	49A0A7C3E3F5DF3DDE7121109F1C9C21
SHA1:	716DA115C392CA06379A33079A54722800C13054
SHA-256:	CA38185341294720808A389C34D45FAF2EF7962A7D45AC7696823A6D05B45072
SHA-512:	9BBD8C585E42EC50D6FA9A38BCD39720F7A4F4730A1C8EECC3C5ECBADAFDFD6120D7FCAFA9A319F8D94FC962F537BD0B50EB7CAE614F5116B55D330F7FCE0118
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...3g..3g..3g...:;.4g..3g...g...:.=.8g...:.<.2g...:.-..g...:.*.sg.....2g..:.:.2g..:.?.2g..Rich3g.....PE..L...$.[J.....!.....-.....m.....]....@.....x.....!.....8.....t..@.....|.....`.....text...k..... ..`.data.....@....rsrc.....@..@.reloc.....@..Bo.[J8...K.[JC.....[JP.....[J].....[Jg.....[Jq.....msvcrt.dll.WINSPOOL.DRV.KERNEL32.dll.NTDLL.DLL.ole32.dll.GDI32.dll.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\unidrv_rupd.hlp

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows 3.1 help, Tue Apr 17 13:11:56 2001, 21225 bytes
Category:	dropped
Size (bytes):	21225
Entropy (8bit):	3.9923245636306675
Encrypted:	false
SSDEEP:	192:g8qo9MqLEGX9WkaNWvbAsmrEGckkwy95/HLQdu:g8rMqLwkW8AsqEHkkwy7N
MD5:	6798F64959C913673BD66CD4E47F4A65
SHA1:	C50FAA64C8267AC7106401E69DA5C15FC3F2034C
SHA-256:	0C02B226BE4E7397F8C98799E58B0A512515E462CCDAAC04EDC10E3E1091C011
SHA-512:	8D208306B6D0F892A2F16F8070A89D8EDB968589896CB70CF46F43BF4BEFB7C4CA6A278C35FE8A2685CC784505EFB77C32B0AABF80D13BCC0D10A39AE8AFB5 5A
Malicious:	false
Preview:	?_.....R..r...i.....(),.aabo.utadvanc.edAllows.andareas.assigned.availabl.ebebookl.etc-.hang.e..racter@Clickc. o.de..sColo.rc.0..scon.taindefa.ultdepth.directlyi.0o r..sh..PD.isplaysd.ocument.P.sdraftse.n, ex..nal.featuref.ilesfl.....PrFor..m..-.to-trayf.romgraph$ic.@sh@.to.neH.@dhig.herIfima.gesininE..atio..sta.ll.@..itLe.t..Listsl. o..*.nualm.em..meta..2mS.tM!...enhoto..Oy.w.o.per\.ngop.timizh ...@.nsor..p.....spa3.Pri.ntp.0..ed.0..0er.@-spe.cific.@s1 .m.q..ityQ.0.relaB.RET.k.ghseese.l..edsets.oft Somes0ourc}.P ed.S.@sb.'.poo...gsuchsu.pporttak.est..tha...eT..'.oTo...TrueType...l.usevie@wWhenw. e.1.rw..hwil.lyouyour.;bynewof.fs/...&....;)....z4.....N .....|CF0.lR..|CF1..R..|CF2..R..|CF4..R..|CF5..R..|CONTEXT..)..|CTXOMAP.. ..|FONT.. ..|Petra..2..|PhrImage.....|PhrIndex.....|SYSTEM.2...|TOPIC.....|TTLBTREE..!..|Topic Id.=J.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\unidrvui_rupd.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	756192
Entropy (8bit):	6.198619685669809
Encrypted:	false
SSDEEP:	12288:lIIoM3g2e9Bg7Lg3yfKDPc97QpAxuKdwSGnZGxS:lvM36KkyCLW7QCwSGoS
MD5:	D66F58A5DF5AADDD348CB06B9326B84D
SHA1:	56B390BBB29DAEFE3171491D5697986A7D7AA0B3
SHA-256:	30D2605C283885C99E3F97D876989DE9E34380B20CF01D24DFDBE4CB50C92603
SHA-512:	5F0BF8698AE8809AF13D7E1504C1BF50BCDEC5C146A0AFA9F78174448E2D9A61AA83589C7836B452F3F9029FFBAAB8902138791EBFAD0EEB31B687A9EF7716E D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....".wf..$f..$f..$o.%$n..$f..$...$o.#$u..$o.3$8..$o."$g..$o.4$.. .$AZ.$g..$o.$$g..$o.!$g..$Richf..$.....PE..L.....L.....!....2...2.....e.....@....(p.....K$....@.....{....3.....p.....h...!...`...0...@ ..8.....@.....text...E1.....2..... ..`.data.....P.....6.....@....rsrc.....p.....T.....@..@.reloc...0...`...2...6..... ....@..B..LX.....Lc...o..Ln...&..Lx.....L....n..L....%..L....K..L.....L....r..L.....msvcrt.dll.RPCRT4.dll.ole32.dll.USER32.dll.KERNEL32.dll.NTDLL.DLL.VERSION.dl l.WINSPOOL.DRV.GDI32.dll.OLEAUT32.dll.....

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\unires_vpd.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	771040
Entropy (8bit):	5.630737263013527
Encrypted:	false
SSDEEP:	12288:UkoGBEoNh3bBPc/s4430ye84TF1dbua5TVhRre3kf8IKHgikinLz:kGBEGbL4Np84TQazCSiRz
MD5:	41933A3BF1A30E05DC81ACCDA893E2B9
SHA1:	3C99CC28A6DB76000E3A31DC93C76AE18E2CD20D
SHA-256:	9C5CDC7BE14F3D404423EF9A8EA5A3EDC0157AA5F96F428FE7D857CE5F312FA2
SHA-512:	C5101249DB23080D76264505BF2DFCD636D99509E2DAA0CF601D5E997D145BF71721C2CFDB05AE0AFFD64317F7585040B2F7B48467367542C89D0F1F40F41D0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u..E...E...E...LI..D...LI..D...RichE.....PE..L.....L.....!.. .....@.....@.....!.....rsrc.....@.. @.....0...8.....P.....@.....r.....s...x...t...8...u.....v.....w...0...x.....y.....(.....X.....(.... .....h.....P..... .....8.....P.....h..... ....0...

C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\vccorlib120.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	247984
Entropy (8bit):	6.601853231729306
Encrypted:	false
SSDEEP:	6144:+SsS5fv6EATwqlGwyfDyodYl3ZubfW5nb2PQuW0x:+l5fv6EATwqlGwyfDyodYl3Zv1C
MD5:	69837E50C50561A083A72A5F8EA1F6A2
SHA1:	1A4B4C6C3CB6A5164CC1018AC72D0300455B3D8F
SHA-256:	9C9D4E421C55F7EF4E455E75B58A6639428CCD75C76E5717F448AFE4C21C52BC
SHA-512:	FD20C6B4EEC972C775681AD7322769D5074108D730727051EF77D779A277D77B12419E1FEE1E2EC0CF376A235573A85AD37975245DBF078DE467953AFD02164A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0p..Q..Q..Q..)..Q.....Q.....Q.....Q.....Q..P...Q..Q...Q.....Q..... .Q.....Q.....Q..Rich.Q.....PE..L....OR....."!.....4.....:....@.....e=...A.....`.....>...p...R..0..... ..../..@.....@.....text..... ..`.data...xp.....n.....@....idata.....@.....".....@..@minATL.....P.....0.....@..@.rsrc.... ....`.....2.....@..@.reloc...R...p...T...6.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\eventmsg.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	53560
Entropy (8bit):	6.504835643855465
Encrypted:	false
SSDEEP:	768:wsmrWdCS5PvBHOUYTKJgr0OMpqdBwFrGjYqSwCpRAMxkE1:wza/pu/TKJ/OMpTryYfwc5x5
MD5:	B2E6147F97DAE696265A089F98CE8106
SHA1:	418F20EC486B7A9368CEFF183E7CEBAE9BA52101
SHA-256:	44917B2C260FEA3A0F4691F6E986C25E31B3F9FF22DCD055526199B4D8A54051
SHA-512:	789DD02281B71FAB54F42B92B5C0C76C0266C40100DBE532AD3EBBF968E8A9E674F0BE57E2FFDB10EB4A6B4FAA15A6A6A92907C020C6CD2990427D890D7F5026
Malicious:	false
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...q.7`.....$.....@.....`.....i..... ..q.....P.....8!...@..... ...$.....text..... ..`.itext..... ..`.data...<.....@....bss.....5.....idata.....@....didata.$..... .....@....edata..q.... .....@..@.rdata..E....0.....@..@.reloc.....@.....@..B.rsrc.....P.....@..@.....`.....@ ..@.....

C:\Program Files (x86)\Remote Utilities - Host\libeay32.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1389368
Entropy (8bit):	6.858641353727598
Encrypted:	false
SSDEEP:	24576:2NaU+KpPikndiNfzN4jH3PlMQzMjYpOtJqTp/kqg1:+lUfzN4jH3PlyjYpOLqd/kP1
MD5:	B043371158191670097861855813192 9
SHA1:	6513C7C14F19FA37C73926FC098A9DA678621E04
SHA-256:	26B24DCD9CB7AB8761AE7FB597704F81E2A6EDE6572A247C39A969960DBBA539
SHA-512:	A1D8BCD4B641B5E54A4435A70E19A56ECCE6DC9C7D9B6FC28F7829DE96D139C9CFD10F35F096529F8D33583BEA8FFE1B6C2636F2710D9D01F1A7513F77DB8589
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....lU.*(4.y(4.y(4.y!L<y.4.y!L-y34.y(4.y.4.y...y#4.y(4.y=4.y!L;y.6 .y!L*y)4.y!L,y)4.y!L)y)4.yRich(4.y.....PE..L...#..]..... !.....d.....A.....6..x.....0.....8!.....p..... .....@.....(.....text..... ..`.rdata..XY.....Z.....@..@.data.....t.....@....rsrc...0.....Z.....@..@.reloc..,... .....`.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10931000
Entropy (8bit):	6.790449999326776
Encrypted:	false
SSDEEP:	196608:mY28xa5k15O2/w9DcmIHsZYk3BL5tksbmd:mY28xZh/xcY6LtbA

MD5:	6AAE165F3B1575DB887A0370CFC80083
SHA1:	18BC72662B4366035932719EF131417AACF9C184
SHA-256:	0C89262A283C80121BA1176345B230D0ADE61CFCF682B92E555A48206FB4074A
SHA-512:	666F1A5C6B0C7A5315D70EB0D75DA6232105E5673B44F6137BE4B10377B8D07C21720D05360CC653F543657478B08EEE1D95DB5FB1CB8D82D5C2A0F2FF68E7C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe, Author: Joe Security • Rule: MALWARE_Win_RemoteUtilitiesRAT, Description: RemoteUtilitiesRAT RAT payload, Source: C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...,.9e.....z...,&.....@.....7.....@.....@.....p.....*W....d.....8!.....D..... ...8.....Dt.....text..... ....`.itext...X...0...Z...$..... ..`.data...p<.....>...~.....@....bss.....idata..*W.....X.....@... .didata.Dt.....v.....@....edata.....p.....@..@.tls....h.....rdata..].....@..@.reloc...D.....F.....@..B.rsrc...d..... .....@..@.....p.....@..@.....

C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21148984
Entropy (8bit):	6.620129778488873
Encrypted:	false
SSDEEP:	196608:Sd9U0CaHFxbNvfkPrWcrKZPYOrnnGdDoFl0wb6AIALUKyL5w2kEdyMZNAxa:Sd9U0HxxUPzoPGUAIALUKy/L
MD5:	652C2A693B333504A3879460D0AF7224
SHA1:	235BA3847DF3F39AD445B5B912CB2FB5224D9E59
SHA-256:	760E2FD3E57186B597D40B996811768E6C4A28CA54685E029104FCF82F68238D
SHA-512:	A717E916E9D881970694856F79F0E571B95C350F0B771027188DC9B27AB99C193149D4FE0E32CB4638C840340EB1DBD7FBF7458A58985A3E5BE7DA3345CD86C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe, Author: Joe Security • Rule: MALWARE_Win_RemoteUtilitiesRAT, Description: RemoteUtilitiesRAT RAT payload, Source: C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe, Author: ditekSHen
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...8.9e.....&...jR.....>.....@....@.....O.....HC...@.....@....._.....T.9.....B.8!.....0..... .....(.....text...`.....`...r..... @....didata.....@....edata.....V.....@..@.tls....h.....rdata..].....X.....@..@.reloc..0.....Z.....@..B.rsrc...T.9..... ..9..x.....@..@.....?.....2.....@..@.....

C:\Program Files (x86)\Remote Utilities - Host\ssleay32.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	346424
Entropy (8bit):	6.566551582367787
Encrypted:	false
SSDEEP:	6144:f6MNzVTEz1LgXCpfoaDRQHojjYkARhcPL0U2pHGS5VdQ/TOEzrqArrpA1riT1PiH:f6MNzVgz1LgXCpfoaDqHojjYkARqPL0Z
MD5:	74F9696BE4B46F04A1263C3181405C35
SHA1:	CF66B349BEAA2BC25ED5807763E32018E4304C7B
SHA-256:	D6E8BEE1A9476ED3BE229F4BE81CC1154F1ED425E50E74FD1ABCD76C56EA062C
SHA-512:	F122E00B795476809994733028346D82945566CE4C2BE26444F02E077658CCB1BA0F3FE221CEF37837941054FE4B3B54B3F9A74861F890E56544D1453823FD68
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....`...3...3...3...3...3..f3...3..w3...3..q3...3...3i..3..a3...3..p3...3.. v3...3..s3...3Rich...3.....PE..L...#..]..... .....!.....l.....i5.....y.....@....).....<....0..0.....(..8!...@....,..@.....@ ...@.....text...j..... ..`.rdata.....@..@.data....[.....@.....@....rsrc...0....0.....@..@.reloc...3...@...4..... .....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\vp8decoder.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	389936
Entropy (8bit):	6.646719638285826
Encrypted:	false

SSDEEP:	6144:EIIDyjBnydesbWoiwS7dVIclCzoqHO/gCaEkkH8TuX6RTrWD4siZMZ+LG4IPWwck:EI8tiDOzyH9H8Tu6h04fZMZoMPuvf6d
MD5:	C14000F68306F1CF0EC799DF9568AE01
SHA1:	788D8D7A0BA86BA6C7EF4F7AE50CDC65DDB348FF
SHA-256:	53B040341CE80F246C8437A99DF5252A48801E2154EB94DC50AF54A75D8D85AC
SHA-512:	2D4769949832794CE310474F843B696EA8EEB819554ECD72C449981988A6F8FBC5155D84A97D8A4C015348B3DFE6708F88C64B257D4A4D0D4A03DD068DDA411
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....".....#.O...T8.....T8.....T8.....'..... ...Rich.....PE..L...v..T.....!..... .....2.....0.....@q.....q.....0!.....(...1..8.....U..@ .....0.....text..... ....`.rdata...J...0...L...$.....@..@.data...H>.....p.....@....rodata.....@..@.rsrc..... .....@..@.reloc...(.....*.....@..B.....

C:\Program Files (x86)\Remote Utilities - Host\vp8encoder.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1641784
Entropy (8bit):	6.688224632605251
Encrypted:	false
SSDEEP:	49152:vSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSvSSSSSSSSSSSSSSlwwwwwwwwwwwwwwW:vSSSSSSSSSSSSSSSSSSSSSSSSSSSSSg
MD5:	30448DB0AAC5AC16D7AD789011BF8D20
SHA1:	457A43F6D2A0120C138DD9D57BCB64B21F84D9D7
SHA-256:	D781088435617CA1FACF74C1304F82AFCB388813A75C8CB32213541D35B21832
SHA-512:	300E3AE2AC133E2494C449354582AD9BE51731D3E92D161B998DB14262CC08436EEDDB2B73A2F47CB4D1245348055F19E02721638A64A0630F513D4919B359DD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:J<A[$oA[$oA[$o...o@[$o...o.[$o...op[$o...o.[$o...oC[$o...oL[$oA[%o.[$oA[$op[$o...o@[$oL..o.[$oL..o@[$oL..o@[$oL..o@[$oRichA[$o.....PE..L...}..T.....!.....>.....*.....!..... (.....7.....8!.....@.....text..... ..`.rdata.....@..@.data...$r.....".....@.... rodata.....@..@.rsrc....7.....8...0.....@..@.reloc.....h.....@..B.....

C:\Program Files (x86)\Remote Utilities - Host\webmmux.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	267064
Entropy (8bit):	6.532234442351241
Encrypted:	false
SSDEEP:	3072:zW218gr7s2yIHB0pTPdTX9zUbEbStE97zjAs1RtTcJTfIv0se7POWu/HgsGU1VTD:zWSfr7sXSmPDbKPJ6/AsNk+N
MD5:	5E8673834662AC42B8363E19BC719282
SHA1:	BB1C1ED731830A03DB47D232E748DF4E4D196DB9
SHA-256:	A64A113955EC0D89AE6FF357F9BB1063C7DD29FE5610EE516A94AC17B11172C2
SHA-512:	3CF558B2D3CA03AED1EF0CFE36FB7FF3FE7A3AF63A4C3B0CB6CF13C58BAACAE17E5A01BAD743AFFAE8C4F5B9F5425DD4A97755ACA2DED99E70D782F699A9E225
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@~..!..!..!...p...!...p..!...p..+!..M...!..M...!..!..!..M...!..s..!..s..!..s..!. .s..!..Rich.!.....PE..L...{..T.....!.....N.....k.....0.....c[.....4...x.....8!...../.....Ha..@..... .!.....text..... ..`.rdata..v.....@..@.data....B....."....@....rsrc.....@..@.reloc.../.....0.....@..B. .....

C:\Program Files (x86)\Remote Utilities - Host\webmvorbisdecoder.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	374584
Entropy (8bit):	6.776430632714067
Encrypted:	false
SSDEEP:	6144:saoH9sDRlDLD0GDkEp00tc6TKUOmrRK1jRsAOO04sAO88Rt:ooPH0GgEp0gVd1ValsQXsH
MD5:	95D30B282132FB591FD5FDD94E52AF05
SHA1:	EB7ABE2F02C19EE41E4EFC2506337288141D70ED
SHA-256:	E6C04DC8359B2C76F765FCE37EC123D33ACBC5CE93E60022BA88EB7C867AC3F6

SHA-512:	9E4EA23519D243D6D3AE93D2501F05F35AA1CC6264ADB8F180F8A255BD35FB7996E110AC0EC7960FA0B93062BE45EB0C0922D9597E76EE8180781CC5C9A9C7 2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Mm..,...,...,...}...,...}...,...}...,...,...,...,...,...,...~...,...~...,...~... ,...~...,..Rich.,.....PE..L...t..T.....!.....b.....K....@.....M.....@N..d.....0.....8!.....d&..... ...p/..@.....T.....text...=..... ..`.rdata...E.....F.....@..@.data...|<...`.....H.....@...._RDATA.....d.....@..@.rsrc...0 .....j.....@..@.reloc..d&.....(...n.....@..B..... .....

C:\Program Files (x86)\Remote Utilities - Host\webmvorbisencoder.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	881464
Entropy (8bit):	5.2453925074994965
Encrypted:	false
SSDEEP:	12288:DTAPYZEyRr+NDnaLyx2lz8MSjtX08pYRc29qcQmsGahsQZsbRNl:cYF+Eyx2lzujtElYRc1cQmsGa7ONl
MD5:	A663E7EF3F3CD7A1D4790B4EBF491C27
SHA1:	BFE086E653D0BC8D20ACAE61990BA4FA33F2A1F7
SHA-256:	8B1F95D7C0FDF25A6278347AFDA2F5AC4C86045C7FC530A330BE885D8A87EA68
SHA-512:	E78460C287646F509A50B878A34392546E01803A46C389E942073013A8292E3653713F2B6067842ECCCB09B7CDC13D1D9FFF76065AA61910FC3CEBE6A1C20C47
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A....u...u...u..C$G.3u..C$y.lu..C$x..u...V..u...S..u...u..ju...H..u...'} .&u...'D..u...'C..u...'F..u..Rich.u.....PE..L...s..T.....!.....R.....0.....\.....@.....`.....d....P..p.....R..8!...`...D.... .....@.....0..T.....text...}..... ..`.rdata.....0....."....@..@.data...|<.....@...._RDATA.....@..... ....@..@.rsrc...p....P.....@..@.reloc...D...`...F.....@..B..... .....

C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	
Process:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
File Type:	HTML document, Unicode text, UTF-8 text, with CR line terminators
Category:	dropped
Size (bytes):	5364
Entropy (8bit):	5.485641443773401
Encrypted:	false
SSDEEP:	96:l0xccoJxML6RLidRLildgy99M/0bSOtfh/:lzcWS6pidpiHgyMMVtJ/
MD5:	F2E6FCC4D409479E68C5301C9A696197
SHA1:	48EBE4DB096CB4E318F3D69BEC6672FE13652035
SHA-256:	2A8CC3D804AA9FE8D87A392B4587D360B3DB47D0B88FDE34943AC395D13E803B
SHA-512:	4E818F5503CF118F80EF0DD6AFAB952F016BE24EBE56D34AEE23F56748361573C03472B194E982C32608973A730CCE525A13D0D1885023F213C691E4C7933131
Malicious:	false
Preview:	<head>.<meta http-equiv="content-type" content="text/html; charset=utf-8" />.<meta name="copyright" content="TektonIT" />.<meta name="description" content="Remote Manipulator System - Server software, event log. Tektonit.com" />.<title>Remote Utilities – ... ..</title>.<style type="text/css">.body {.font-family: Courier New, monospace;.font-size: 100%;.background-color: #FFFFFF;.} .h1 {.font-size: 130%;.margin: 0px 0px 0px 0px;.} .textarea {.display: none;.margin-top: 5px;.width: 100%;.} . .main_table td {.border: 1px dashed #DADADA;.} ..e_l_0 {.background-color: #4c4cff;.border: 1px solid red;.} ..e_l_1 {.background-color: #fff04c;.border: none;.} ..e_l_2 {.background-color: #ffa94c;.border: none;.} ..e_l_3 {.background-color: #fc2727;.border: none;.} .#log_header td {.font-weight: bold;.} .#subheader {.font-size: 70%;.color: #DADADA;.margin-bottom: 10px;.} .</style>.<script language="javascript">.function show_textarea(elem) {.var parent_node = elem.parentNode;.var nod

C:\ProgramData\Remote Utilities\install.log	
Process:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	333
Entropy (8bit):	4.961347298932099
Encrypted:	false
SSDEEP:	6:HUc+jLmKRLQUUc+jLdd/ao+Uc+jLhHujHO7eVmUc+jLwmnXjKV+Uc+jLOLGeXkR+:0c+jfCvc+jDSoRc+j9Be7c+jRTmc+j6l
MD5:	57527D70DBA3E2FEB786357C144B5586
SHA1:	AFA68E6C5CC3FFA2E1B0148168C961B124B1FAB3
SHA-256:	85AEC0FB9F246A37363CD4FD1FAED3168DDC09901F700C7A4D1A6B6B3FA7625B
SHA-512:	01787D98D47BE918869D421405C8CFAB7D5AE0F8984E24BF6103614C8D2AC9A8A19468CD2E222EF4E69BBCD5CDE2FEB359113B2435C12C270F6886ED4792CA 8
Malicious:	false

Preview:	02-02-2024_09:37:08#T:SilentInstall: installation 70220..02-02-2024_09:37:08#T:SilentInstall: NTSetPrivilege:SE_DEBUG_NAME:false. OK..02-02-2024_09:37:08#T:SilentInstall: OpenService: service not found_1. OK..02-02-2024_09:37:08#T:SilentInstall: CreateService. OK..02-02-2024_09:37:08#T:SilentInstall: finished (installation) 70220..

C:\ProgramData\Remote Utilities\msi\70220_{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\Exel.msi

Process:	C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Number of Characters: 0, Last Saved By: InstallShield, Number of Words: 0, Title: Remote Utilities - Host 7.2 installation package, Comments: This installer contains the logic and data to install Remote Utilities - Host 7.2, Keywords: Installer,MSI,Database, Subject: Remote Utilities - Host 7.2, Author: Remote Utilities Pty (Cy) Ltd., Security: 1, Number of Pages: 200, Name of Creating Application: InstallShield 2021 - Premier Edition with Virtualization Pack 27, Last Saved Time/Date: Wed Oct 25 17:17:52 2023, Create Time/Date: Wed Oct 25 17:17:52 2023, Last Printed: Wed Oct 25 17:17:52 2023, Revision Number: {BFB6CB81-8A2D-41FC-A737-5CF8EB370093}, Code page: 1252, Template: Intel;1033
Category:	dropped
Size (bytes):	22656000
Entropy (8bit):	7.906722436026202
Encrypted:	false
SSDEEP:	393216:WL2lXkXWYidpIsMLU9zQR5bFvt8uy+zZKKRa8n2o8lQKai847ZxNwb:WLY6G3Mgxmvtry+zxk8wTxNO
MD5:	DBC84F3FE9ECE7369D0FA36E34CE4844
SHA1:	37412165A73BCD574D7F2F34147F2A530FEB7936
SHA-256:	3E88E8A58C47562ED0FC4302BC22247C6D5282757CC18C316757475176FF48C1
SHA-512:	F0969CFB4B23050779391C852961E71A93C8CB1ED7378585FB573A15510D289F942286B7D302D9E352DC77CBE5A539307DC3EA923EC4A06895E072E36B815111
Malicious:	false
Preview:	.....>.....Z.....8.....6.....}..... ....!...!..."..."...#...#...$...$...%...%...&...&...'...'...(...(...)...)...*...*...+...+...,...,...-...-...../.../...0...0...1...1...2...2...3...3...4...4...5...5...6.....<..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...@...M...:...;...=.....?.....A...B...C...D...E...F...G...H...I...J...O...L...N.....P...Q...R...U.....V...Z...X...Y.....[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\Exel.msi

Process:	C:\Users\user\Desktop\3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Number of Characters: 0, Last Saved By: InstallShield, Number of Words: 0, Title: Remote Utilities - Host 7.2 installation package, Comments: This installer contains the logic and data to install Remote Utilities - Host 7.2, Keywords: Installer,MSI,Database, Subject: Remote Utilities - Host 7.2, Author: Remote Utilities Pty (Cy) Ltd., Security: 1, Number of Pages: 200, Name of Creating Application: InstallShield 2021 - Premier Edition with Virtualization Pack 27, Last Saved Time/Date: Wed Oct 25 17:17:52 2023, Create Time/Date: Wed Oct 25 17:17:52 2023, Last Printed: Wed Oct 25 17:17:52 2023, Revision Number: {BFB6CB81-8A2D-41FC-A737-5CF8EB370093}, Code page: 1252, Template: Intel;1033
Category:	dropped
Size (bytes):	22656000
Entropy (8bit):	7.906722436026202
Encrypted:	false
SSDEEP:	393216:WL2lXkXWYidpIsMLU9zQR5bFvt8uy+zZKKRa8n2o8lQKai847ZxNwb:WLY6G3Mgxmvtry+zxk8wTxNO
MD5:	DBC84F3FE9ECE7369D0FA36E34CE4844
SHA1:	37412165A73BCD574D7F2F34147F2A530FEB7936
SHA-256:	3E88E8A58C47562ED0FC4302BC22247C6D5282757CC18C316757475176FF48C1
SHA-512:	F0969CFB4B23050779391C852961E71A93C8CB1ED7378585FB573A15510D289F942286B7D302D9E352DC77CBE5A539307DC3EA923EC4A06895E072E36B815111
Malicious:	**true**
Preview:	.....>.....Z.....8.....6.....}..... ....!...!..."..."...#...#...$...$...%...%...&...&...'...'...(...(...)...)...*...*...+...+...,...,...-...-...../.../...0...0...1...1...2...2...3...3...4...4...5...5...6.....<..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...@...M...:...;...=.....?.....A...B...C...D...E...F...G...H...I...J...O...L...N.....P...Q...R...U.....V...Z...X...Y.....[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Windows\Installer\49a7b6.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Number of Characters: 0, Last Saved By: InstallShield, Number of Words: 0, Title: Remote Utilities - Host 7.2 installation package, Comments: This installer contains the logic and data to install Remote Utilities - Host 7.2, Keywords: Installer,MSI,Database, Subject: Remote Utilities - Host 7.2, Author: Remote Utilities Pty (Cy) Ltd., Security: 1, Number of Pages: 200, Name of Creating Application: InstallShield 2021 - Premier Edition with Virtualization Pack 27, Last Saved Time/Date: Wed Oct 25 17:17:52 2023, Create Time/Date: Wed Oct 25 17:17:52 2023, Last Printed: Wed Oct 25 17:17:52 2023, Revision Number: {BFB6CB81-8A2D-41FC-A737-5CF8EB370093}, Code page: 1252, Template: Intel;1033
Category:	dropped
Size (bytes):	22656000
Entropy (8bit):	7.906722436026202
Encrypted:	false
SSDEEP:	393216:WL2lXkXWYidpIsMLU9zQR5bFvt8uy+zZKKRa8n2o8lQKai847ZxNwb:WLY6G3Mgxmvtry+zxk8wTxNO
MD5:	DBC84F3FE9ECE7369D0FA36E34CE4844
SHA1:	37412165A73BCD574D7F2F34147F2A530FEB7936
SHA-256:	3E88E8A58C47562ED0FC4302BC22247C6D5282757CC18C316757475176FF48C1
SHA-512:	F0969CFB4B23050779391C852961E71A93C8CB1ED7378585FB573A15510D289F942286B7D302D9E352DC77CBE5A539307DC3EA923EC4A06895E072E36B815111

Malicious:	false
Preview:	.....>.....Z.....8.....6.....}..... ....!...!..."..."...#...#...$...$...%...%...&...&...'...'...(...(...)...)...*...*...+...+...,...,...-...-...../.../...0...0...1...1...2...2...3...3...4...4...5 ...5...6.....<..... ....!..."...#...$...%...&...'...(...)...*...+...,...,...-...-...../...0...0...1...2...2...3...3...4...5...6...6...7...7...@...@...M...M...: ..:...=.....?.....A...B...C...D...E...F...G...H...I...J...O...L...N.....P...Q...R...U.....V...Z...X...Y.....[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q. ..r...s...t...u...v...w...x...y...z...

C:\Windows\Installer\49a7b9.msi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Number of Characters: 0, Last Saved By: InstallShield, Number of W ords: 0, Title: Remote Utilities - Host 7.2 installation package, Comments: This installer contains the logic and data to install Remote Utilities - Host 7.2, Keywords: I nstaller,MSI,Database, Subject: Remote Utilities - Host 7.2, Author: Remote Utilities Pty (Cy) Ltd., Security: 1, Number of Pages: 200, Name of Creating Application: Inst allShield 2021 - Premier Edition with Virtualization Pack 27, Last Saved Time/Date: Wed Oct 25 17:17:52 2023, Create Time/Date: Wed Oct 25 17:17:52 2023, Last Printed: Wed Oct 25 17:17:52 2023, Revision Number: {BFB6CB81-8A2D-41FC-A737-5CF8EB370093}, Code page: 1252, Template: Intel;1033
Category:	dropped
Size (bytes):	22656000
Entropy (8bit):	7.906722436026202
Encrypted:	false
SSDEEP:	393216:WL2lXkXWYidpIsMLU9zQR5bFvt8uy+zZKKRa8n2o8lQKai847ZxNwb:WLY6G3Mgxmvtry+zxk8wTxNO
MD5:	DBC84F3FE9ECE7369D0FA36E34CE4844
SHA1:	37412165A73BCD574D7F2F34147F2A530FEB7936
SHA-256:	3E88E8A58C47562ED0FC4302BC22247C6D5282757CC18C316757475176FF48C1
SHA-512:	F0969CFB4B23050779391C852961E71A93C8CB1ED7378585FB573A15510D289F942286B7D302D9E352DC77CBE5A539307DC3EA923EC4A06895E072E36B815111
Malicious:	false
Preview:	.....>.....Z.....8.....6.....}..... ....!...!..."..."...#...#...$...$...%...%...&...&...'...'...(...(...)...)...*...*...+...+...,...,...-...-...../.../...0...0...1...1...2...2...3...3...4...4...5 ...5...6.....<..... ....!..."...#...$...%...&...'...(...)...*...+...,...,...-...-...../...0...0...1...2...2...3...3...4...5...6...6...7...@...M...: ..:...=.....?.....A...B...C...D...E...F...G...H...I...J...O...L...N.....P...Q...R...U.....V...Z...X...Y.....[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q. ..r...s...t...u...v...w...x...y...z...

C:\Windows\Installer\MSIAB6F.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	169896
Entropy (8bit):	6.068969720857241
Encrypted:	false
SSDEEP:	3072:jqSoP/44Yvge5XKhpKJJdu+ew+BZPHbN2e9n2p+:j5g/ve5XKhMVJSIun6+
MD5:	B5ADF92090930E725510E2AAFE97434F
SHA1:	EB9AFF632E16FCB0459554979D3562DCF5652E21
SHA-256:	1F6F0D9F136BC170CFBC48A1015113947087AC27AED1E3E91673FFC91B9F390B
SHA-512:	1076165011E20C2686FB6F84A47C31DA939FA445D9334BE44BDAA515C9269499BD70F83EB5FCFA6F34CF7A707A828FF1B192EC21245EE61817F06A66E74FF509
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....`,"..Bq..Bq..Bq..q..Bq<.q..Bq..q..Bq..q/.Bq..qh.Bq.y.q..Bq.y. q..Bq..Cq..Bq..q..Bq..q..Bq..q..Bq...q..Bq..q..BqRich..Bq.....PE..L.....,a.....!.....p...$.....U.....m.....`..p.....x.. .....p.....@.....text....o.....p..... ..`.rdata..M.....t.....@..@.data....1... .....@....rsrc...p....`.....$..... .....@..@.reloc...L...p...N...*.....@..B.....

C:\Windows\Installer\MSIACD8.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	1408583
Entropy (8bit):	4.8128312343081046
Encrypted:	false
SSDEEP:	24576:HMMMMMMSLLLLLLLTMMMMMMSLLLLLLLJMMMMMMSLLLLLLLg:HMMMMMMSLLLLLLLTMMMMMMSLLLLLLLJr
MD5:	C1D50A44D3E5171DAEC6BDBF802AC9A5
SHA1:	0707ACD0DED1024989A8043E344D87E7A96218F8
SHA-256:	26C3BE848122AD72E9AF24FE877761D46AE92E34383704F763B4D3D529446D86
SHA-512:	C08F0A7E8741B7C12604A1C267CEA786C917FBC916748DD52D05D80603C2DEB5F23EAAE202A71E5157466CE54CBCA1BE6798A22BFB79D94FA81D2FE3EF1F31 3B
Malicious:	false

Preview:	...@IXOS.@.....@.LBX.@.....@.....@.....@.....@.....@.....&.{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}..Remote Utilities - Host..Exel.msi.@.....@.....@.....@.....@.....ARPPRODUCTICON.exe..&.{BFB6CB81-8A2D-41FC-A737-5CF8EB370093}.....@.....@.....@.....@.....@.....@.....@.....@.....@.....Remote Utilities - Host.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration...@.....@.....@.].....&.{26EAB54E-4659-47E8-86F9-4CB74F7E03BE}/.C:\Program Files (x86)\Remote Utilities - Host\.@.....@.....@.....@.....&.{596F4636-5D51-49F5-B3B4-F3C366E9DC23}...@.....@.....@.....@.....@.....@....&.{00000000-0000-0000-0000-000000000000}.@.....@.....@.....&.{3244CDE6-6414-4399-B0D5-424562747210}...@.....@.....@.....@.....@.....&.{197F692B-7CCA-4D79-85A5-ED04202D08D0}...@.....@.....@.....@.....&.{E79AC184-AD38-4B26-89D0-75B7CEA19FA2};.C:\Program Files (x86)\Remote Utilities - Host\Printer\x86\.@.....@.....@..

C:\Windows\Installer\SourceHash{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1620403438347329
Encrypted:	false
SSDEEP:	12:JSbX72FjMiliAGiLlIHVRpzh/77777777777777777777777vDHFwd8mvbLHpc:JEQI53W8qXa8F
MD5:	0A729EC420FB3F9CFEEA56D3C5E02D22
SHA1:	781F706A6827E089154CE5270FC9F2D27C503F35
SHA-256:	D14BFCF752F4EDD77151479A460CCD7F085C2803D594A1325A016FD215E8B9C6
SHA-512:	E2BFD7255B6296B52C95C91917C101A9C7F0C74DA4373FC784B5213B142CF278E9787B7E4418F07302BCEF9785E450F4C745A4313084B70BA856916DDA061262
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\inprogressinstallinfo.ipi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.895945339984345
Encrypted:	false
SSDEEP:	48:g8Ph4uRc06WXJuFT5d9ue9mSKdTfdTuOdThRXdTpkdTpdTKdTt6AdTnUo94SB29Y:Ph41FFT4lXJnBy/itbCqLJnBy/i0
MD5:	C54E6183C8ADF3D4D90D07D00FA4BD0E
SHA1:	5E8D8E07E5B9609C8FDF6D055E926F719561027B
SHA-256:	3DB177C510404B0889856D3828FF6AB9E6A1F057A6878304B3DF3E4890F79E78
SHA-512:	60C821E1AD75FB9E2915142222168FB672E9571DD71E0F3A51D19EE8AA13B89F0C325CC8C4D471B9F881C7762D395228D541466978E52B4C3C748142ABC826C4
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\ARPPRODUCTICON.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	71360
Entropy (8bit):	5.493854356833401
Encrypted:	false
SSDEEP:	768:PMAyYdTmPJbgqcnDckJdtwCpKAMxkE0twCRr5AMxkEo:P1U81ckJdtwsoxYtwUdxc
MD5:	C5D9AD25A352AB74B481CB2A0E938E40
SHA1:	400D21EEB68A31136C49C4FE5B3FC042CB278CAB
SHA-256:	885C1CD9C61F93C7284FD1DA853D5C58000419655525413CA469B9D5E806403F
SHA-512:	E919646B606B2C8984D1DD9FF5B6FC4F92930290339263D56487DA8A702EC68551B2950E20EF531B452022F3F9FB61A72F73196826AB3E70BDE5521717666FD5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C...C...C...C...CD..C...C...C...C=..C...C...C...C...C...CRich...C .....PE..L.....-a.....@.....P....@.....4T..(.....t0.....F.....P..... .....text....5.....@..... ..`.rdata.....P.....P.....@..@.data...)...`...0...`.....@....rsrc...t0.....@.....@..@..... ....

C:\Windows\Installer\{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\UNINST_Uninstall_R_3B1E3C8B7D0945898DA82CEEED02F0C7.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	63168
Entropy (8bit):	5.217205507888401
Encrypted:	false
SSDEEP:	768:0dMAyYdTmPJbgqcnDc/soJCtwChfqAMxkE1twC53AMxkE7:u1U81cLJCtwsgxJtws3xP
MD5:	D0F686C7B7334657E93B8DB349F9540D
SHA1:	F855C4FA5FBBCF79C6246AF94EB0046CE8FDCE45
SHA-256:	8DECE53004FFEE3BA42A820D1EBEA3CA1482299A6B5B80D682D9D8CDE3070B31
SHA-512:	C883A8DCD573DF1757FB3737D93B40AB25F83A3896DAF610C0112AF2FDE79EDEE1EC9B9499DF073F4F9D7FB80CD51A8663C4485C8B0DC426CA339032B1902C5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C...C...C...C...CD..C...C...C...C=..C...C...C...C...C...CRich...C.....PE..L.....-a.....@..`.....P....@.....\.....4T..(.....\.....F.....P.....text....5.....@..... ..`.rdata.....P.....P.....@..@.data....)...`...0...`.....@....rsrc...\..... .....@..@.....

C:\Windows\Installer\{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\en_server_settings_E3BFC76BE38F4CF79D2ED7163B7DECEE.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	415424
Entropy (8bit):	4.597963610747478
Encrypted:	false
SSDEEP:	1536:01U81cqS/ZJgAmxJtAqXy/yxREpU1WyY68iuuuu6AppppppppEMMMMMMMSLLLLLl:cjcT6uuuutMMMMMMSLLLLLLeYCk
MD5:	0A46537981B366DA572524EA4F0F834D
SHA1:	55AA01DF1728DEF4F143084839980043DDB536A3
SHA-256:	FA4A8E01B7748A816CDF2CF7D29E2B926EE4200F685DC87B2CFEB3CE4D0AA55D
SHA-512:	D1EA98137B8FC3B9F88500E0CF40792937B6A8C5FC918ED6E20C5304A6E779F4864DDEE70D67E1B5FCDCF1CB63E185E5F6CB66AC08A2993F644D41EFEDA97F40
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C...C...C...C...CD..C...C...C...C=..C...C...C...C...C...CRich...C.....PE..L.....-a.....@.....P....@.....Zj.....4T..(.....u.....F.....P.....text....5.....@..... ..`.rdata.....P.....P.....@..@.data....)...`...0...`.....@....rsrc....u.....@..@.....

C:\Windows\Installer\{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\en_server_start_85DB64512C79429FA70AC6C0611579DD.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	415424
Entropy (8bit):	4.597721784431409
Encrypted:	false
SSDEEP:	1536:W1U81cqS/ZJgAmxJtAqXy/yxREpU1WyY68iuuuu6AppppppppEMMMMMMMSLLLLLj:CjcT6uuuutMMMMMMSLLLLLLeYSa
MD5:	0DFAE3FEC66BC6813B9C75C76DBDF0F4
SHA1:	537352720EB1427EFD8E971C7B1CC4F2A007868F
SHA-256:	3F2B3730D09552BED4B2CF28C1E237313A7BE313F9E330BC77B147F29B96081E
SHA-512:	84BBBAA2A91AB2E6A2D5ACF7D956DCCD24B1ED55F5E1913601EAB2BE5F5BBE8FA59048BCF27A7F731A878990AB6AF644386F2FC41749236F23FE559093B2BDB3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C...C...C...C...CD..C...C...C...C=..C...C...C...C...C...CRich...C.....PE..L.....-a.....@.....P....@.....F.....4T..(.....u.....F.....P.....text....5.....@..... ..`.rdata.....P.....P.....@..@.data....)...`...0...`.....@....rsrc....u.....@..@.....

C:\Windows\Installer\{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\en_server_stop_B603677802D142C98E7A415B72132E14.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	415424
Entropy (8bit):	4.597627123267687
Encrypted:	false
SSDEEP:	1536:31U81cqS/ZJgAmxJtAqXy/yxREpU1WyY68iuuuu6AppppppppEMMMMMMMSLLLLL2:ljcT6uuuutMMMMMMSLLLLLLLeYe
MD5:	13D157111B98791617D98963B653F7FD
SHA1:	062439148EE03C9EFBE24C2E4D801B55F6D76389
SHA-256:	23ACEF13F15429D6F30531224CB1E9C58E64B804351C58A89CE7597CAE1DA6AB
SHA-512:	AC435AC73809178001233E6C8753C5320EE271721E903D1D66FBC65994985A9656CF2A31FD215BC230E5C10F1CAD6B49616E2B6BFEF4FF1213E518E4E8BFE10
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C...C...C...C...CD..C...C...C...C=..C...C...C...C...C...CRich...C .....PE..L.....-a.....@.....P....@.....\.....4T..(.....u.....F.....P..... .....text....5.....@..... ..`.rdata.....P.....P.....@..@.data...)...`...0...`.....@....rsrc....u.....@..@..... ....

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log

Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	432221
Entropy (8bit):	5.375172572548565
Encrypted:	false
SSDEEP:	1536:6qELG7gK+RaOOp3LCCpfmLgYI66xgFF9Sq8K6MAS2OMUHI6Gin327D22A26KgauB:zTtbmkExhMJCIpEr4
MD5:	6BC3260469EC902DB1D090931B067D6A
SHA1:	2A20547F710A0AF56CF53F253B12AE6E35522274
SHA-256:	E87E04370D79BC679540D592857C0C34F36876A8698ACBEBB8CBF9FC24C2024E
SHA-512:	F4913C0EA6682CEE3C9E23F8DC263630F16D68517A08C3265F03407CCF08701C3899E658C8BC8A885B755AB7846699AAE7C49CCDE3261AC0D1EC6CB9889015
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..12/07/2019 14:54:22.458 [5488]: Command line: D:\wd\compilerTemp\BMT.200yuild.1bk\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe executeQueuedItems /nologo ..12/07/2019 14:54:22.473 [5488]: Executing command from offline queue: install "System.Runtime.WindowsRuntime.UI.Xaml, Version=4.0.0.0, Culture=Neutral, PublicKeyToken=b77a5c561934e089, processorArchitecture=msil" /NoDependencies /queue:1..12/07/2019 14:54:22.490 [5488]: Executing command from offline queue: install "System.Web.ApplicationServices, Version=4.0.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil" /NoDependencies /queue:3..12/07/2019 14:54:22.490 [5488]: Exclusion list entry found for System.Web.ApplicationServices, Version=4.0.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil; it will not be installed..12/07/2019 14:54:22.490 [

C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\26C212D9399727259664BDFCA07 3966E_C5856A5EB1E3B74AE8014850A678CDBF

Process:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
File Type:	data
Category:	dropped
Size (bytes):	314
Entropy (8bit):	6.642066835146045
Encrypted:	false
SSDEEP:	6:ZOxjUpUGgtzuaUUG5o7lpP/pUG3QltzuanflflcZa3kK6l2cZbNjF:ZPnaUUG5FgIgaNfGZaUycZbNB
MD5:	7C8F509EE8BA0782632512240F655578
SHA1:	D41ED379B131EE745D21B000DF047E1A07C76F88
SHA-256:	56C31A3824DC1B9DB307931E3F4F698D9757C22E2011B7DFB381E5EAC0A12366
SHA-512:	A9D6D4AB73527699B1C03C6215DBE7E06D2DCE0597A1DEF28CF4016B541BDE20CD07DB04A29488C1CB7E634305874734AF9A4BFFEC52C5296B5DC5D9AB68B 4C
Malicious:	false
Preview:	0..6...../0..+..+.....0.....0...0.....H.....6A..cib).K...20240201184200Z0s0q0I0...+.....G+~..w.#.....W.....H.....6A..cib).K.....@....QC.Y..@)....20240201184200Z....20240 208184200Z0...*.H.=....i.0f.1..J(.\.x....5.*..2z.....LY.i;Bn....;r..X..4...1...5...<]VZ..[..?:4O.._..I..'....X.....xk...2...

C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\3EC49180A59F0C351C30F112AD97CFA5_ED80 F76A55EEDF047A88FD3F37D62FA3

Process:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
File Type:	data
Category:	dropped
Size (bytes):	313

Entropy (8bit):	6.5546319534749
Encrypted:	false
SSDEEP:	6:MBN7ULL7ujQQW+G5o7/MqexL7hf4c+ouzQVtqpmwdFiOfUOELX6eqSJZ:MbY+WX5nrxaStqowd7fUOEj6HgZ
MD5:	888564A0B6D055C179A5CA8137F69617
SHA1:	6A31E95C20B58030865F3CA6D1E8CED3794C259F
SHA-256:	5A4A8BEF73E85D46EC53B81F57BA964FD755D101CF7AE7B60F0EB0451B6DE64D
SHA-512:	D7161FA3675131C1359674CE5CEE688FCF96C7129D5A7DE1BE5C08CCD4358F3D8D404D2DF9656E6C2492115257D664D4C7DE787F7B9988C274CCD009DBF804
Malicious:	false
Preview:	0..5.....0..*..+.....0.....0...0....._.6.....'..."...8w...20240202051846Z0s0q0I0...+.....[.x.A.<.q)nj.L.._..._.6.....'..."...8w.....*G..jZ.n#.A~.....20240202050302Z....20240209040302Z0...*.H.=....h.0e.0.}.H.....hw^Cb..'.x.).2.^..-~1p0a.q..'.2.1..OoEb.p1.$7<'.....-}.....V]e%....3s.p1d

C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\26C212D93997272596 64BDFCA073966E_C5856A5EB1E3B74AE8014850A678CDBF

Process:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
File Type:	data
Category:	dropped
Size (bytes):	404
Entropy (8bit):	3.913938006640074
Encrypted:	false
SSDEEP:	12:tcNldkEX66sMNmxMiv8sFpT6er+iTw73br:eAEXbsOmxxvbLFTkbr
MD5:	E27E17654028F5B828483EAD36078AD0
SHA1:	4B7D6AE60A07C14BF50B715D0DBC9B5FDE4C03F3
SHA-256:	2F0A81F46DBE0C6B8FD86D1034000E88A308FFB01CDD299048B9421522EAA070
SHA-512:	9B7754066626796334389 12C80BB2C0BD0E0717B87AE5D9AF37CD6D88000F3E22B8EE2426D59A0838E424D2D84D0087D2B83AE003B58297C31CC74BC0D1F338
Malicious:	false
Preview:	p..... ....g.U..(.....0W>U.....Z.....Z.. .....9a.U.. .....:...h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.r.j.r.y.d.R.y.t.%.2.B.A.p.F.3.G.S.P.y.p.f.H.B.x.R.5.X.t.Q.Q.U.s.9.t.I.p.P.m.h.x.d.i.u.N.k.H.M.E.W.N.p.Y.i.m.8.S.8.Y.C.E.A.%.2.B.4.p.0.C.5.F.Y.0.D.U.U.O.8.W.d.n.w.Q.C.k.%.3.D...

C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3EC49180A59F0C351C30F112AD97CFA5_ED80F76A55EEDF047A88FD3F37D62FA3

Process:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	3.9247957560796167
Encrypted:	false
SSDEEP:	6:kKe38qwaRNfOAUMivhClroFH18WilzmlwyiilHDuel8DtQHl+w4lWqlk77ANn:S8faLmxMiv8sFarlyFiiMe+4l+w4PlZ
MD5:	57DA74F59030AED7A30414D6DD925FBB
SHA1:	39FB0C31C8BF2A032F3D788402B33F4C0E363964
SHA-256:	78D399CA8C184B2F7017C8FEAF5B44D237C4379F7CE95A0A013C707C9501614B
SHA-512:	743F7DEE3E86D585EBCB844F8CA099CB5B2CBC9218F0F842069F50639FAA4D666351314D80051F3F2BCE1F746B12EAD15F7A6FFA1F812E6331AB302F37908F8
Malicious:	false
Preview:	p..... ....$...C.T.U..(.....U....2..[.....2..[.. .....(..U.. .....9...h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.S.E.6.7.N.b.q.3.j.f.Q.Q.g.8.y.X.E.p.b.m.q.L.T.N.n.7.X.w.Q.U.m.1.%.2.B.w.N.r.q.d.B.q.4.Z.J.7.3.A.o.C.L.A.i.4.s.4.d.%.2.B.0.C.E.A.7.z.K.k.e.s.D.W.p.a.7.2.4.j.j.E.F.%.2.B.2.x.0.%.3.D...

C:\Windows\Temp\~DF10BD94535F44088B.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.49702049430394
Encrypted:	false
SSDEEP:	48:2dwuMO+CFXJvT55Ukym9ue9mSKdTfdTuOdThRXdTpkdTpdTKdTt6AdTnUo94SB2i:iwGHT3twlXJnBy/itbCqLJnBy/i0
MD5:	1A8F292A886E376D3C2C702958B09E06
SHA1:	7BCBF4DAE59C69329CDD083A6F192E312E06368C
SHA-256:	800111B992522BBAF77236A54AE82173F1CB7FA83180322908950C4E926A8625
SHA-512:	96FF0F3398CFA46F847CCEA2335AC84D117DDA5A5E945C6D2E2CDAF33DC12A093463AB9F28FACB26D94EFBA5D149591B7AF0B5DBB8798BF375BE1CD3BB1FD640

Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF43AE85119F93081A.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.06887906536849638
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOwd6SumvbfzYsEoVky6l0t/:2F0i8n0itFzDHFwd8mvbLK01
MD5:	BE571F185F10B61BEC870EE494C2DB99
SHA1:	F2C1BE92CDA3689AE4B7C426715C8FA1C31A31CA
SHA-256:	F6BF0799FD664C0732F91B052E213BDBB42BA5AC71D0F846739E9E85B21A59D2
SHA-512:	0D8425263AC7F1B7EF53A3CDB2019135A651BDA8283CE5568A8EC0C8B8ED88ACAFE2A6F00ACD0FD92035D1A0EE9EC2DF04E21B76ADB79CF790883B55AE888 92F
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF46A59DA49B45DF44.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.895945339984345
Encrypted:	false
SSDEEP:	48:g8Ph4uRc06WXJuFT5d9ue9mSKdTfdTuOdThRXdTpkdTpdTKdTt6AdTnUo94SB29Y:Ph41FFT4lXJnBy/itbCqLJnBy/i0
MD5:	C54E6183C8ADF3D4D90D07D00FA4BD0E
SHA1:	5E8D8E07E5B9609C8FDF6D055E926F719561027B
SHA-256:	3DB177C510404B0889856D3828FF6AB9E6A1F057A6878304B3DF3E4890F79E78
SHA-512:	60C821E1AD75FB9E2915142222168FB672E9571DD71E0F3A51D19EE8AA13B89F0C325CC8C4D471B9F881C7762D395228D541466978E52B4C3C748142ABC826C4
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF529C0FE4C5A9CE4B.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF70B43A60818B563C.TMP

Process:	C:\Windows\System32\msiexec.exe

File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF8E23FC32B87CAA71.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF9FE2B93D9F6F7365.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFB588C3675999CB76.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.895945339984345
Encrypted:	false
SSDEEP:	48:g8Ph4uRc06WXJuFT5d9ue9mSKdTfdTuOdThRXdTpkdTpdTKdTt6AdTnUo94SB29Y:Ph41FFT4lXJnBy/itbCqLJnBy/i0
MD5:	C54E6183C8ADF3D4D90D07D00FA4BD0E
SHA1:	5E8D8E07E5B9609C8FDF6D055E926F719561027B
SHA-256:	3DB177C510404B0889856D3828FF6AB9E6A1F057A6878304B3DF3E4890F79E78

SHA-512:	60C821E1AD75FB9E2915142222168FB672E9571DD71E0F3A51D19EE8AA13B89F0C325CC8C4D471B9F881C7762D395228D541466978E52B4C3C748142ABC826C4
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFCE78CABB386C66F3.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DFD5F4580B380072C8.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.49702049430394
Encrypted:	false
SSDEEP:	48:2dwuMO+CFXJvT55Ukym9ue9mSKdTfdTuOdThRXdTpkdTpdTKdTt6AdTnUo94SB2i:iwGHT3twlXJnBy/itbCqLJnBy/i0
MD5:	1A8F292A886E376D3C2C702958B09E06
SHA1:	7BCBF4DAE59C69329CDD083A6F192E312E06368C
SHA-256:	800111B992522BBAF77236A54AE82173F1CB7FA83180322908950C4E926A8625
SHA-512:	96FF0F3398CFA46F847CCEA2335AC84D117DDA5A5E945C6D2E2CDAF33DC12A093463AB9F28FACB26D94EFBA5D149591B7AF0B5DBB8798BF375BE1CD3BB1FD640
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFDE25689DD43B2CB0.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	0.26499363023775985
Encrypted:	false
SSDEEP:	48:QtwXSB29odTfdTuOdThRXdTpkdTpdTKdTl9mSKdTfdTuOdThRXdTpkdTpdTKdTtR:w+qLJnBy/ifXJnBy/itbV
MD5:	4B10A259B2226A26CD98E062FB70F4D6
SHA1:	C6D44E56DEEAD4F3ED0F2AE9D656E88A8A2B258A
SHA-256:	C15AC826D08AB6FC2DDA39716E318A15F291FE8C226AC339B0F56AE784A30407
SHA-512:	63E623E51AC09C3BB7A22AA787C13A06006DAB60CE25020FBDFD4FBEDF808FE82FC555C244246182233E39D091B76C0C379EC3A25C87DFAD4A35FDC5498D34B
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DFE4BF60F9C7AF91F3.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.49702049430394
Encrypted:	false
SSDEEP:	48:2dwuMO+CFXJvT55Ukym9ue9mSKdTfdTuOdThRXdTpkdTpdTKdTt6AdTnUo94SB2i:iwGHT3twlXJnBy/itbCqLJnBy/i0
MD5:	1A8F292A886E376D3C2C702958B09E06
SHA1:	7BCBF4DAE59C69329CDD083A6F192E312E06368C
SHA-256:	800111B992522BBAF77236A54AE82173F1CB7FA83180322908950C4E926A8625
SHA-512:	96FF0F3398CFA46F847CCEA2335AC84D117DDA5A5E945C6D2E2CDAF33DC12A093463AB9F28FACB26D94EFBA5D149591B7AF0B5DBB8798BF375BE1CD3BB1FD640
Malicious:	false
Preview:	.....>..... ....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64, for MS Windows
Entropy (8bit):	7.99798080331911
TrID:	• Win64 Executable GUI (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe
File size:	20'949'417 bytes
MD5:	075d6c122274cb9226521d3cd298f2f2
SHA1:	6f54d70f39fa28596ef90bfcb0c14278b016db1b
SHA256:	92192af947017c20ad861faf4459fb705e63f7083b34c77c1727891b88091573
SHA512:	c89f25e451ae095635bee4df25cbf7bb8431d87017ae65898471b346ee3b2a8694b5a45aa00e4dc54881905643c62843216d402e10faadd195e10922a29573be
SSDEEP:	393216:9Vz6+gdQzi/Ew1x1vXYQBEPDdasNaAzEFuEaP3CxMk50pRZfQCy0lifWA5J8EOx:LHSvl+EPDdXNaHaP4Mk50hfh/ieA5nOx
TLSH:	14273306D79D18FCC8A9E67D985B4C47E633784D2211A48F176949A22F83334ED3F72A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$.2.`.\.`.\.`.\..y..h.\..y....\..y..m.\.....b.\...X.r.\..._.j.\...Y.Y.\.i...i.\.i...b.\.i...g.\.`.].C.\...Y.R.\...\.a.\.....a.\

File Icon

Icon Hash:	0e0f7834fc39070c

Static PE Info

General

Entrypoint:	0x140032dc0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x6579B995 [Wed Dec 13 14:03:01 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5

OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	b1c5b1beabd90d9fdabd1df0779ea832

Entrypoint Preview
Instruction
dec eax
sub esp, 28h
call 00007F11E0BCA2E8h
dec eax
add esp, 28h
jmp 00007F11E0BC9C7Fh
int3
int3
dec eax
mov eax, esp
dec eax
mov dword ptr [eax+08h], ebx
dec eax
mov dword ptr [eax+10h], ebp
dec eax
mov dword ptr [eax+18h], esi
dec eax
mov dword ptr [eax+20h], edi
inc ecx
push esi
dec eax
sub esp, 20h
dec ebp
mov edx, dword ptr [ecx+38h]
dec eax
mov esi, edx
dec ebp
mov esi, eax
dec eax
mov ebp, ecx
dec ecx
mov edx, ecx
dec eax
mov ecx, esi
dec ecx
mov edi, ecx
inc ecx
mov ebx, dword ptr [edx]
dec eax
shl ebx, 04h
dec ecx
add ebx, edx
dec esp
lea eax, dword ptr [ebx+04h]
call 00007F11E0BC9103h
mov eax, dword ptr [ebp+04h]
and al, 66h
neg al
mov eax, 00000001h
sbb edx, edx
neg edx

Instruction
add edx, eax
test dword ptr [ebx+04h], edx
je 00007F11E0BC9E13h
dec esp
mov ecx, edi
dec ebp
mov eax, esi
dec eax
mov edx, esi
dec eax
mov ecx, ebp
call 00007F11E0BCBE27h
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov ebp, dword ptr [esp+38h]
dec eax
mov esi, dword ptr [esp+40h]
dec eax
mov edi, dword ptr [esp+48h]
dec eax
add esp, 20h
inc ecx
pop esi
ret
int3
int3
int3
dec eax
sub esp, 48h
dec eax
lea ecx, dword ptr [esp+20h]
call 00007F11E0BB8693h
dec eax
lea edx, dword ptr [00025887h]
dec eax
lea ecx, dword ptr [esp+20h]
call 00007F11E0BCAEE2h
int3
jmp 00007F11E0BD10C4h
int3
int3
int3
int3
int3
int3

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x597c0	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x597f4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x70000	0x1e324	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x6a000	0x306c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8f000	0x970	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x536c0	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x53780	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x4b3f0	0x140	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x48000	0x508	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x588dc	0x120	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4664e	0x46800	cb5fa3169f581ba82faed363ff4f6e49	False	0.5365483710106383	data	6.468535106678591	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x48000	0x128e4	0x12a00	919da1ea112d11a732dbc754aee3741b	False	0.44967753775167785	data	5.272430005055125	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5b000	0xe75c	0x1a00	17e6aee7483d05299c67ef1c20548699	False	0.28260216346153844	data	3.2575802848760493	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x6a000	0x306c	0x3200	bb12e72c2a1957150354ef39796c9470	False	0.485625	data	5.507547185354104	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.didat	0x6e000	0x360	0x400	ced4b34f6105bed5c533724cbd855e33	False	0.2568359375	data	3.0248828943464656	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
_RDATA	0x6f000	0x15c	0x200	c67570d55af77c6d3a435fe95a2589ac	False	0.40625	data	3.3215020267482327	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x70000	0x1e324	0x1e400	89bca75165439faf93b747f75742c27d	False	0.938646048553719	data	7.896782666673534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8f000	0x970	0xa00	77a9ddfc47a5650d6eebbcc823e39532	False	0.52421875	data	5.336289720085303	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
PNG	0x70524	0x13154	PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced			0.9947162376541631
RT_ICON	0x83678	0x858e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced			0.9985668324071366
RT_DIALOG	0x8bc08	0x2ba	data			0.5286532951289399
RT_DIALOG	0x8bec4	0x13a	data			0.6560509554140127
RT_DIALOG	0x8c000	0xf2	data			0.71900826446281
RT_DIALOG	0x8c0f4	0x14a	data			0.6
RT_DIALOG	0x8c240	0x314	data			0.47588832487309646
RT_DIALOG	0x8c554	0x24a	data			0.6279863481228669
RT_STRING	0x8c7a0	0x1fc	data			0.421259842519685
RT_STRING	0x8c99c	0x246	data			0.41924398625429554
RT_STRING	0x8cbe4	0x1a6	data			0.514218009478673
RT_STRING	0x8cd8c	0xdc	data			0.65

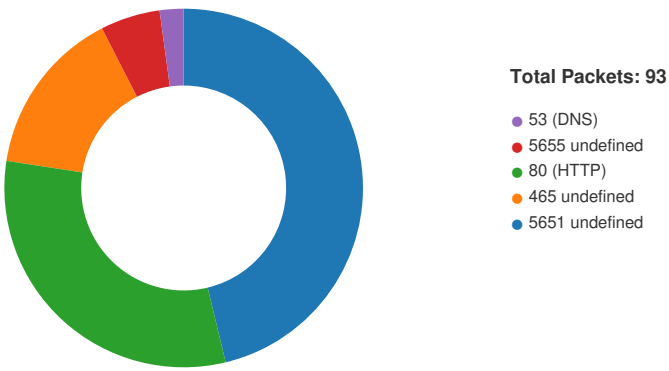
Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_STRING	0x8ce68	0x470	data			0.3873239436619718
RT_STRING	0x8d2d8	0x164	data			0.5056179775280899
RT_STRING	0x8d43c	0x110	data			0.5772058823529411
RT_STRING	0x8d54c	0x158	data			0.4563953488372093
RT_STRING	0x8d6a4	0xe8	data			0.5948275862068966
RT_STRING	0x8d78c	0x1c6	data			0.5242290748898678
RT_STRING	0x8d954	0x268	data			0.4837662337662338
RT_GROUP_ICON	0x8dbbc	0x14	data			1.05
RT_MANIFEST	0x8dbd0	0x753	XML 1.0 document, ASCII text, with CRLF line terminators			0.39786666666666665

Imports

DLL	Import
KERNEL32.dll	LocalFree, GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, GetCurrentProcessId, CreateDirectoryW, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, GetVersionExW, GetModuleFileNameW, SetCurrentDirectoryW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, ExpandEnvironmentStringsW, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, GlobalMemoryStatusEx, LoadResource, SizeofResource, GetTimeFormatW, GetDateFormatW, GetExitCodeProcess, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetNumberFormatW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetOEMCP, IsValidCodePage, FindNextFileA, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TerminateProcess, IsProcessorFeaturePresent, InitializeCriticalSectionAndSpinCount, WaitForSingleObjectEx, IsDebuggerPresent, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlPcToFileHeader, RtlUnwindEx, EncodePointer, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, GetStringTypeW, HeapReAlloc, LCMapStringW, FindFirstFileExA
OLEAUT32.dll	SysAllocString, SysFreeString, VariantClear
gdiplus.dll	GdipCloneImage, GdipFree, GdipDisposeImage, GdipCreateBitmapFromStream, GdipCreateHBITMAPFromBitmap, GdiplusStartup, GdiplusShutdown, GdipAlloc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2024 09:37:22.025059938 CET	49734	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:22.028461933 CET	49735	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:22.041404009 CET	49736	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:22.042712927 CET	49737	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:22.042725086 CET	49738	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:22.051462889 CET	49739	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:22.247539043 CET	5651	49735	101.99.94.54	192.168.2.4
Feb 2, 2024 09:37:22.247647047 CET	49735	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:22.260546923 CET	465	49736	101.99.94.54	192.168.2.4
Feb 2, 2024 09:37:22.260616064 CET	49736	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:22.263031006 CET	80	49737	101.99.94.54	192.168.2.4
Feb 2, 2024 09:37:22.263729095 CET	49737	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:23.027426004 CET	49734	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:23.027559042 CET	49738	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:23.121231079 CET	49737	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:23.121229887 CET	49735	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:23.230521917 CET	49739	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:23.230535984 CET	49736	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:23.714910984 CET	49735	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:23.715123892 CET	49737	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:23.933636904 CET	49736	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:25.105581999 CET	49737	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:25.105581045 CET	49735	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:25.105592012 CET	49734	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:25.105974913 CET	49738	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:25.230550051 CET	49739	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:25.418035030 CET	49736	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:27.368830919 CET	49741	5655	192.168.2.4	64.20.61.146
Feb 2, 2024 09:37:27.489749908 CET	5655	49741	64.20.61.146	192.168.2.4
Feb 2, 2024 09:37:27.489840984 CET	49741	5655	192.168.2.4	64.20.61.146
Feb 2, 2024 09:37:27.490696907 CET	49741	5655	192.168.2.4	64.20.61.146
Feb 2, 2024 09:37:27.490799904 CET	49741	5655	192.168.2.4	64.20.61.146
Feb 2, 2024 09:37:27.611716986 CET	5655	49741	64.20.61.146	192.168.2.4
Feb 2, 2024 09:37:27.683662891 CET	49735	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:27.699285030 CET	49737	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:28.152405977 CET	49736	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:29.105572939 CET	49734	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:29.105745077 CET	49738	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:29.230571985 CET	49739	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:32.840043068 CET	49735	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:32.886811972 CET	49737	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:33.621156931 CET	49736	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:35.988476992 CET	49742	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:35.988694906 CET	49743	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:35.999866962 CET	49744	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:36.018121958 CET	49745	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:36.114202023 CET	49747	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:36.114248037 CET	49746	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:36.996181965 CET	49742	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:36.997667074 CET	49743	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:37.011818886 CET	49744	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:37.027415991 CET	49745	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:37.121166945 CET	49746	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:37.121167898 CET	49747	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:37.532773972 CET	49748	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:37.533879995 CET	49749	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:37.534821033 CET	49750	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:37.621692896 CET	5655	49741	64.20.61.146	192.168.2.4
Feb 2, 2024 09:37:37.621757030 CET	49741	5655	192.168.2.4	64.20.61.146

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2024 09:37:37.753740072 CET	5651	49748	101.99.94.54	192.168.2.4
Feb 2, 2024 09:37:37.753849030 CET	49748	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:37.755201101 CET	465	49750	101.99.94.54	192.168.2.4
Feb 2, 2024 09:37:37.755371094 CET	49750	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:37.755496979 CET	80	49749	101.99.94.54	192.168.2.4
Feb 2, 2024 09:37:37.755561113 CET	49749	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:38.418041945 CET	49748	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:38.418060064 CET	49749	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:38.418364048 CET	49750	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:38.949394941 CET	49750	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:38.949395895 CET	49748	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:38.949398041 CET	49749	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:38.996162891 CET	49742	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:38.996314049 CET	49743	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:39.011812925 CET	49744	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:39.043061972 CET	49745	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:39.121176958 CET	49747	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:39.136789083 CET	49746	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:40.261966944 CET	49750	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:40.261971951 CET	49749	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:40.277654886 CET	49748	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:42.871217966 CET	49749	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:42.873662949 CET	49750	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:42.933794022 CET	49748	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:42.996592999 CET	49742	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:42.997653008 CET	49743	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:43.027424097 CET	49744	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:43.043051958 CET	49745	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:43.121186972 CET	49747	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:43.136895895 CET	49735	5651	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:43.136895895 CET	49746	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:43.246273041 CET	49737	80	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:43.796216965 CET	49751	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:43.875823975 CET	49752	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:44.558669090 CET	49736	465	192.168.2.4	101.99.94.54
Feb 2, 2024 09:37:44.796236038 CET	49751	80	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:44.886828899 CET	49752	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:46.063117981 CET	49753	5651	192.168.2.4	185.70.104.90
Feb 2, 2024 09:37:46.076226950 CET	49754	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:46.173964024 CET	49755	5651	192.168.2.4	77.105.132.70
Feb 2, 2024 09:37:46.191998959 CET	49756	80	192.168.2.4	77.105.132.70

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2024 09:37:27.247483015 CET	65129	53	192.168.2.4	1.1.1.1
Feb 2, 2024 09:37:27.366250038 CET	53	65129	1.1.1.1	192.168.2.4
Feb 2, 2024 09:38:26.122497082 CET	50422	53	192.168.2.4	1.1.1.1
Feb 2, 2024 09:38:26.240483046 CET	53	50422	1.1.1.1	192.168.2.4

DNS Queries

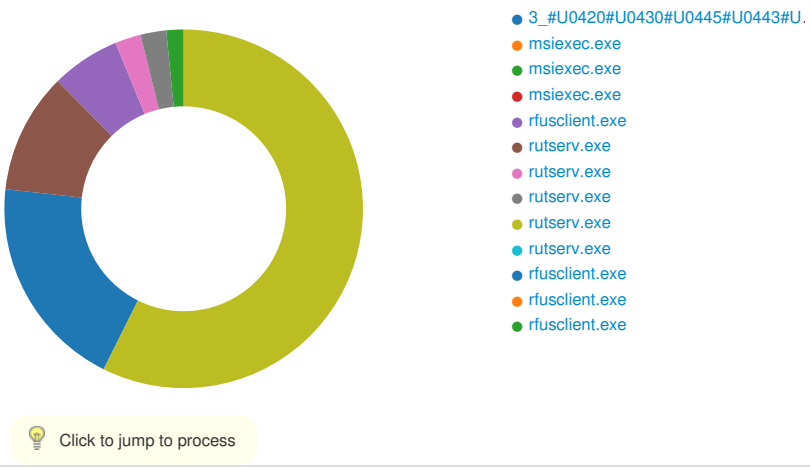
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 2, 2024 09:37:27.247483015 CET	192.168.2.4	1.1.1.1	0x5fc8	Standard query (0)	id72.remotutilities.com	A (IP address)	IN (0x0001)	false
Feb 2, 2024 09:38:26.122497082 CET	192.168.2.4	1.1.1.1	0x5fe1	Standard query (0)	id72.remotutilities.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 2, 2024 09:37:17.167222023 CET	1.1.1.1	192.168.2.4	0x989a	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 2, 2024 09:37:17.167222023 CET	1.1.1.1	192.168.2.4	0x989a	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Feb 2, 2024 09:37:27.366250038 CET	1.1.1.1	192.168.2.4	0x5fc8	No error (0)	id72.remoteutilities.com	id.remoteutilities.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 2, 2024 09:37:27.366250038 CET	1.1.1.1	192.168.2.4	0x5fc8	No error (0)	id.remoteutilities.com		64.20.61.146	A (IP address)	IN (0x0001)	false
Feb 2, 2024 09:38:26.240483046 CET	1.1.1.1	192.168.2.4	0x5fe1	No error (0)	id72.remoteutilities.com	id.remoteutilities.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 2, 2024 09:38:26.240483046 CET	1.1.1.1	192.168.2.4	0x5fe1	No error (0)	id.remoteutilities.com		64.20.61.146	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: 3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe PID: **7316**, Parent PID: **2580**

General

Target ID:	0
Start time:	09:36:56
Start date:	02/02/2024
Path:	C:\Users\user\Desktop\3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\3_#U0420#U0430#U0445#U0443#U043d#U043e#U043a.pdf.exe
Imagebase:	0x7ff6cdb10000
File size:	20'949'417 bytes
MD5 hash:	075D6C122274CB9226521D3CD298F2F2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Has exited:	true

File Activities

Analysis Process: msiexec.exe PID: **7416**, Parent PID: **7316**

General

Target ID:	1
Start time:	09:36:58
Start date:	02/02/2024
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i Exel.msi /qn
Imagebase:	0x7ff6043c0000
File size:	69'632 bytes
MD5 hash:	E5DA170027542E25EDE42FC54C929077
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **7448**, Parent PID: **620**

General

Target ID:	2
Start time:	09:36:58
Start date:	02/02/2024
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff6043c0000
File size:	69'632 bytes
MD5 hash:	E5DA170027542E25EDE42FC54C929077
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	432127	94	30 32 2f 30 32 2f 32 30 32 34 20 30 39 3a 33 36 3a 35 39 2e 34 30 34 20 5b 37 34 34 38 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	02/02/2024 09:36:59.404 [7448]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFDFB0A4B25	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	0	3	success or wait	1	7FFDFB0A4723	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **7528**, Parent PID: **7448**

General

Target ID:	3
Start time:	09:36:59
Start date:	02/02/2024
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 494BECA00E3009394CA5F2713F238EA9
Imagebase:	0xf30000
File size:	59'904 bytes
MD5 hash:	9D09DC1EDA745A5F87553048E57620CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

Analysis Process: rfusclient.exe PID: **7600**, Parent PID: **7448**

General

Target ID:	4
Start time:	09:37:03
Start date:	02/02/2024
Path:	C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe" -msi_copy "C:\Users\user\AppData\Local\Temp\Exel.msi
Imagebase:	0x650000
File size:	10'931'000 bytes
MD5 hash:	6AAE165F3B1575DB887A0370CFC80083
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 00000004.00000000.1716230830.0000000001091000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe, Author: Joe Security • Rule: MALWARE_Win_RemoteUtilitiesRAT, Description: RemoteUtilitiesRAT RAT payload, Source: C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe, Author: ditekSHen
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CC1EE	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\rfusclient.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC262	CreateDirectoryW
C:\ProgramData\Remote Utilities	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AAECE	CreateDirectoryW
C:\ProgramData\Remote Utilities\msi	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AAECE	CreateDirectoryW
C:\ProgramData\Remote Utilities\msi\70220_{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AAECE	CreateDirectoryW
C:\ProgramData\Remote Utilities\msi\70220_{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\Exel.msi	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	E2FCA2	CopyFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Remote Utilities\msi\70220_{3FF12DDA-38DA-466F-B4E3-6775ACEF5538}\Exel.msi	0	1048576	fd fd 11 71 1a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fd fd 09 00 06 00 00 00 00 00 00 00 00 00 00 00 00 5a 01 00 00 01 00 00 00 00 00 00 00 00 10 00 00 38 00 00 00 04 00 00 00 fd 36 00 00 02 00 00 00 00 00 00 fd 00 00 00 fd 00 00 00 7d 01 00 00 00 02 00 00 7f 02 00 00 00 03 00 00 7f 03 00 00 00 04 00 00 7f 04 00 00 00 05 00 00 fd 05 00 00 fd 05 00 00 fd 06 00 00 fd 06 00 00 fd 07 00 00 fd 07 00 00 7f 08 00 00 00 09 00 00 7f 09 00 00 00 0a 00 00 7f 0a 00 00 00 0b 00 00 7f 0b 00 00 fd 0b 00 00 7f 0c 00 00 00 0d 00 00 7f 0d 00 00 00 0e 00 00 7f 0e 00 00 00 0f 00 00 fd 0f 00 00 00 10 00 00 7f 10 00 00 00 11 00 00 7f 11 00 00 00 12 00 00 7f 12 00 00 00 13 00 00 7f 13 00 00 00 14 00 00 7f 14 00 00 00 15 00 00 7f 15 00 00 00 16 00	>Z86}	success or wait	22	E2FCA2	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	0	144	pipe empty	8	6FEB13	ReadFile

Analysis Process: rutserv.exe PID: **7640**, Parent PID: **7448**

General

Target ID:	5
Start time:	09:37:05
Start date:	02/02/2024
Path:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" /silentinstall
Imagebase:	0x340000
File size:	21'148'984 bytes
MD5 hash:	652C2A693B333504A3879460D0AF7224
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 00000005.00000000.1747218595.0000000001803000.00000002.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 00000005.00000000.1747218595.0000000001739000.00000002.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe, Author: Joe Security • Rule: MALWARE_Win_RemoteUtilitiesRAT, Description: RemoteUtilitiesRAT RAT payload, Source: C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe, Author: ditekSHen
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3BE532	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\ProgramData\Remote Utilities\install.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	348415	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Remote Utilities\install.log	0	57	30 32 2d 30 32 2d 32 30 32 34 5f 30 39 3a 33 37 3a 30 38 23 54 3a 53 69 6c 65 6e 74 49 6e 73 74 61 6c 6c 3a 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 37 30 32 32 30 0d 0a	02-02-2024_09:37:08#T:SilentInstall: installation 70220	success or wait	1	34827C	WriteFile
C:\ProgramData\Remote Utilities\install.log	57	77	30 32 2d 30 32 2d 32 30 32 34 5f 30 39 3a 33 37 3a 30 38 23 54 3a 53 69 6c 65 6e 74 49 6e 73 74 61 6c 6c 3a 20 4e 54 53 65 74 50 72 69 76 69 6c 65 67 65 3a 53 45 5f 44 45 42 55 47 5f 4e 41 4d 45 3a 66 61 6c 73 65 2e 20 4f 4b 0d 0a	02-02-2024_09:37:08#T:SilentInstall: NTSetPrivilege:SE_DEBUG_NAME:false. OK	success or wait	1	34827C	WriteFile
C:\ProgramData\Remote Utilities\install.log	134	75	30 32 2d 30 32 2d 32 30 32 34 5f 30 39 3a 33 37 3a 30 38 23 54 3a 53 69 6c 65 6e 74 49 6e 73 74 61 6c 6c 3a 20 4f 70 65 6e 53 65 72 76 69 63 65 3a 20 73 65 72 76 69 63 65 20 6e 6f 74 20 66 6f 75 6e 64 5f 31 2e 20 4f 4b 0d 0a	02-02-2024_09:37:08#T:SilentInstall: OpenService: service not found_1. OK	success or wait	1	34827C	WriteFile
C:\ProgramData\Remote Utilities\install.log	209	56	30 32 2d 30 32 2d 32 30 32 34 5f 30 39 3a 33 37 3a 30 38 23 54 3a 53 69 6c 65 6e 74 49 6e 73 74 61 6c 6c 3a 20 43 72 65 61 74 65 53 65 72 76 69 63 65 2e 20 4f 4b 0d 0a	02-02-2024_09:37:08#T:SilentInstall: CreateService. OK	success or wait	1	34827C	WriteFile
C:\ProgramData\Remote Utilities\install.log	265	68	30 32 2d 30 32 2d 32 30 32 34 5f 30 39 3a 33 37 3a 30 38 23 54 3a 53 69 6c 65 6e 74 49 6e 73 74 61 6c 6c 3a 20 66 69 6e 69 73 68 65 64 20 28 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 29 20 37 30 32 32 30 0d 0a	02-02-2024_09:37:08#T:SilentInstall: finished (installation) 70220	success or wait	1	34827C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	0	144	pipe empty	13	3F0E57	ReadFile
C:\ProgramData\Remote Utilities\install.log	0	128	success or wait	1	348496	ReadFile
C:\ProgramData\Remote Utilities\install.log	0	128	success or wait	1	348496	ReadFile
C:\ProgramData\Remote Utilities\install.log	0	128	success or wait	1	348496	ReadFile
C:\ProgramData\Remote Utilities\install.log	0	128	success or wait	1	348496	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\RManService	success or wait	1	4DC755	RegCreateKeyExW

Analysis Process: rutserv.exe PID: 7676, Parent PID: 7448

General

Target ID:	6
Start time:	09:37:09
Start date:	02/02/2024
Path:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" /firewall
Imagebase:	0x340000
File size:	21'148'984 bytes
MD5 hash:	652C2A693B333504A3879460D0AF7224
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3BE532	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW

File Path	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	0	144	pipe empty	11	3F0E57	ReadFile

Analysis Process: rutserv.exe PID: 7772, Parent PID: 7448

General

Target ID:	8
Start time:	09:37:14
Start date:	02/02/2024
Path:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" /start
Imagebase:	0x7ff6ec4b0000
File size:	21'148'984 bytes
MD5 hash:	652C2A693B333504A3879460D0AF7224
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3BE532	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW

File Path	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	0	144	pipe empty	61	3F0E57	ReadFile

Analysis Process: rutserv.exe PID: **7876**, Parent PID: **620**

General

Target ID:	9
Start time:	09:37:15
Start date:	02/02/2024
Path:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" -service
Imagebase:	0x340000
File size:	21'148'984 bytes
MD5 hash:	652C2A693B333504A3879460D0AF7224
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 00000009.00000003.1896822360.000000000890F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\TEMP\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3BE532	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\ProgramData\Remote Utilities\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	39C3A2	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	39B342	CreateFileW
C:\Windows\TEMP\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	66	3BE532	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	4	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	2	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	3	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	8	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	5	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	13	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	5	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	9	3BE5A6	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	2	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	2	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	3	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW
C:\Windows\TEMP\rutserv.madExcept	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BE5A6	CreateDirectoryW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	0	1993	3c 68 65 61 64 3e 0d 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0d 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 63 6f 70 79 72 69 67 68 74 22 20 63 6f 6e 74 65 6e 74 3d 22 54 65 6b 74 6f 6e 49 54 22 20 2f 3e 0d 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 52 65 6d 6f 74 65 20 4d 61 6e 69 70 75 6c 61 74 6f 72 20 53 79 73 74 65 6d 20 2d 20 53 65 72 76 65 72 20 73 6f 66 74 77 61 72 65 2c 20 65 76 65 6e 74 20 6c 6f 67 2e 20 54 65 6b 74 6f 6e 69 74 2e 63 6f 6d 22 20 2f 3e 0d 3c 74 69 74 6c 65 3e 52 65 6d 6f 74 65 20 55 74 69 6c 69 74 69 65 73 20 26 6e	<head><meta http-equiv="content-type" content="text/html; charset=utf-8" /><meta name="copyright" content="TektonIT" /><meta name="description" content="Remote Manipulator System - Server software, event log. Tektonit.com" /><title>Remote Utilities &n	success or wait	1	39B645	WriteFile
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	1993	275	3c 21 2d 2d 20 7b 35 30 46 46 39 36 43 38 2d 33 36 33 32 2d 34 31 45 37 2d 38 38 39 45 2d 45 38 42 35 32 46 35 46 32 38 32 46 7d 20 2d 2d 3e 0d 3c 74 72 20 63 6c 61 73 73 3d 22 72 65 63 6f 72 64 22 3e 3c 74 64 20 73 74 79 6c 65 3d 22 62 6f 72 64 65 72 3a 20 6e 6f 6e 65 3b 22 20 63 6c 61 73 73 3d 22 65 5f 6c 5f 30 22 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 30 32 2e 30 32 2e 32 30 32 34 2d 2d 2d 30 38 3a 33 38 3a 31 38 3a 37 38 31 3c 2f 74 64 3e 0d 3c 74 64 3e 33 34 3c 2f 74 64 3e 0d 3c 74 64 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 52 65 6d 6f 74 65 20 55 74 69 6c 69 74 69 65 73 20 2d 20 48 6f 73 74 20 37 30 32 32 30 20 69 73 20 73 74 61 72 74 65 64 2e 20 47 4d 54 2b 30 31 3c 2f 74 64 3e 0d 3c 74 64 3e 57 69 6e 64 6f 77 73 20 31 30 2e	{50FF96C8-3632-41E7-889E-E8B52F5F282F} --><tr class="record"><td style="border: none;" class="e_l_0"> </td><td>02.02.2024---08:38:18:781</td><td>34</td><td> </td><td>Remote Utilities - Host 70220 is started. GMT+01</td><td>Windows 10.	success or wait	1	39B645	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	2268	268	3c 21 2d 2d 20 7b 31 45 31 30 46 45 30 31 2d 37 31 33 38 2d 34 33 39 43 2d 41 44 43 46 2d 43 41 32 32 46 42 43 44 38 44 33 46 7d 20 2d 2d 3e 0d 3c 74 72 20 63 6c 61 73 73 3d 22 72 65 63 6f 72 64 22 3e 3c 74 64 20 73 74 79 6c 65 3d 22 62 6f 72 64 65 72 3a 20 6e 6f 6e 65 3b 22 20 63 6c 61 73 73 3d 22 65 5f 6c 5f 30 22 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 30 32 2e 30 32 2e 32 30 32 34 2d 2d 2d 30 38 3a 34 34 3a 30 33 3a 36 37 35 3c 2f 74 64 3e 0d 3c 74 64 3e 39 36 3c 2f 74 64 3e 0d 3c 74 64 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 52 65 6c 61 79 20 6e 6f 64 65 3a 20 4f 4b 3c 2f 74 64 3e 0d 3c 74 64 3e 49 44 3a 20 33 35 30 2d 37 30 30 2d 34 38 39 2d 37 30 39 3b 20 50 6f 72 74 3a 20 35 36 35 35 3b 20 54 72 79 20 63 6f 75 6e 74 3a 20 31	{1E10FE01-7138-439C-ADCF-CA22FBCD8D3F} --><tr class="record"><td style="border: none;" class="e_l_0"> </td><td>02.02.2024---08:44:03:675</td><td>96</td><td> </td><td>Relay node: OK</td><td>ID: 350-700-489-709; Port: 5655; Try count: 1	success or wait	1	39B645	WriteFile
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	2536	248	3c 21 2d 2d 20 7b 31 31 30 33 38 39 46 37 2d 38 46 46 44 2d 34 35 31 35 2d 38 35 37 33 2d 32 36 37 35 38 37 43 42 30 39 36 41 7d 20 2d 2d 3e 0d 3c 74 72 20 63 6c 61 73 73 3d 22 72 65 63 6f 72 64 22 3e 3c 74 64 20 73 74 79 6c 65 3d 22 62 6f 72 64 65 72 3a 20 6e 6f 6e 65 3b 22 20 63 6c 61 73 73 3d 22 65 5f 6c 5f 32 22 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 30 32 2e 30 32 2e 32 30 32 34 2d 2d 2d 30 38 3a 34 37 3a 35 39 3a 33 38 31 3c 2f 74 64 3e 0d 3c 74 64 3e 39 36 3c 2f 74 64 3e 0d 3c 74 64 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 49 6e 74 65 72 6e 65 74 2d 49 44 20 45 72 72 6f 72 43 6f 64 65 20 3c 3e 20 30 3c 2f 74 64 3e 0d 3c 74 64 3e 45 72 72 6f 72 20 63 6f 64 65 3a 20 31 3c 2f 74 64 3e 0d 3c 2f 74 72 3e 0d 0d	{110389F7-8FFD-4515-8573-267587CB096A} --><tr class="record"><td style="border: none;" class="e_l_2"> </td><td>02.02.2024---08:47:59:381</td><td>96</td><td> </td><td>Internet-ID ErrorCode <> 0</td><td>Error code: 1</td></tr>	success or wait	1	39B645	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	3052	248	3c 21 2d 2d 20 7b 35 30 36 30 45 42 41 32 2d 44 30 31 43 2d 34 42 35 44 2d 38 32 30 41 2d 30 43 35 32 44 30 37 34 32 36 37 35 7d 20 2d 2d 3e 0d 3c 74 72 20 63 6c 61 73 73 3d 22 72 65 63 6f 72 64 22 3e 3c 74 64 20 73 74 79 6c 65 3d 22 62 6f 72 64 65 72 3a 20 6e 6f 6e 65 3b 22 20 63 6c 61 73 73 3d 22 65 5f 6c 5f 32 22 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 30 34 2e 30 32 2e 32 30 32 34 2d 2d 2d 31 30 3a 31 30 3a 35 32 3a 37 38 30 3c 2f 74 64 3e 0d 3c 74 64 3e 39 36 3c 2f 74 64 3e 0d 3c 74 64 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 49 6e 74 65 72 6e 65 74 2d 49 44 20 45 72 72 6f 72 43 6f 64 65 20 3c 3e 20 30 3c 2f 74 64 3e 0d 3c 74 64 3e 45 72 72 6f 72 20 63 6f 64 65 3a 20 31 3c 2f 74 64 3e 0d 3c 2f 74 72 3e 0d 0d	{5060EBA2-D01C-4B5D-820A-0C52D0742675} --><tr class="record"><td style="border: none;" class="e_l_2"> </td><td>04.02.2024---10:10:52:780</td><td>96</td><td> </td><td>Internet-ID ErrorCode <> 0</td><td>Error code: 1</td></tr>	success or wait	1	39B645	WriteFile
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	3568	248	3c 21 2d 2d 20 7b 30 46 39 43 37 45 43 38 2d 38 33 32 42 2d 34 36 32 35 2d 38 39 37 39 2d 39 34 30 41 41 43 46 46 37 35 44 33 7d 20 2d 2d 3e 0d 3c 74 72 20 63 6c 61 73 73 3d 22 72 65 63 6f 72 64 22 3e 3c 74 64 20 73 74 79 6c 65 3d 22 62 6f 72 64 65 72 3a 20 6e 6f 6e 65 3b 22 20 63 6c 61 73 73 3d 22 65 5f 6c 5f 32 22 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 30 36 2e 30 32 2e 32 30 32 34 2d 2d 2d 31 32 3a 32 38 3a 32 37 3a 32 35 38 3c 2f 74 64 3e 0d 3c 74 64 3e 39 36 3c 2f 74 64 3e 0d 3c 74 64 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 49 6e 74 65 72 6e 65 74 2d 49 44 20 45 72 72 6f 72 43 6f 64 65 20 3c 3e 20 30 3c 2f 74 64 3e 0d 3c 74 64 3e 45 72 72 6f 72 20 63 6f 64 65 3a 20 31 3c 2f 74 64 3e 0d 3c 2f 74 72 3e 0d 0d	{0F9C7EC8-832B-4625-8979-940AACFF75D3} --><tr class="record"><td style="border: none;" class="e_l_2"> </td><td>06.02.2024---12:28:27:258</td><td>96</td><td> </td><td>Internet-ID ErrorCode <> 0</td><td>Error code: 1</td></tr>	success or wait	1	39B645	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	4084	248	3c 21 2d 2d 20 7b 46 36 36 43 33 36 31 35 2d 34 36 44 30 2d 34 32 39 33 2d 38 37 32 45 2d 39 44 43 32 37 30 33 35 43 46 42 41 7d 20 2d 2d 3e 0d 3c 74 72 20 63 6c 61 73 73 3d 22 72 65 63 6f 72 64 22 3e 3c 74 64 20 73 74 79 6c 65 3d 22 62 6f 72 64 65 72 3a 20 6e 6f 6e 65 3b 22 20 63 6c 61 73 73 3d 22 65 5f 6c 5f 32 22 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 30 36 2e 30 32 2e 32 30 32 34 2d 2d 2d 31 38 3a 34 30 3a 32 37 3a 39 39 36 3c 2f 74 64 3e 0d 3c 74 64 3e 39 36 3c 2f 74 64 3e 0d 3c 74 64 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 49 6e 74 65 72 6e 65 74 2d 49 44 20 45 72 72 6f 72 43 6f 64 65 20 3c 3e 20 30 3c 2f 74 64 3e 0d 3c 74 64 3e 45 72 72 6f 72 20 63 6f 64 65 3a 20 31 3c 2f 74 64 3e 0d 3c 2f 74 72 3e 0d 0d	{F66C3615-46D0-4293-872E-9DC27035CFBA} --><tr class="record"><td style="border: none;" class="e_l_2"> </td><td>06.02.2024---18:40:27:996</td><td>96</td><td> </td><td>Internet-ID ErrorCode <> 0</td><td>Error code: 1</td></tr>	success or wait	1	39B645	WriteFile
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	4600	248	3c 21 2d 2d 20 7b 46 41 36 31 39 36 44 43 2d 31 46 46 39 2d 34 46 46 43 2d 39 35 46 42 2d 42 34 35 46 45 35 41 31 34 31 45 42 7d 20 2d 2d 3e 0d 3c 74 72 20 63 6c 61 73 73 3d 22 72 65 63 6f 72 64 22 3e 3c 74 64 20 73 74 79 6c 65 3d 22 62 6f 72 64 65 72 3a 20 6e 6f 6e 65 3b 22 20 63 6c 61 73 73 3d 22 65 5f 6c 5f 32 22 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 30 36 2e 30 32 2e 32 30 32 34 2d 2d 2d 32 31 3a 35 35 3a 30 34 3a 33 38 33 3c 2f 74 64 3e 0d 3c 74 64 3e 39 36 3c 2f 74 64 3e 0d 3c 74 64 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 49 6e 74 65 72 6e 65 74 2d 49 44 20 45 72 72 6f 72 43 6f 64 65 20 3c 3e 20 30 3c 2f 74 64 3e 0d 3c 74 64 3e 45 72 72 6f 72 20 63 6f 64 65 3a 20 31 3c 2f 74 64 3e 0d 3c 2f 74 72 3e 0d 0d	{FA6196DC-1FF9-4FFC-95FB-B45FE5A141EB} --><tr class="record"><td style="border: none;" class="e_l_2"> </td><td>06.02.2024---21:55:04:383</td><td>96</td><td> </td><td>Internet-ID ErrorCode <> 0</td><td>Error code: 1</td></tr>	success or wait	1	39B645	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Remote Utilities\Logs\rut_log_2024-02.html	5116	248	3c 21 2d 2d 20 7b 42 31 32 41 34 36 43 41 2d 37 39 43 44 2d 34 45 34 46 2d 41 37 33 43 2d 46 36 42 46 33 37 38 44 38 44 46 44 7d 20 2d 2d 3e 0d 3c 74 72 20 63 6c 61 73 73 3d 22 72 65 63 6f 72 64 22 3e 3c 74 64 20 73 74 79 6c 65 3d 22 62 6f 72 64 65 72 3a 20 6e 6f 6e 65 3b 22 20 63 6c 61 73 73 3d 22 65 5f 6c 5f 32 22 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 30 37 2e 30 32 2e 32 30 32 34 2d 2d 2d 30 32 3a 31 33 3a 31 31 3a 34 34 31 3c 2f 74 64 3e 0d 3c 74 64 3e 39 36 3c 2f 74 64 3e 0d 3c 74 64 3e 26 6e 62 73 70 3b 3c 2f 74 64 3e 0d 3c 74 64 3e 49 6e 74 65 72 6e 65 74 2d 49 44 20 45 72 72 6f 72 43 6f 64 65 20 3c 3e 20 30 3c 2f 74 64 3e 0d 3c 74 64 3e 45 72 72 6f 72 20 63 6f 64 65 3a 20 31 3c 2f 74 64 3e 0d 3c 2f 74 72 3e 0d 0d	{B12A46CA-79CD-4E4F-A73C-F6BF378D8DFD} --><tr class="record"><td style="border: none;" class="e_l_2"> </td><td>07.02.2024---02:13:11:441</td><td>96</td><td> </td><td>Internet-ID ErrorCode <> 0</td><td>Error code: 1</td></tr>	success or wait	1	39B645	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	0	144	pipe empty	827	3F0E57	ReadFile
C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe	0	21148984	success or wait	1	39B619	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	5	AF1899	ReadFile
\pipe\RManFUSServerNotify32	0	1048576	access violation	1	AF1440	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	1	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	1	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	3	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	4	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	1	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	3	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	2	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	1	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	1	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	1	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	1	AF1899	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	1	AF1899	ReadFile
\pipe	0	144	success or wait	68	3F0E57	ReadFile
\pipe\RManFUSCallbackNotify32	0	4	success or wait	1	AF1899	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris	success or wait	1	7E45C7	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host	success or wait	1	7E45C7	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host	success or wait	1	7E45C7	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	success or wait	1	7E45C7	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	notification	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			46 2D 38 22 3F 3E 0D 0A 3C 72 6D 73 5F 69 6E 65 74 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 73 65 74 74 69 6E 67 73 5F 61 70 70 6C 69 65 64 3E 66 61 6C 73 65 3C 2F 73 65 74 74 69 6E 67 73 5F 61 70 70 6C 69 65 64 3E 3C 75 73 65 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 75 73 65 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 69 64 3E 74 72 75 65 3C 2F 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 69 64 3E 3C 73 65 6E 64 5F 74 6F 5F 65 6D 61 69 6C 3E 66 61 6C 73 65 3C 2F 73 65 6E 64 5F 74 6F 5F 65 6D 61 69 6C 3E 3C 69 64 3E 7B 42 31 37 34 32 43 32 32 2D 36 35 45 41 2D 34 36 35 33 2D 39 43 34 38 2D 43 36 43 42 39 33 42 38 31 31 46 32 7D 3C 2F 69 64 3E 3C 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 70 61 73 73 77 6F 72 64 3E 66 61 6C 73 65 3C 2F 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 70 61 73 73 77 6F 72 64 3E 3C 61 73 6B 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 66 61 6C 73 65 3C 2F 61 73 6B 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 65 6E 74 3E 66 61 6C 73 65 3C 2F 73 65 6E 74 3E 3C 76 65 72 73 69 6F 6E 3E 37 30 32 32 30 3C 2F 76 65 72 73 69 6F 6E 3E 3C 70 75 62 6C 69 63 5F 6B 65 79 5F 6D 3E 3C 2F 70 75 62 6C 69 63 5F 6B 65 79 5F 6D 3E 3C 70 75 62 6C 69 63 5F 6B 65 79 5F 65 3E 3C 2F 70 75 62 6C 69 63 5F 6B 65 79 5F 65 3E 3C 70 61 73 73 77 6F 72 64 3E 3C 2F 70 61 73 73 77 6F 72 64 3E 3C 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 2F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 64 69 73 63 6C 61 69 6D 65 72 3E 3C 2F 64 69 73 63 6C 61 69 6D 65 72 3E 3C 6F 76 65 72 77 72 69 74 65 5F 69 64 5F 63 6F 64 65 3E 66 61 6C 73 65 3C 2F 6F 76 65 72 77 72 69 74 65 5F 69 64 5F 63 6F 64 65 3E 3C 6F 76 65 72 77 72 69 74 65 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 66 61 6C 73 65 3C 2F 6F 76 65 72 77 72 69 74 65 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 3E 66 61 6C 73 65 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 61 64 64 72 65 73 73 3E 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 61 64 64 72 65 73 73 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 6F 72 74 3E 35 36 35 35 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 6F 72 74 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 69 70 76 36 3E 66 61 6C 73 65 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 69 70 76 36 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 5F 70 69 6E 3E 66 61 6C 73 65 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 5F 70 69 6E 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 69 6E 3E 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 69 6E 3E 3C 63 6F 6D 70 75 74 65 5F 6E 61 6D 65 3E 3C 2F 63 6F 6D 70 75 74 65 5F 6E 61 6D 65 3E 3C 73 65 6C 66 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 3C 2F 73 65 6C 66 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 65 6E 64 5F 74 6F 5F 73 65 74 74 69 6E 67 73 3E 3C 68 6F 73 74 3E 3C 2F 68 6F 73 74 3E 3C 70 6F 72 74 3E 35 38 37 3C 2F 70 6F 72 74 3E 3C 75 73 65 72 6E 61 6D 65 3E 3C 2F 75 73 65 72 6E 61 6D 65 3E 3C 70 61 73 73 77 6F 72 64 3E 3C 2F 70 61 73 73 77 6F 72 64 3E 3C 66				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			73 6F 6D 5F 65 6D 61 69 6C 3E 3C 2F 66 72 6F 6D 5F 65 6D 61 69 6C 3E 3C 75 73 65 5F 74 6C 73 3E 74 72 75 65 3C 2F 75 73 65 5F 74 6C 73 3E 3C 65 6D 61 69 6C 3E 3C 2F 65 6D 61 69 6C 3E 3C 73 75 62 6A 65 63 74 3E 3C 2F 73 75 62 6A 65 63 74 3E 3C 74 65 78 74 3E 3C 2F 74 65 78 74 3E 3C 2F 73 6D 74 70 5F 73 65 74 74 69 6E 67 73 3E 3C 2F 72 6D 73 5F 69 6E 65 74 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 0D 0A				
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	Security	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 73 65 63 75 72 69 74 79 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 77 69 6E 64 6F 77 73 5F 73 65 63 75 72 69 74 79 3E 3C 2F 77 69 6E 64 6F 77 73 5F 73 65 63 75 72 69 74 79 3E 3C 73 69 6E 67 6C 65 5F 70 61 73 73 77 6F 72 64 5F 68 61 73 68 3E 37 45 34 43 43 42 33 39 30 36 32 46 38 46 44 35 32 45 44 30 41 35 30 34 38 39 34 37 36 46 33 31 41 35 42 33 31 31 36 37 42 30 35 39 46 37 31 45 42 36 39 37 38 36 41 31 46 41 39 44 30 33 31 45 46 46 33 30 42 45 31 32 31 35 46 46 34 34 38 37 33 36 36 46 41 36 33 44 36 42 33 43 42 39 34 36 37 43 35 38 42 32 41 46 45 31 36 44 32 38 44 33 46 35 34 33 46 39 46 43 37 41 35 38 32 37 37 44 3C 2F 73 69 6E 67 6C 65 5F 70 61 73 73 77 6F 72 64 5F 68 61 73 68 3E 3C 6D 79 5F 75 73 65 72 5F 61 63 63 65 73 73 5F 6C 69 73 74 3E 3C 75 73 65 72 5F 61 63 63 65 73 73 5F 6C 69 73 74 2F 3E 3C 2F 6D 79 5F 75 73 65 72 5F 61 63 63 65 73 73 5F 6C 69 73 74 3E 3C 69 70 5F 66 69 6C 74 65 72 5F 74 79 70 65 3E 32 3C 2F 69 70 5F 66 69 6C 74 65 72 5F 74 79 70 65 3E 3C 69 70 5F 62 6C 61 63 6B 5F 6C 69 73 74 3E 3C 2F 69 70 5F 62 6C 61 63 6B 5F 6C 69 73 74 3E 3C 69 70 5F 77 68 69 74 65 5F 6C 69 73 74 3E 3C 2F 69 70 5F 77 68 69 74 65 5F 6C 69 73 74 3E 3C 61 75 74 68 5F 6B 69 6E 64 3E 31 3C 2F 61 75 74 68 5F 6B 69 6E 64 3E 3C 6F 74 70 5F 65 6E 61 62 6C 65 3E 66 61 6C 73 65 3C 2F 6F 74 70 5F 65 6E 61 62 6C 65 3E 3C 6F 74 70 5F 70 72 69 76 61 74 65 5F 6B 65 79 3E 3C 2F 6F 74 70 5F 70 72 69 76 61 74 65 5F 6B 65 79 3E 3C 6F 74 70 5F 71 72 5F 73 65 63 72 65 74 3E 3C 2F 6F 74 70 5F 71 72 5F 73 65 63 72 65 74 3E 3C 75 73 65 72 5F 70 65 72 6D 69 73 73 69 6F 6E 5F 61 73 6B 3E 66 61 6C 73 65 3C 2F 75 73 65 72 5F 70 65 72 6D 69 73 73 69 6F 6E 5F 61 73 6B 3E 3C 75 73 65 72 5F 70 65 72 6D 69 73 73 69 6F 6E 5F 69 6E 74 65 72 76 61 6C 3E 31 30 30 30 30 3C 2F 75 73 65 72 5F 70 65 72 6D 69 73 73 69 6F 6E 5F 69 6E 74 65 72 76 61 6C 3E 3C 75 73 65 72 5F 70 65 72 6D 69 73 73 69 6F 6E 5F 61 6C 6C 6F 77 5F 64 65 66 61 75 6C 74 3E 66 61 6C 73 65 3C 2F 75 73 65 72 5F 70 65 72 6D 69 73 73 69 6F 6E 5F 61 6C 6C 6F 77 5F 64 65 66 61 75 6C 74 3E 3C 75 73 65 72 5F 70 65 72 6D 69 73 73 69 6F 6E 5F 6F 6E 6C 79 5F 69 66 5F 75 73 65 72 5F 6C 6F 67 67 65 64 5F 6F 6E 3E 66 61 6C 73 65 3C 2F 75 73 65 72 5F 70 65 72 6D 69 73 73 69 6F 6E 5F 6F 6E 6C 79 5F 69 66 5F 75 73 65 72 5F 6C 6F 67 67 65 64 5F 6F 6E 3E 3C 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 63 6F 6E 74 72 6F 6C 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 63 6F 6E 74 72 6F 6C 3E 3C 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 73 63 72 65 65 6E 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 73 63 72 65 65 6E 3E 3C 64 69 73 61 62 6C	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			65 5F 66 69 6C 65 5F 74 72 61 6E 73 66 65 72 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 66 69 6C 65 5F 74 72 61 6E 73 66 65 72 3E 3C 64 69 73 61 62 6C 65 5F 72 65 64 69 72 65 63 74 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 72 65 64 69 72 65 63 74 3E 3C 64 69 73 61 62 6C 65 5F 74 65 6C 6E 65 74 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 74 65 6C 6E 65 74 3E 3C 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 65 78 65 63 75 74 65 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 65 78 65 63 75 74 65 3E 3C 64 69 73 61 62 6C 65 5F 74 61 73 6B 5F 6D 61 6E 61 67 65 72 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 74 61 73 6B 5F 6D 61 6E 61 67 65 72 3E 3C 64 69 73 61 62 6C 65 5F 73 68 75 74 64 6F 77 6E 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 73 68 75 74 64 6F 77 6E 3E 3C 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 75 70 67 72 61 64 65 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 75 70 67 72 61 64 65 3E 3C 64 69 73 61 62 6C 65 5F 70 72 65 76 69 65 77 5F 63 61 70 74 75 72 65 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 70 72 65 76 69 65 77 5F 63 61 70 74 75 72 65 3E 3C 64 69 73 61 62 6C 65 5F 64 65 76 69 63 65 5F 6D 61 6E 61 67 65 72 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 64 65 76 69 63 65 5F 6D 61 6E 61 67 65 72 3E 3C 64 69 73 61 62 6C 65 5F 63 68 61 74 3E 74 72 75 65 3C 2F 64 69 73 61 62 6C 65 5F 63 68 61 74 3E 3C 64 69 73 61 62 6C 65 5F 73 63 72 65 65 6E 5F 72 65 63 6F 72 64 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 73 63 72 65 65 6E 5F 72 65 63 6F 72 64 3E 3C 64 69 73 61 62 6C 65 5F 61 76 5F 63 61 70 74 75 72 65 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 61 76 5F 63 61 70 74 75 72 65 3E 3C 64 69 73 61 62 6C 65 5F 73 65 6E 64 5F 6D 65 73 73 61 67 65 3E 74 72 75 65 3C 2F 64 69 73 61 62 6C 65 5F 73 65 6E 64 5F 6D 65 73 73 61 67 65 3E 3C 64 69 73 61 62 6C 65 5F 72 65 67 69 73 74 72 79 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 72 65 67 69 73 74 72 79 3E 3C 64 69 73 61 62 6C 65 5F 61 76 5F 63 68 61 74 3E 74 72 75 65 3C 2F 64 69 73 61 62 6C 65 5F 61 76 5F 63 68 61 74 3E 3C 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 73 65 74 74 69 6E 67 73 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 73 65 74 74 69 6E 67 73 3E 3C 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 70 72 69 6E 74 69 6E 67 3E 74 72 75 65 3C 2F 64 69 73 61 62 6C 65 5F 72 65 6D 6F 74 65 5F 70 72 69 6E 74 69 6E 67 3E 3C 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 6C 69 73 74 3E 37 37 75 2F 50 44 39 34 62 57 77 67 64 6D 56 79 63 32 6C 76 62 6A 30 69 4D 53 34 77 49 69 42 6C 62 6D 4E 76 5A 47 6C 75 5A 7A 30 69 56 56 52 47 4C 54 67 69 50 7A 34 4E 43 6A 78 7A 5A 58 4A 32 5A 58 4A 66 59 32 39 75 62 6D 56 6A 64 46 39 6A 62 32 35 30 5A 58 68 30 49 48 5A 6C 63 6E 4E 70 62 32 34 39 49 6A 63 77 4D 6A 49 77 49 6A 34 38 63 6D 31 7A 58 33 4E 6C 63 6E 5A 6C 63 6E 4D 76 50 6A 77 76 63 32 56 79 64 6D 56 79 58 32 4E 76 62 6D 35 6C 59 33 52 66 59 32 39 75 64 47 56 34 64 44 34 4E 43 67 3D 3D 3C 2F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 6C 69 73 74 3E 3C 73 65 6C 65 63 74 65 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 69 64 3E 3C 2F 73 65 6C				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			65 63 74 65 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 69 64 3E 3C 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 61 63 63 65 73 73 3E 37 37 75 2F 50 44 39 34 62 57 77 67 64 6D 56 79 63 32 6C 76 62 6A 30 69 4D 53 34 77 49 69 42 6C 62 6D 4E 76 5A 47 6C 75 5A 7A 30 69 56 56 52 47 4C 54 67 69 50 7A 34 4E 43 6A 78 79 62 58 4E 66 59 57 4E 73 49 48 5A 6C 63 6E 4E 70 62 32 34 39 49 6A 63 77 4D 6A 49 77 49 6A 34 38 63 6D 31 7A 58 32 46 6A 5A 58 4D 76 50 6A 78 6C 62 6D 46 69 62 47 56 66 61 57 35 6F 5A 58 4A 70 64 44 35 30 63 6E 56 6C 50 43 39 6C 62 6D 46 69 62 47 56 66 61 57 35 6F 5A 58 4A 70 64 44 34 38 4C 33 4A 74 63 31 39 68 59 32 77 2B 44 51 6F 3D 3C 2F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 61 63 63 65 73 73 3E 3C 2F 73 65 63 75 72 69 74 79 5F 73 65 74 74 69 6E 67 73 3E 0D 0A				
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	General	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 70 6F 72 74 3E 35 36 35 30 3C 2F 70 6F 72 74 3E 3C 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 74 72 75 65 3C 2F 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 3C 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 74 72 75 65 3C 2F 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 3C 6C 61 6E 67 75 61 67 65 3E 4B 6F 72 65 61 6E 3C 2F 6C 61 6E 67 75 61 67 65 3E 3C 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 74 72 75 65 3C 2F 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 3C 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 3C 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 37 65 69 36 75 6A 77 78 39 4B 41 3D 3C 2F 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 3C 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 3C 70 72 6F 74 65 63 74 5F 69 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 69 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 3C 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 66 61 6C 73 65 3C 2F 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 3C 75 73 65 5F 69 70 5F 76 5F 36 3E 74 72 75 65 3C 2F 75 73 65 5F 69 70 5F 76 5F 36 3E 3C 6C 6F 67 5F 75 73 65 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 3E 3C 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 3C 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 2F 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 2F 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 73 69 64 5F 69 64 3E 3C 2F 73 69 64 5F 69 64 3E 3C 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 3C 6E 6F 74 69 66	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 74 72 75 65 3C 2F 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 3C 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 3C 6E 6F 74 69 66 79 5F 70 6C 61 79 5F 73 6F 75 6E 64 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 70 6C 61 79 5F 73 6F 75 6E 64 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 3C 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 37 37 75 2F 50 44 39 34 62 57 77 67 64 6D 56 79 63 32 6C 76 62 6A 30 69 4D 53 34 77 49 69 42 6C 62 6D 4E 76 5A 47 6C 75 5A 7A 30 69 56 56 52 47 4C 54 67 69 50 7A 34 4E 43 6A 78 77 63 6D 39 34 65 56 39 7A 5A 58 52 30 61 57 35 6E 63 79 42 32 5A 58 4A 7A 61 57 39 75 50 53 49 33 4D 44 49 79 4D 43 49 2B 50 48 56 7A 5A 56 39 77 63 6D 39 34 65 54 35 6D 59 57 78 7A 5A 54 77 76 64 58 4E 6C 58 33 42 79 62 33 68 35 50 6A 78 77 63 6D 39 34 65 56 39 30 65 58 42 6C 50 6A 41 38 4C 33 42 79 62 33 68 35 58 33 52 35 63 47 55 2B 50 47 68 76 63 33 51 2B 50 43 39 6F 62 33 4E 30 50 6A 78 77 62 33 4A 30 50 6A 67 77 4F 44 41 38 4C 33 42 76 63 6E 51 2B 50 47 35 6C 5A 57 52 66 59 58 56 30 61 44 35 6D 59 57 78 7A 5A 54 77 76 62 6D 56 6C 5A 46 39 68 64 58 52 6F 50 6A 78 75 64 47 31 73 58 32 46 31 64 47 67 2B 5A 6D 46 73 63 32 55 38 4C 32 35 30 62 57 78 66 59 58 56 30 61 44 34 38 64 58 4E 6C 63 6D 35 68 62 57 55 2B 50 43 39 31 63 32 56 79 62 6D 46 74 5A 54 34 38 63 47 46 7A 63 33 64 76 63 6D 51 2B 50 43 39 77 59 58 4E 7A 64 32 39 79 5A 44 34 38 5A 47 39 74 59 57 6C 75 50 6A 77 76 5A 47 39 74 59 57 6C 75 50 6A 77 76 63 48 4A 76 65 48 6C 66 63 32 56 30 64 47 6C 75 5A 33 4D 2B 44 51 6F 3D 3C 2F 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 3C 61 64 64 69 74 69 6F 6E 61 6C 3E 37 64 32 37 6A 77 67 78 77 61 54 5A 33 59 36 50 50 44 48 30 70 41 3D 3D 3C 2F 61 64 64 69 74 69 6F 6E 61 6C 3E 3C 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 66 61 6C 73 65 3C 2F 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 3C 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 74 72 75 65 3C 2F 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 3C 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 30 3C 2F 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F							

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			6F 5F 69 64 6C 65 3E 66 61 6C 73 65 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 3C 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 3C 2F 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 3E 0D 0A				
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	CallbackSettings	binary	FF FE 5B 00 7B 00 32 00 33 00 35 00 32 00 45 00 33 00 30 00 33 00 2D 00 30 00 37 00 37 00 31 00 2D 00 34 00 42 00 41 00 45 00 2D 00 39 00 45 00 31 00 46 00 2D 00 30 00 46 00 34 00 44 00 31 00 42 00 30 00 37 00 31 00 39 00 46 00 38 00 7D 00 5D 00 0D 00 0A 00 69 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 5F 00 69 00 64 00 3D 00 2D 00 2D 00 0D 00 0A 00 68 00 6F 00 73 00 74 00 3D 00 31 00 30 00 31 00 2E 00 39 00 39 00 2E 00 39 00 34 00 2E 00 35 00 34 00 0D 00 0A 00 70 00 6F 00 72 00 74 00 3D 00 35 00 36 00 35 00 31 00 0D 00 0A 00 74 00 65 00 78 00 74 00 5F 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 3D 00 20 00 0D 00 0A 00 61 00 75 00 74 00 6F 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 31 00 0D 00 0A 00 73 00 74 00 61 00 74 00 75 00 73 00 3D 00 32 00 0D 00 0A 00 64 00 69 00 73 00 70 00 6C 00 61 00 79 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 31 00 30 00 31 00 2E 00 39 00 39 00 2E 00 39 00 34 00 2E 00 35 00 34 00 0D 00 0A 00 64 00 69 00 73 00 61 00 6C 00 6C 00 6F 00 77 00 5F 00 74 00 72 00 61 00 79 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 30 00 0D 00 0A 00 61 00 70 00 70 00 65 00 6E 00 64 00 5F 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 31 00 0D 00 0A 00 0D 00 0A 00 5B 00 7B 00 31 00 43 00 43 00 30 00 35 00 32 00 43 00 35 00 2D 00 30 00 30 00 35 00 45 00 2D 00 34 00 43 00 36 00 30 00 2D 00 39 00 37 00 38 00 32 00 2D 00 33 00 31 00 42 00 42 00 46 00 41 00 31 00 32 00 30 00 33 00 42 00 36 00 7D 00 5D 00 0D 00 0A 00 69 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 5F 00 69 00 64 00 3D 00 2D 00 2D 00 0D 00 0A 00 68 00 6F 00 73 00 74 00 3D 00 31 00 30 00 31 00 2E 00 39 00 39 00 2E 00 39 00 34 00 2E 00 35 00 34 00 0D 00 0A 00 70 00 6F 00 72 00 74 00 3D 00 34 00 36 00 35 00 0D 00 0A 00 74 00 65 00 78 00 74 00 5F 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 3D 00 20 00 0D 00 0A 00 61 00 75 00 74 00 6F 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 31 00 0D 00 0A 00 73 00 74 00 61 00 74 00 75 00 73 00 3D 00 32 00 0D 00 0A 00 64 00 69 00 73 00 70 00 6C 00 61 00 79 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 31 00 30 00 31 00 2E 00 39 00 39 00 2E 00 39 00 34 00 2E 00 35 00 34 00 0D 00 0A 00 64 00 69 00 73 00 61 00 6C 00 6C 00 6F 00 77 00 5F 00 74 00 72 00 61 00 79 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 30 00 0D 00 0A 00 61 00 70 00 70 00 65 00 6E 00 64 00 5F 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 31 00 0D 00 0A 00 0D 00 0A 00 5B 00 7B 00 44 00 39 00 30 00 43 00	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			30 00 30 00 45 00 34 00 2D 00 35 00 30 00 44 00 35 00 2D 00 34 00 37 00 42 00 34 00 2D 00 42 00 46 00 43 00 37 00 2D 00 46 00 38 00 37 00 31 00 31 00 39 00 30 00 45 00 32 00 33 00 38 00 38 00 7D 00 5D 00 0D 00 0A 00 69 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 5F 00 69 00 64 00 3D 00 2D 00 2D 00 0D 00 0A 00 68 00 6F 00 73 00 74 00 3D 00 31 00 30 00 31 00 2E 00 39 00 39 00 2E 00 39 00 34 00 2E 00 35 00 34 00 0D 00 0A 00 70 00 6F 00 72 00 74 00 3D 00 38 00 30 00 0D 00 0A 00 74 00 65 00 78 00 74 00 5F 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 3D 00 20 00 0D 00 0A 00 61 00 75 00 74 00 6F 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 31 00 0D 00 0A 00 73 00 74 00 61 00 74 00 75 00 73 00 3D 00 32 00 0D 00 0A 00 64 00 69 00 73 00 70 00 6C 00 61 00 79 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 31 00 30 00 31 00 2E 00 39 00 39 00 2E 00 39 00 34 00 2E 00 35 00 34 00 0D 00 0A 00 64 00 69 00 73 00 61 00 6C 00 6C 00 6F 00 77 00 5F 00 74 00 72 00 61 00 79 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 30 00 0D 00 0A 00 61 00 70 00 70 00 65 00 6E 00 64 00 5F 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 31 00 0D 00 0A 00 0D 00 0A 00 5B 00 7B 00 31 00 31 00 38 00 32 00 37 00 32 00 41 00 35 00 2D 00 38 00 33 00 42 00 41 00 2D 00 34 00 41 00 32 00 31 00 2D 00 38 00 33 00 37 00 30 00 2D 00 41 00 35 00 42 00 42 00 32 00 36 00 43 00 33 00 38 00 43 00 32 00 41 00 7D 00 5D 00 0D 00 0A 00 69 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 5F 00 69 00 64 00 3D 00 2D 00 2D 00 0D 00 0A 00 68 00 6F 00 73 00 74 00 3D 00 31 00 38 00 35 00 2E 00 37 00 30 00 2E 00 31 00 30 00 34 00 2E 00 39 00 30 00 0D 00 0A 00 70 00 6F 00 72 00 74 00 3D 00 35 00 36 00 35 00 31 00 0D 00 0A 00 74 00 65 00 78 00 74 00 5F 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 3D 00 20 00 0D 00 0A 00 61 00 75 00 74 00 6F 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 31 00 0D 00 0A 00 73 00 74 00 61 00 74 00 75 00 73 00 3D 00 32 00 0D 00 0A 00 64 00 69 00 73 00 70 00 6C 00 61 00 79 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 31 00 38 00 35 00 2E 00 37 00 30 00 2E 00 31 00 30 00 34 00 2E 00 39 00 30 00 0D 00 0A 00 64 00 69 00 73 00 61 00 6C 00 6C 00 6F 00 77 00 5F 00 74 00 72 00 61 00 79 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 30 00 0D 00 0A 00 61 00 70 00 70 00 65 00 6E 00 64 00 5F 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 31 00 0D 00 0A 00 0D 00 0A 00 5B 00 7B 00 46 00 46 00 31 00 42 00 32 00 42 00 33 00 36 00 2D 00 46 00 42 00 41 00 32 00 2D 00 34 00 39 00 31 00 35 00 2D 00 39 00 31 00 34 00 37 00 2D 00 39 00 31 00 41 00 43 00 33 00 42 00 43 00 38 00 34 00 39 00 39 00 41 00 7D 00 5D 00 0D 00 0A 00 69 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 5F 00 69 00 64 00 3D 00 2D 00 2D 00 0D 00 0A 00 68 00 6F 00 73 00 74 00 3D 00 37 00 37 00 2E 00 31 00 30 00 35 00 2E 00 31 00 33 00 32 00 2E 00 37 00 30 00 0D 00 0A 00 70 00 6F 00 72 00 74 00 3D 00 35 00 36 00 35 00 31 00 0D 00 0A 00 74 00 65 00 78 00 74 00 5F 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 3D 00 20 00				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			0D 00 0A 00 61 00 75 00 74 00 6F 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 31 00 0D 00 0A 00 73 00 74 00 61 00 74 00 75 00 73 00 3D 00 32 00 0D 00 0A 00 64 00 69 00 73 00 70 00 6C 00 61 00 79 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 37 00 37 00 2E 00 31 00 30 00 35 00 2E 00 31 00 33 00 32 00 2E 00 37 00 30 00 0D 00 0A 00 64 00 69 00 73 00 61 00 6C 00 6C 00 6F 00 77 00 5F 00 74 00 72 00 61 00 79 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 30 00 0D 00 0A 00 61 00 70 00 70 00 65 00 6E 00 64 00 5F 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 31 00 0D 00 0A 00 0D 00 0A 00 5B 00 7B 00 33 00 36 00 35 00 38 00 41 00 38 00 45 00 34 00 2D 00 31 00 42 00 44 00 31 00 2D 00 34 00 35 00 32 00 30 00 2D 00 41 00 46 00 35 00 45 00 2D 00 46 00 38 00 41 00 31 00 38 00 44 00 35 00 41 00 42 00 35 00 37 00 38 00 7D 00 5D 00 0D 00 0A 00 69 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 5F 00 69 00 64 00 3D 00 2D 00 2D 00 0D 00 0A 00 68 00 6F 00 73 00 74 00 3D 00 37 00 37 00 2E 00 31 00 30 00 35 00 2E 00 31 00 33 00 32 00 2E 00 37 00 30 00 0D 00 0A 00 70 00 6F 00 72 00 74 00 3D 00 38 00 30 00 0D 00 0A 00 74 00 65 00 78 00 74 00 5F 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 3D 00 20 00 0D 00 0A 00 61 00 75 00 74 00 6F 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 31 00 0D 00 0A 00 73 00 74 00 61 00 74 00 75 00 73 00 3D 00 32 00 0D 00 0A 00 64 00 69 00 73 00 70 00 6C 00 61 00 79 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 37 00 37 00 2E 00 31 00 30 00 35 00 2E 00 31 00 33 00 32 00 2E 00 37 00 30 00 0D 00 0A 00 64 00 69 00 73 00 61 00 6C 00 6C 00 6F 00 77 00 5F 00 74 00 72 00 61 00 79 00 5F 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 3D 00 30 00 0D 00 0A 00 61 00 70 00 70 00 65 00 6E 00 64 00 5F 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 5F 00 6E 00 61 00 6D 00 65 00 3D 00 31 00 0D 00 0A 00 0D 00 0A 00				
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	FUSClientPath	unicode	C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	InternetId	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 72 6D 73 5F 69 6E 74 65 72 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 2F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 75 73 65 5F 69 6E 65 74 5F 63 6F 6E 6E 65 63 74 69 6F 6E 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 69 6E 65 74 5F 63 6F 6E 6E 65 63 74 69 6F 6E 3E 3C 69 6E 65 74 5F 73 65 72 76 65 72 3E 3C 2F 69 6E 65 74 5F 73 65 72 76 65 72 3E 3C 75 73 65 5F 63 75 73 74 6F 6D 5F 69 6E 65 74 5F 73 65 72 76 65 72 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 63 75 73 74 6F 6D 5F 69 6E 65 74 5F 73 65 72 76 65 72 3E 3C 69 6E 65 74 5F 69 64 5F 70 6F 72 74 3E 35 36 35 35 3C 2F 69 6E 65 74 5F 69 64 5F 70 6F 72 74 3E 3C 75 73 65 5F 69 6E 65 74 5F 69 64 5F 69 70 76 36 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 69 6E 65 74 5F 69 64 5F 69 70 76 36 3E 3C 69 6E 65 74 5F 69 64 5F 75 73 65 5F 70 69 6E 3E 66 61 6C 73 65 3C 2F 69 6E 65 74 5F 69 64 5F 75 73 65 5F 70 69 6E 3E 3C 69 6E 65 74 5F 69 64 5F 70 69 6E 3E 3C 2F 69 6E 65 74 5F 69 64 5F 70 69 6E 3E 3C 2F 72 6D 73 5F 69 6E 74 65 72 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 0D 0A	success or wait	1	4DD51F	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	Certificates	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 63 65 72 74 69 66 69 63 74 65 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 63 65 72 74 69 66 69 63 61 74 65 3E 3C 2F 63 65 72 74 69 66 69 63 61 74 65 3E 3C 70 72 69 76 61 74 65 5F 6B 65 79 3E 3C 2F 70 72 69 76 61 74 65 5F 6B 65 79 3E 3C 2F 63 65 72 74 69 66 69 63 74 65 5F 73 65 74 74 69 6E 67 73 3E 0D 0A	success or wait	1	4DD51F	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	CalendarRecordSettings	binary	FF FE 3C 00 3F 00 78 00 6D 00 6C 00 20 00 76 00 65 00 72 00 73 00 69 00 6F 00 6E 00 3D 00 22 00 31 00 2E 00 30 00 22 00 20 00 65 00 6E 00 63 00 6F 00 64 00 69 00 6E 00 67 00 3D 00 22 00 55 00 54 00 46 00 2D 00 31 00 36 00 22 00 3F 00 3E 00 0D 00 0A 00 3C 00 73 00 72 00 65 00 65 00 6E 00 5F 00 72 00 65 00 63 00 6F 00 72 00 64 00 5F 00 6F 00 70 00 74 00 69 00 6F 00 6E 00 20 00 76 00 65 00 72 00 73 00 69 00 6F 00 6E 00 3D 00 22 00 37 00 30 00 32 00 32 00 30 00 22 00 3E 00 3C 00 6D 00 61 00 69 00 6E 00 5F 00 6F 00 70 00 74 00 69 00 6F 00 6E 00 73 00 3E 00 3C 00 61 00 63 00 74 00 69 00 76 00 65 00 3E 00 66 00 61 00 6C 00 73 00 65 00 3C 00 2F 00 61 00 63 00 74 00 69 00 76 00 65 00 3E 00 3C 00 69 00 6E 00 74 00 65 00 72 00 76 00 61 00 6C 00 5F 00 73 00 68 00 6F 00 74 00 3E 00 36 00 30 00 3C 00 2F 00 69 00 6E 00 74 00 65 00 72 00 76 00 61 00 6C 00 5F 00 73 00 68 00 6F 00 74 00 3E 00 3C 00 70 00 72 00 6F 00 74 00 65 00 63 00 74 00 5F 00 72 00 65 00 63 00 6F 00 72 00 64 00 3E 00 66 00 61 00 6C 00 73 00 65 00 3C 00 2F 00 70 00 72 00 6F 00 74 00 65 00 63 00 74 00 5F 00 72 00 65 00 63 00 6F 00 72 00 64 00 3E 00 3C 00 63 00 6F 00 6D 00 70 00 72 00 65 00 73 00 73 00 69 00 6F 00 6E 00 5F 00 71 00 75 00 61 00 6C 00 69 00 74 00 79 00 3E 00 39 00 30 00 3C 00 2F 00 63 00 6F 00 6D 00 70 00 72 00 65 00 73 00 73 00 69 00 6F 00 6E 00 5F 00 71 00 75 00 61 00 6C 00 69	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 74 00 79 00 3E 00 3C 00 73 00 63 00 61 00 6C 00 65 00 5F 00 71 00 75 00 61 00 6C 00 69 00 74 00 79 00 3E 00 31 00 30 00 30 00 3C 00 2F 00 73 00 63 00 61 00 6C 00 65 00 5F 00 71 00 75 00 61 00 6C 00 69 00 74 00 79 00 3E 00 3C 00 63 00 6F 00 6D 00 70 00 72 00 65 00 73 00 73 00 69 00 6F 00 6E 00 5F 00 74 00 79 00 70 00 65 00 3E 00 30 00 3C 00 2F 00 63 00 6F 00 6D 00 70 00 72 00 65 00 73 00 73 00 69 00 6F 00 6E 00 5F 00 74 00 79 00 70 00 65 00 3E 00 3C 00 6D 00 61 00 78 00 5F 00 66 00 69 00 6C 00 65 00 5F 00 73 00 69 00 7A 00 65 00 3E 00 31 00 30 00 30 00 3C 00 2F 00 6D 00 61 00 78 00 5F 00 66 00 69 00 6C 00 65 00 5F 00 73 00 69 00 7A 00 65 00 3E 00 3C 00 61 00 75 00 74 00 6F 00 5F 00 63 00 6C 00 65 00 61 00 72 00 3E 00 66 00 61 00 6C 00 73 00 65 00 3C 00 2F 00 61 00 75 00 74 00 6F 00 5F 00 63 00 6C 00 65 00 61 00 72 00 3E 00 3C 00 61 00 75 00 74 00 6F 00 5F 00 63 00 6C 00 65 00 61 00 72 00 5F 00 64 00 61 00 79 00 73 00 3E 00 30 00 3C 00 2F 00 61 00 75 00 74 00 6F 00 5F 00 63 00 6C 00 65 00 61 00 72 00 5F 00 64 00 61 00 79 00 73 00 3E 00 3C 00 75 00 73 00 65 00 64 00 5F 00 66 00 69 00 6C 00 65 00 5F 00 6C 00 69 00 6D 00 69 00 74 00 3E 00 74 00 72 00 75 00 65 00 3C 00 2F 00 75 00 73 00 65 00 64 00 5F 00 66 00 69 00 6C 00 65 00 5F 00 6C 00 69 00 6D 00 69 00 74 00 3E 00 3C 00 61 00 6C 00 6C 00 5F 00 66 00 69 00 6C 00 65 00 73 00 5F 00 6C 00 69 00 6D 00 69 00 74 00 5F 00 6D 00 62 00 3E 00 31 00 30 00 30 00 30 00 3C 00 2F 00 61 00 6C 00 6C 00 5F 00 66 00 69 00 6C 00 65 00 73 00 5F 00 6C 00 69 00 6D 00 69 00 74 00 5F 00 6D 00 62 00 3E 00 3C 00 64 00 72 00 61 00 77 00 5F 00 64 00 61 00 74 00 61 00 74 00 69 00 6D 00 65 00 5F 00 6F 00 6E 00 5F 00 69 00 6D 00 61 00 67 00 65 00 3E 00 74 00 72 00 75 00 65 00 3C 00 2F 00 64 00 72 00 61 00 77 00 5F 00 64 00 61 00 74 00 61 00 74 00 69 00 6D 00 65 00 5F 00 6F 00 6E 00 5F 00 69 00 6D 00 61 00 67 00 65 00 3E 00 3C 00 63 00 75 00 73 00 74 00 6F 00 6D 00 5F 00 72 00 65 00 6D 00 6F 00 74 00 65 00 5F 00 64 00 69 00 72 00 65 00 63 00 74 00 6F 00 72 00 79 00 3E 00 3C 00 2F 00 63 00 75 00 73 00 74 00 6F 00 6D 00 5F 00 72 00 65 00 6D 00 6F 00 74 00 65 00 5F 00 64 00 69 00 72 00 65 00 63 00 74 00 6F 00 72 00 79 00 3E 00 3C 00 6D 00 61 00 69 00 6E 00 5F 00 6F 00 70 00 74 00 69 00 6F 00 6E 00 73 00 3E 00 3C 00 73 00 63 00 68 00 65 00 64 00 75 00 6C 00 65 00 3C 00 2F 00 73 00 72 00 65 00 65 00 6E 00 5F 00 72 00 65 00 63 00 6F 00 72 00 64 00 5F 00 6F 00 70 00 74 00 69 00 6F 00 6E 00 3E 00 0D 00 0A 00				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	General	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 70 6F 72 74 3E 35 36 35 30 3C 2F 70 6F 72 74 3E 3C 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 70 6F 72 74 3E 35 36 35 30 3C 2F 70 6F 72 74 3E 3C 68 69 64 65 5F 74 72 61 79	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			75 3E 74 72 75 65 3C 2F 63 6B 6E 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 3C 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 74 72 75 65 3C 2F 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 3C 6C 61 6E 67 75 61 67 65 3E 4B 6F 72 65 61 6E 3C 2F 6C 61 6E 67 75 61 67 65 3E 3C 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 74 72 75 65 3C 2F 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 3C 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 3C 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 37 65 69 36 75 6A 77 78 39 4B 41 3D 3C 2F 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 3C 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 3C 70 72 6F 74 65 63 74 5F 69 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 69 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 3C 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 66 61 6C 73 65 3C 2F 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 3C 75 73 65 5F 69 70 5F 76 5F 36 3E 74 72 75 65 3C 2F 75 73 65 5F 69 70 5F 76 5F 36 3E 3C 6C 6F 67 5F 75 73 65 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 3E 3C 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 3C 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 2F 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 2F 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 73 69 64 5F 69 64 3E 3C 2F 73 69 64 5F 69 64 3E 3C 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 3C 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 74 72	5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 74 72 75 65 3C 2F 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 3C 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 74 72 75 65 3C 2F 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 3C 6C 61 6E 67 75 61 67 65 3E 4B 6F 72 65 61 6E 3C 2F 6C 61 6E 67 75 61 67 65 3E 3C 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 74 72 75 65 3C 2F 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 3C 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 3C 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 37 65 69 36 75 6A 77 78 39 4B 41 3D 3C 2F 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 3C 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 3C 70 72 6F 74 65 63 74 5F 69 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 69 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 3C 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 66 61 6C 73 65 3C 2F 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 3C 75 73 65 5F 69 70 5F 76 5F 36 3E 74 72 75 65 3C 2F 75 73 65 5F 69 70 5F 76 5F 36 3E 3C 6C 6F 67 5F 75 73 65 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 3E 3C 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 3C 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 2F 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			75 65 3C 2F 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 3C 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 3C 6E 6F 74 69 66 79 5F 70 6C 61 79 5F 73 6F 75 6E 64 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 70 6C 61 79 5F 73 6F 75 6E 64 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 3C 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 37 37 75 2F 50 44 39 34 62 57 77 67 64 6D 56 79 63 32 6C 76 62 6A 30 69 4D 53 34 77 49 69 42 6C 62 6D 4E 76 5A 47 6C 75 5A 7A 30 69 56 56 52 47 4C 54 67 69 50 7A 34 4E 43 6A 78 77 63 6D 39 34 65 56 39 7A 5A 58 52 30 61 57 35 6E 63 79 42 32 5A 58 4A 7A 61 57 39 75 50 53 49 33 4D 44 49 79 4D 43 49 2B 50 48 56 7A 5A 56 39 77 63 6D 39 34 65 54 35 6D 59 57 78 7A 5A 54 77 76 64 58 4E 6C 58 33 42 79 62 33 68 35 50 6A 78 77 63 6D 39 34 65 56 39 30 65 58 42 6C 50 6A 41 38 4C 33 42 79 62 33 68 35 58 33 52 35 63 47 55 2B 50 47 68 76 63 33 51 2B 50 43 39 6F 62 33 4E 30 50 6A 78 77 62 33 4A 30 50 6A 67 77 4F 44 41 38 4C 33 42 76 63 6E 51 2B 50 47 35 6C 5A 57 52 66 59 58 56 30 61 44 35 6D 59 57 78 7A 5A 54 77 76 62 6D 56 6C 5A 46 39 68 64 58 52 6F 50 6A 78 75 64 47 31 73 58 32 46 31 64 47 67 2B 5A 6D 46 73 63 32 55 38 4C 32 35 30 62 57 78 66 59 58 56 30 61 44 34 38 64 58 4E 6C 63 6D 35 68 62 57 55 2B 50 43 39 31 63 32 56 79 62 6D 46 74 5A 54 34 38 63 47 46 7A 63 33 64 76 63 6D 51 2B 50 43 39 77 59 58 4E 7A 64 32 39 79 5A 44 34 38 5A 47 39 74 59 57 6C 75 50 6A 77 76 5A 47 39 74 59 57 6C 75 50 6A 77 76 63 48 4A 76 65 48 6C 66 63 32 56 30 64 47 6C 75 5A 33 4D 2B 44 51 6F 3D 3C 2F 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 3C 61 64 64 69 74 69 6F 6E 61 6C 3E 37 64 32 37 6A 77 67 78 77 61 54 5A 33 59 36 50 50 44 48 30 70 41 3D 3D 3C 2F 61 64 64 69 74 69 6F 6E 61 6C 3E 3C 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 73 61 66 65 5F 6D 6F 64 65	3C 2F 61 75 74 68 5F 65 6E 73 5F 73 74 72 69 6E 67 3E 3C 73 69 64 5F 69 64 3E 34 35 33 32 34 2E 34 30 31 30 31 33 37 30 33 37 3C 2F 73 69 64 5F 69 64 3E 3C 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 3C 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 74 72 75 65 3C 2F 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 3C 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 3C 6E 6F 74 69 66 79 5F 70 6C 61 79 5F 73 6F 75 6E 64 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 70 6C 61 79 5F 73 6F 75 6E 64 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 3C 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 37 37 75 2F 50 44 39 34 62 57 77 67 64 6D 56 79 63 32 6C 76 62 6A 30 69 4D 53 34 77 49 69 42 6C 62 6D 4E 76 5A 47 6C 75 5A 7A 30 69 56 56 52 47 4C 54 67 69 50 7A 34 4E 43 6A 78 77 63 6D 39 34 65 56 39 7A 5A 58 52 30 61 57 35 6E 63 79 42 32 5A 58 4A 7A 61 57 39 75 50 53 49 33 4D 44 49 79 4D 43 49 2B 50 48 56 7A 5A 56 39 77 63 6D 39 34 65 54 35 6D 59 57 78 7A 5A 54 77 76 64 58 4E 6C 58 33 42 79 62 33 68 35 50 6A 78 77 63 6D 39 34 65 56 39 30 65 58 42 6C 50 6A 41 38 4C 33 42 79 62 33 68 35 58 33 52 35 63 47 55 2B 50 47 68 76 63 33 51 2B 50 43 39 6F 62 33 4E 30 50 6A 78 77 62 33 4A 30 50 6A 67 77 4F 44 41 38 4C 33 42 76 63 6E 51 2B 50 47 35 6C 5A 57 52 66 59 58 56 30 61 44 35 6D 59 57 78 7A 5A 54 77 76 62 6D 56 6C 5A 46 39 68 64 58 52 6F 50 6A 78 75 64 47 31 73 58 32 46 31 64 47 67 2B 5A 6D 46 73 63 32 55 38 4C 32 35 30 62 57 78 66 59 58 56 30 61 44 34 38 64 58 4E 6C 63 6D 35 68 62 57 55 2B 50 43 39 31				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			5F 73 65 74 3E 66 61 6C 73 65 3C 2F 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 3C 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 74 72 75 65 3C 2F 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 3C 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 30 3C 2F 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 66 61 6C 73 65 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 3C 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 3C 2F 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 3E 0D 0A	63 32 56 79 62 6D 46 [illegible] 34 38 63 47 46 7A 63 33 64 76 63 6D 51 2B 50 43 39 77 59 58 4E 7A 64 32 39 79 5A 44 34 38 5A 47 39 74 59 57 6C 75 50 6A 77 76 5A 47 39 74 59 57 6C 75 50 6A 77 76 63 48 4A 76 65 48 6C 66 63 32 56 30 64 47 6C 75 5A 33 4D 2B 44 51 6F 3D 3C 2F 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 3C 61 64 64 69 74 69 6F 6E 61 6C 3E 37 64 32 37 6A 77 67 78 77 61 54 5A 33 59 36 50 50 44 48 30 70 41 3D 3D 3C 2F 61 64 64 69 74 69 6F 6E 61 6C 3E 3C 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 66 61 6C 73 65 3C 2F 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 3C 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 74 72 75 65 3C 2F 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 3C 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 30 3C 2F 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 66 61 6C 73 65 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 6C 6F 73 65 5F 73 65 73				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				73 69 6F 6E 5F 69 64 65 63 3F 69 6E 74 65 72 76 61 6C 3E 3C 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 3C 2F 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 3E 0D 0A				
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	General	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 70 6F 72 74 3E 35 36 35 30 3C 2F 70 6F 72 74 3E 3C 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 74 72 75 65 3C 2F 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 3C 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 74 72 75 65 3C 2F 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 3C 6C 61 6E 67 75 61 67 65 3E 4B 6F 72 65 61 6E 3C 2F 6C 61 6E 67 75 61 67 65 3E 3C 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 74 72 75 65 3C 2F 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 3C 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 3C 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 37 65 69 36 75 6A 77 78 39 4B 41 3D 3C 2F 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 3C 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 3C 70 72 6F 74 65 63 74 5F 69 6E 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 69 6E 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 3C 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 66 61 6C 73 65 3C 2F 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 3C 75 73 65 5F 69 70 5F 76 5F 36 3E 74	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 70 6F 72 74 3E 35 36 35 30 3C 2F 70 6F 72 74 3E 3C 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 74 72 75 65 3C 2F 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 3C 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 74 72 75 65 3C 2F 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 3C 6C 61 6E 67 75 61 67 65 3E 4B 6F 72 65 61 6E 3C 2F 6C 61 6E 67 75 61 67 65 3E 3C 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 74 72 75 65 3C 2F 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 3C 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 3C 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 37 65 69 36 75 6A 77 78 39 4B 41 3D 3C 2F 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 3C 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 3C 70 72 6F 74 65 63 74 5F 69 6E 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 69 6E 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 3C 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 66 61 6C 73 65 3C 2F 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 3C 75 73 65 5F 69 70 5F 76 5F 36 3E 74	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			72 75 65 3C 2F 75 73 65 3C 6D 73 5F 76 5F 36 3E 3C 6C 6F 67 5F 75 73 65 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 3E 3C 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 3C 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 2F 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 2F 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 73 69 64 5F 69 64 3E 34 35 33 32 34 2E 34 30 31 30 31 33 37 30 33 37 3C 2F 73 69 64 5F 69 64 3E 3C 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 3C 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 74 72 75 65 3C 2F 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 3C 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 3C 6E 6F 74 69 66 79 5F 70 6C 61 79 5F 73 6F 75 6E 64 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 70 6C 61 79 5F 73 6F 75 6E 64 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 3C 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 37 37 75 2F 50 44 39 34 62 57 77 67 64 6D 56 79 63 32 6C 76 62 6A 30 69 4D 53 34 77 49 69 42 6C 62 6D 4E 76 5A 47 6C 75 5A 7A 30 69 56 56 52 47 4C 54 67 69 50 7A 34 4E 43 6A 78 77 63 6D 39 34 65 56 39 7A 5A 58 52 30 61 57 35 6E 63 79 42 32 5A 58 4A 7A 61 57 39 75 50 53 49 33 4D 44 49 79 4D 43 49 2B 50 48 56 7A 5A 56 39 77 63 6D 39 34 65 54 35 6D 59 57 78 7A 5A 54 77 76 64 58 4E 6C 58 33 42 79 62 33 68 35 50 6A 78 77 63 6D 39 34 65 56 39 30 65 58 42 6C 50 6A 41 38 4C 33 42 79 62 33 68 35 58 33 52 35 63 47 55 2B 50 47 68 76 63 33 51 2B 50 43 39 6F 62 33 4E 30 50 6A 78 77 62 33 4A 30 50 6A 67 77 4F 44 41 38 4C 33 42 76 63 6E 51 2B 50 47 35 6C 5A 57 52 66 59 58 56 30 61 44 35 6D 59 57 78 7A 5A 54 77 76 62 6D 56 6C 5A 46 39 68 64 58 52 6F 50 6A 78 75 64 47 31 73 58 32 46 31	5F 6C 65 67 61 63 79 5F 70 61 6E 65 6C 5F 79 3E 3C 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 66 61 6C 73 65 3C 2F 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 3C 75 73 65 5F 69 70 5F 76 5F 36 3E 74 72 75 65 3C 2F 75 73 65 5F 69 70 5F 76 5F 36 3E 3C 6C 6F 67 5F 75 73 65 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 3E 3C 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 3C 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 2F 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 2F 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 73 69 64 5F 69 64 3E 34 35 33 32 34 2E 34 30 31 30 31 33 37 30 33 37 3C 2F 73 69 64 5F 69 64 3E 3C 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 3C 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 74 72 75 65 3C 2F 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 3C 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 3C 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 37 37 75 2F 50 44 39 34 62 57 77 67 64 6D 56 79 63 32 6C 76 62 6A 30 69 4D 53 34 77 49 69 42 6C 62 6D 4E 76 5A 47 6C 75 5A 7A 30 69 56 56 52 47 4C 54 67 69 50 7A 34 4E 43 6A 78 77 63 6D 39 34 65 56 39 7A 5A 58 52 30 61 57 35 6E 63 79 42 32 5A 58 4A 7A 61 57 39 75 50 53 49 33 4D 44				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			64 47 67 2B 5A 6D 46 73 63 32 55 38 4C 32 35 30 62 57 78 66 59 58 56 30 61 44 34 38 64 58 4E 6C 63 6D 35 68 62 57 55 2B 50 43 39 31 63 32 56 79 62 6D 46 74 5A 54 34 38 63 47 46 7A 63 33 64 76 63 6D 51 2B 50 43 39 77 59 58 4E 7A 64 32 39 79 5A 44 34 38 5A 47 39 74 59 57 6C 75 50 6A 77 76 5A 47 39 74 59 57 6C 75 50 6A 77 76 63 48 4A 76 65 48 6C 66 63 32 56 30 64 47 6C 75 5A 33 4D 2B 44 51 6F 3D 3C 2F 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 3C 61 64 64 69 74 69 6F 6E 61 6C 3E 37 64 32 37 6A 77 67 78 77 61 54 5A 33 59 36 50 50 44 48 30 70 41 3D 3D 3C 2F 61 64 64 69 74 69 6F 6E 61 6C 3E 3C 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 66 61 6C 73 65 3C 2F 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 3C 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 74 72 75 65 3C 2F 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 3C 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 30 3C 2F 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 66 61 6C 73 65 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 3C 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65	49 79 4D 43 49 2B 50 46 56 7A 5A 56 39 77 63 6D 39 34 65 54 35 6D 59 57 78 7A 5A 54 77 76 64 58 4E 6C 58 33 42 79 62 33 68 35 50 6A 78 77 63 6D 39 34 65 56 39 30 65 58 42 6C 50 6A 41 38 4C 33 42 79 62 33 68 35 58 33 52 35 63 47 55 2B 50 47 68 76 63 33 51 2B 50 43 39 6F 62 33 4E 30 50 6A 78 77 62 33 4A 30 50 6A 67 77 4F 44 41 38 4C 33 42 76 63 6E 51 2B 50 47 35 6C 5A 57 52 66 59 58 56 30 61 44 35 6D 59 57 78 7A 5A 54 77 76 62 6D 56 6C 5A 46 39 68 64 58 52 6F 50 6A 78 75 64 47 31 73 58 32 46 31 64 47 67 2B 5A 6D 46 73 63 32 55 38 4C 32 35 30 62 57 78 66 59 58 56 30 61 44 34 38 64 58 4E 6C 63 6D 35 68 62 57 55 2B 50 43 39 31 63 32 56 79 62 6D 46 74 5A 54 34 38 63 47 46 7A 63 33 64 76 63 6D 51 2B 50 43 39 77 59 58 4E 7A 64 32 39 79 5A 44 34 38 5A 47 39 74 59 57 6C 75 50 6A 77 76 5A 47 39 74 59 57 6C 75 50 6A 77 76 63 48 4A 76 65 48 6C 66 63 32 56 30 64 47 6C 75 5A 33 4D 2B 44 51 6F 3D 3C 2F 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 3C 61 64 64 69 74 69 6F 6E 61 6C 3E 3C 2F 61 64 64 69 74 69 6F 6E 61 6C 3E 3C 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 66 61 6C 73 65 3C 2F 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 3C 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			72 74 5F 66 6F 72 5F 61 6C 6C 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 3C 2F 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 3E 0D 0A	74 5F 73 74 61 72 74 75 70 3E 74 72 75 65 3C 2F 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 3C 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 30 3C 2F 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 66 61 6C 73 65 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 3C 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 3C 2F 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 3E 0D 0A				
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	Certificates	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 63 65 72 74 69 66 69 63 74 65 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 63 65 72 74 69 66 69 63 61 74 65 3E 3C 2F 63 65 72 74 69 66 69 63 61 74 65 3E 3C 70 72 69 76 61 74 65 5F 6B 65 79 3E 3C 2F 70 72 69 76 61 74 65 5F 6B 65 79 3E 3C 2F 63 65 72 74 69 66 69 63 74 65 5F 73 65 74 74 69 6E 67 73 3E 0D 0A	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 63 65 72 74 69 66 69 63 74 65 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 63 65 72 74 69 66 69 63 61 74 65 3E 4C 53 30 74 4C 53 31 43 52 55 64 4A 54 69 42 44 52 56 4A 55 53 55 5A 4A 51 30 46 55 52 53 30 74 4C 53 30 74 43 6B 31 4A 53 55 52 42 61 6B 4E 44 51 57 56 78 5A 30 46 33 53 55 4A 42 5A 30 6C 46 56 7A 6C 33 61 45 39 45 51 55 35 43 5A 32 74 78 61 47 74 70 52 7A 6C 33 4D 45 4A 42 55 58 4E 47 51 55 52 43 52 45 31 52 63 33 64 44 55 56 6C 45 56 6C 46 52 52 30 56 33 53 6C 59 4B 56 58 70 46 57 6B 31 43 59 30 64 42 4D 56 56 46 51 32 64 33 55 56 56 74 56 6E 52 69 4D 31 4A 73 53 55 5A 57 4D 47 46 58 65 48 42 6B 52 32 78 73 59 33 70 46 57 6B 31 43 59 30 64 42 4D 56 56 46 51 58 64 33 55 56 56 74 56 6E 52 69 4D 31 4A 73 53 55 5A 57 4D 41 70 68 56 33 68 77 5A 45 64 73 62 47 4E 36 51 57 56 47 64 7A 42 35 54 6B 52 42 65 55 31 45 53 58	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				64 50 52 45 30 30 54 56 6D 55 59 55 5A 33 4D 48 70 4F 52 45 46 34 54 58 70 42 64 30 39 45 54 54 52 4E 56 47 68 68 54 55 56 4E 65 45 4E 36 51 55 70 43 5A 30 35 57 43 6B 4A 42 57 56 52 42 62 46 5A 55 54 56 4A 72 64 30 5A 33 57 55 52 57 55 56 46 4C 52 45 4A 43 55 31 70 58 4D 58 5A 6B 52 31 56 6E 56 6C 68 53 63 47 4A 48 62 44 42 68 56 31 5A 36 54 56 4A 72 64 30 5A 33 57 55 52 57 55 56 46 45 52 45 4A 43 55 31 70 58 4D 58 59 4B 5A 45 64 56 5A 31 5A 59 55 6E 42 69 52 32 77 77 59 56 64 57 65 6B 31 4A 53 55 4A 4A 61 6B 46 4F 51 6D 64 72 63 57 68 72 61 55 63 35 64 7A 42 43 51 56 46 46 52 6B 46 42 54 30 4E 42 55 54 68 42 54 55 6C 4A 51 6B 4E 6E 53 30 4E 42 55 55 56 42 63 7A 46 6E 4D 67 70 77 55 55 52 51 53 6E 70 70 56 57 56 57 56 32 6B 72 54 6B 4D 7A 52 6A 46 6A 5A 54 6C 78 62 55 4A 53 57 54 4A 5A 54 48 52 56 63 58 4A 78 62 6E 4E 70 54 55 64 4D 51 6C 49 79 56 32 31 50 5A 30 55 72 53 6C 5A 46 61 31 4A 56 4E 58 42 4D 51 53 39 42 64 58 56 31 43 6D 46 48 52 32 4E 69 55 47 6F 34 61 48 52 49 4D 31 59 72 57 44 52 6A 4C 7A 52 6F 59 6E 5A 68 54 6A 63 32 57 6D 46 42 63 56 64 71 65 55 52 52 55 45 4A 34 4E 54 68 32 59 6E 56 47 61 6A 52 55 59 7A 52 54 56 30 68 73 55 6A 4A 70 61 30 39 75 53 58 64 33 56 30 34 4B 5A 55 5A 70 54 32 74 7A 56 31 46 43 4D 33 6B 34 55 6E 4A 51 56 6B 56 55 54 30 4A 73 52 31 5A 33 53 31 42 72 51 55 4D 79 57 6D 6F 79 65 56 4A 4A 52 33 5A 4E 63 47 67 7A 55 31 55 34 63 33 59 35 63 55 49 7A 62 56 51 30 64 46 68 56 51 56 5A 4F 51 7A 46 31 54 51 70 6A 55 7A 52 57 64 57 34 32 54 79 39 36 53 45 52 54 64 57 64 69 5A 45 35 34 61 7A 6C 35 63 57 6B 33 62 32 5A 73 56 6C 46 43 55 6C 6B 32 64 7A 68 44 4F 55 5A 7A 61 56 56 68 53 48 4A 79 64 6B 70 4C 59 6C 68 57 5A 47 70 72 4C 30 30 33 64 55 70 70 56 6B 39 43 43 6B 78 74 61 56 5A 58 61 43 39 61 61 6B 39 75 5A 30 46 52 4B 7A 41 7A 53 57 56 4C 51 6B 68 7A 64 46 4E 68 51 57 78 61 63 6A 4E 48 4D 54 4A 73 51 57 56 4D 53 44 67 30 57 6A 59 77 4D 57 59				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				76 4F 44 64 42 63 7A 5A 30 35 57 74 6D 64 32 56 54 55 6D 64 36 56 33 63 4B 57 56 5A 6B 5A 32 67 32 61 6A 63 78 57 54 6C 57 5A 6E 56 69 54 6D 4A 52 53 55 52 42 55 55 46 43 54 55 45 77 52 30 4E 54 63 55 64 54 53 57 49 7A 52 46 46 46 51 6B 4E 33 56 55 46 42 4E 45 6C 43 51 56 46 44 52 6B 38 7A 59 31 56 51 5A 56 63 31 61 31 5A 58 54 41 70 4E 63 30 46 69 4D 6D 6C 36 4D 45 6B 77 54 6D 6C 36 59 56 56 61 65 55 4A 77 5A 46 52 6B 61 6A 6C 4B 4E 31 6B 35 53 33 4A 4B 62 48 52 71 53 31 41 7A 63 46 49 7A 4E 55 64 59 56 33 68 49 53 6E 4D 31 61 54 6C 34 4E 57 67 34 4E 56 70 4E 52 6B 31 45 4B 33 68 79 43 6B 68 70 53 55 52 36 56 46 4A 4C 53 54 5A 68 4D 56 4E 4B 5A 32 5A 31 51 6D 35 56 52 6D 68 4D 63 46 56 36 61 56 42 77 59 6D 70 69 4E 31 68 55 5A 46 46 44 4D 46 51 33 62 6C 68 48 63 32 64 33 65 43 39 61 62 48 46 35 4E 31 5A 4C 64 45 55 31 65 6E 42 61 4D 46 4D 4B 57 6D 6B 33 4F 45 64 6E 4B 30 5A 6F 4F 55 49 30 59 31 4D 79 4F 45 5A 34 64 46 6C 35 52 47 51 78 4C 32 31 70 5A 56 70 73 56 43 38 72 4E 55 64 47 64 48 52 4C 53 56 52 52 61 7A 5A 4B 53 6B 38 78 4C 30 78 33 54 46 46 78 54 30 49 79 56 48 5A 50 53 6C 64 4A 55 77 70 30 63 30 4E 42 64 44 5A 6B 4C 33 4D 72 57 44 56 78 5A 31 52 47 55 6B 6B 77 55 44 64 5A 52 6B 4A 6C 4F 46 52 77 52 6E 68 34 61 30 5A 49 61 6A 56 6C 51 33 64 6C 64 6E 55 34 64 6B 70 34 52 7A 67 79 55 46 56 54 62 53 74 59 4F 48 5A 57 4D 31 42 6A 62 30 6B 31 43 6E 5A 6F 51 55 49 78 4D 6C 4E 32 56 30 5A 4B 51 55 78 75 57 55 35 4D 61 6C 70 43 65 46 5A 55 51 31 68 78 64 54 46 35 4E 55 52 73 4E 54 6C 75 59 32 5A 61 53 30 68 33 64 54 4A 32 51 6C 63 31 4E 55 74 4F 62 6D 52 7A 4F 44 4E 4B 5A 48 56 76 4E 46 4E 54 56 45 77 4B 55 57 74 33 51 54 42 74 61 57 67 4B 4C 53 30 74 4C 53 31 46 54 6B 51 67 51 30 56 53 56 45 6C 47 53 55 4E 42 56 45 55 74 4C 53 30 74 4C 51 6F 3D 3C 2F 63 65 72 74 69 66 69 63 61 74 65 3E 3C 70 72 69 76 61 74 65 5F 6B 65 79 3E 4C 53 30 74 4C 53 31 43 52 55				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				64 4A 54 69 42 51 55 52 46 51 56 52 46 49 45 74 46 57 53 30 74 4C 53 30 74 43 6B 31 4A 53 55 56 32 64 30 6C 43 51 55 52 42 54 6B 4A 6E 61 33 46 6F 61 32 6C 48 4F 58 63 77 51 6B 46 52 52 55 5A 42 51 56 4E 44 51 6B 74 72 64 32 64 6E 55 32 78 42 5A 30 56 42 51 57 39 4A 51 6B 46 52 51 33 70 58 52 47 46 73 51 55 30 34 62 6B 39 4B 55 6A 55 4B 56 6D 46 4D 4E 44 42 4D 59 31 68 57 65 44 63 79 63 56 6C 47 52 6D 70 61 5A 33 55 78 55 33 46 31 63 57 56 35 53 58 64 5A 63 30 5A 49 57 6D 46 5A 4E 6B 46 55 4E 47 78 56 55 31 4A 47 56 47 31 72 63 30 51 34 51 7A 59 32 4E 57 39 5A 57 6E 68 7A 4B 31 42 35 52 77 6F 77 5A 6D 52 59 4E 57 5A 6F 65 69 39 70 52 6E 55 35 62 7A 4E 32 63 47 78 76 51 33 42 68 55 45 6C 4F 51 54 68 49 53 47 35 35 4F 58 55 30 56 31 42 6F 54 6E 70 6F 53 6C 6C 6C 56 6B 68 68 53 31 45 32 59 32 70 45 51 6C 6B 78 4E 46 64 4A 4E 6C 4E 34 57 6B 46 49 43 6D 5A 4D 65 45 64 7A 4F 56 56 53 54 54 52 48 56 56 70 59 51 57 38 72 55 55 46 4D 57 6D 31 51 59 6B 70 46 5A 32 45 34 65 57 31 49 5A 45 70 55 65 58 6B 76 4D 6D 39 49 5A 56 70 51 61 54 46 6B 55 55 4A 56 4D 45 78 58 4E 48 68 34 54 47 68 58 4E 6D 5A 76 4E 79 38 4B 54 57 4E 4F 53 7A 5A 43 64 44 41 7A 52 31 51 7A 53 33 46 4D 64 57 67 72 56 6C 5A 42 52 6B 5A 71 63 6B 52 33 54 44 42 58 65 55 70 53 62 32 56 31 64 54 68 72 63 48 52 6B 56 6A 4A 50 56 44 68 36 64 54 52 74 53 6C 55 30 52 58 56 68 53 6C 5A 68 53 44 6C 74 54 51 6F 32 5A 55 46 43 52 44 64 55 59 32 67 30 62 30 56 6C 65 54 46 4B 62 30 4E 57 62 58 5A 6A 59 6C 68 68 56 55 49 30 63 32 5A 36 61 47 35 79 56 46 59 76 4C 33 70 7A 51 33 70 78 4D 55 4E 53 4C 30 49 31 53 6B 64 45 54 6D 4A 43 61 46 59 79 51 30 68 78 55 48 5A 57 43 6D 6F 78 56 69 73 31 63 7A 46 30 51 57 64 4E 51 6B 46 42 52 55 4E 6E 5A 30 56 42 52 48 64 4C 53 30 4E 46 54 6B 74 46 65 55 5A 46 53 53 74 6C 54 44 64 56 52 57 6C 76 59 6E 68 36 4E 57 5A 6A 53 48 6F 33 5A 48 4A 45 61 6D 68 6D 51 33 6C 47 52 47 34 32 63 44 63 4B 53 6C 4E	Completion			

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				47 4D 54 42 71 55 6C 45 76 6F 6B 56 59 4C 31 46 44 52 33 63 30 59 6C 46 79 4D 45 52 72 57 6E 55 30 54 57 52 75 4E 57 4E 51 52 47 68 72 5A 55 4E 49 55 30 74 75 63 31 4A 6B 4D 46 56 43 56 32 68 61 56 6B 6C 45 56 31 64 33 53 6B 68 44 4D 55 52 70 65 67 6F 76 5A 6D 74 7A 4D 44 4E 6A 64 55 39 57 56 7A 4E 34 52 44 52 75 64 47 5A 4E 63 6B 51 77 4F 58 56 78 53 33 70 5A 64 57 56 59 4E 55 4E 51 5A 47 6C 73 63 46 4A 46 5A 44 6B 77 56 58 4E 72 55 46 42 4A 52 54 59 72 64 48 70 58 53 6D 73 76 55 7A 42 68 52 46 52 6D 43 6E 52 6D 4E 57 68 4A 63 44 5A 6E 65 6E 68 6A 5A 30 51 7A 63 30 31 44 56 32 35 4D 54 6A 42 57 5A 53 39 76 63 6B 55 35 5A 6A 52 79 61 32 31 61 65 58 4E 76 54 55 56 71 4E 45 35 49 65 58 41 34 54 48 4E 46 55 47 78 4C 56 47 34 77 59 33 64 50 54 6D 52 51 4E 55 77 4B 5A 56 64 54 62 58 68 69 54 33 49 30 56 55 4A 73 5A 55 70 4A 54 31 5A 32 61 6E 56 59 59 6D 56 35 56 6D 52 4E 64 6D 39 7A 52 31 4E 33 54 33 5A 54 53 47 74 6B 53 30 31 51 64 45 74 69 57 47 64 35 57 44 6C 4B 5A 6E 56 33 64 48 4D 76 61 6C 56 71 56 47 39 6F 52 67 70 45 55 30 56 4C 64 47 70 54 4D 32 6B 77 61 30 4E 69 55 32 38 78 4B 32 35 30 4E 31 6C 70 57 47 70 56 56 6A 4E 79 62 32 67 78 55 79 39 58 63 45 73 32 4F 45 56 48 51 56 46 4C 51 6D 64 52 52 48 4A 51 63 57 63 35 61 46 59 79 56 6E 5A 50 4D 32 5A 35 4E 48 4A 4E 43 6A 46 4A 62 30 52 49 54 79 39 6B 5A 30 52 7A 63 32 35 56 54 55 4A 31 4E 44 51 7A 4C 30 74 56 4E 30 49 72 52 32 4E 79 63 6E 42 51 51 57 31 7A 51 57 35 49 5A 44 4A 43 64 48 51 78 65 58 70 36 63 32 74 75 52 58 6B 34 64 55 46 6F 54 47 4E 43 61 56 70 72 52 33 51 4B 56 32 6C 33 62 54 5A 6F 51 7A 56 4B 4E 6C 4A 47 59 30 31 6C 56 30 6C 42 57 55 31 4D 4F 47 56 77 57 6A 5A 4A 4B 31 55 33 52 45 6F 72 54 7A 5A 34 62 7A 64 78 4E 57 5A 76 4F 46 59 35 59 30 59 77 62 79 74 31 59 6B 78 74 52 45 46 4E 65 57 64 6C 53 55 46 4A 57 51 70 6D 57 45 63 30 54 57 45 30 51 53 74 55 63 56 70 58 5A 57 56 46 61 55 6B 79 65				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				56 52 43 4D 47 63 33 56 6D 74 43 5A 31 46 45 52 45 74 32 61 46 70 45 4E 6B 5A 50 56 48 5A 76 59 32 68 47 54 47 73 32 59 55 31 6C 54 57 6C 73 4F 55 31 54 4E 54 67 76 51 58 4A 4E 43 6D 74 76 4C 30 46 48 51 7A 56 4C 57 6C 45 78 4E 7A 52 73 4B 30 4D 7A 52 54 6C 79 61 6C 67 34 4D 54 6C 4D 51 6B 56 78 59 33 4A 44 53 31 4E 52 52 47 52 6A 5A 31 4E 31 62 6D 4A 4C 4E 58 56 79 53 6B 63 72 63 55 5A 6B 54 6C 56 61 52 58 42 71 64 57 64 6F 61 45 30 4B 55 6C 4E 56 53 45 45 77 64 58 42 36 5A 6D 6C 34 55 58 5A 35 4D 56 68 59 53 6C 52 4C 61 57 4A 43 55 32 46 47 4E 30 39 57 63 79 73 79 62 46 45 30 4D 47 68 4D 4C 31 52 52 51 57 34 77 62 6D 4D 31 52 6B 34 30 59 6A 68 43 51 30 34 72 61 56 42 79 55 56 5A 43 53 41 70 75 55 57 77 79 5A 54 6C 57 54 32 64 52 53 30 4A 6E 55 55 52 6E 4D 30 51 72 54 58 4A 30 53 6B 70 7A 65 45 68 6B 5A 6C 67 7A 63 6C 5A 4C 4D 6D 35 57 51 6A 4A 71 63 55 5A 4D 62 6E 70 73 63 57 6C 68 56 6D 74 46 51 58 6C 6A 5A 46 4E 6C 5A 45 74 46 56 33 42 6A 43 6A 51 7A 4E 30 31 56 63 30 39 4F 64 57 5A 6F 52 57 35 46 55 6D 4E 45 57 54 64 50 62 55 6C 49 54 58 52 54 54 46 51 32 4F 55 74 55 62 46 56 49 62 54 52 4A 4D 6D 70 79 62 46 52 45 56 7A 51 30 63 6A 4E 6C 61 48 41 35 59 6B 68 33 53 69 39 4F 57 6D 6C 45 4D 31 45 4B 61 31 68 59 4D 33 4A 32 4D 58 42 48 59 56 4A 45 4E 56 64 73 53 6E 6C 51 57 55 6C 74 4D 47 63 7A 4E 7A 59 31 52 6C 42 58 64 45 52 61 57 56 56 34 4C 7A 5A 79 53 47 30 7A 54 6A 63 32 5A 32 59 7A 52 54 45 76 4B 30 31 6C 63 31 59 34 55 55 74 43 5A 31 46 44 4E 51 6F 76 4E 6D 56 36 59 56 4A 32 4D 33 59 7A 61 6B 6F 79 53 32 39 51 61 7A 42 4B 63 6E 4E 78 4E 6E 4A 78 4D 46 59 34 64 7A 67 72 5A 54 59 77 59 57 39 6A 5A 55 31 69 4E 7A 4E 68 54 56 52 46 4F 58 56 4D 57 48 68 69 53 32 5A 36 52 57 52 54 4C 31 46 4A 52 32 74 73 43 6A 56 5A 54 6A 49 34 54 47 49 72 59 32 74 77 62 31 56 50 4E 45 35 51 4F 57 56 6D 4D 30 70 78 51 31 52 4C 52 55 68 49 56 30 51 72 64 6E 67 33 63 33 4E 6E 4D 56 6C 43 55 44				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				52 33 53 56 6C 46 63 4F 49 32 5A 46 63 33 64 55 31 46 59 6E 46 49 51 6B 4E 42 59 56 67 4B 64 6D 64 6B 63 55 6F 7A 63 30 68 68 52 30 52 32 61 33 4A 7A 5A 7A 52 58 65 46 51 76 4F 56 46 75 52 33 55 35 52 57 4D 7A 61 55 6B 31 4D 31 70 32 55 48 52 46 63 45 46 52 53 30 4A 6E 55 55 4E 4F 61 46 5A 48 55 32 31 59 4C 32 6B 33 59 57 4A 4D 61 6B 46 45 59 51 6F 72 63 6E 46 34 64 32 70 4C 4D 48 56 51 4F 46 5A 69 5A 32 74 46 54 44 4D 77 4E 33 6C 57 63 6B 5A 31 64 6B 77 76 4E 56 4E 70 55 33 56 35 51 33 64 6E 53 44 6B 33 4E 33 70 4C 4D 45 31 61 53 33 6C 35 61 6C 5A 36 59 6D 5A 78 61 48 55 79 61 6C 63 76 62 57 67 35 43 6D 74 52 56 32 77 77 55 44 46 47 54 79 73 79 57 69 39 44 61 6B 31 57 63 32 78 55 59 30 74 47 4E 44 6C 47 55 30 6B 76 4F 58 6C 73 51 55 56 47 51 54 56 6B 4F 54 6C 45 52 57 78 4C 54 53 74 6E 54 57 73 31 61 32 6C 49 5A 56 56 70 4E 44 45 30 65 48 46 79 4F 57 59 4B 55 31 4E 61 62 6E 4D 30 57 45 31 4F 53 30 5A 35 57 56 5A 61 62 56 6C 34 4E 30 74 74 54 45 4A 50 52 45 45 39 50 51 6F 74 4C 53 30 74 4C 55 56 4F 52 43 42 51 55 6B 6C 57 51 56 52 46 49 45 74 46 57 53 30 74 4C 53 30 74 43 67 3D 3D 3C 2F 70 72 69 76 61 74 65 5F 6B 65 79 3E 3C 2F 63 65 72 74 69 66 69 63 74 65 5F 73 65 74 74 69 6E 67 73 3E 0D 0A			
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	notification	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 72 6D 73 5F 69 6E 65 74 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 73 65 74 74 69 6E 67 73 5F 61 70 70 6C 69 65 64 3E 66 61 6C 73 65 3C 2F 73 65 74 74 69 6E 67 73 5F 61 70 70 6C 69 65 64 3E 3C 75 73 65 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 75 73 65 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 69 64 3E 74 72 75 65 3C 2F 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 69 64 3E 3C 73 65 6E 64 5F 74 6F 5F 65 6D 61 69 6C 3E 66 61 6C 73 65 3C 2F 73 65 6E 64 5F 74 6F 5F 65 6D 61 69 6C 3E 3C 69 64 3E 7B 42 31 37 34 32 43 32 32 2D 36 35 45 41 2D 34 36 35 33 2D 39 43 34 38 2D 43	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 72 6D 73 5F 69 6E 65 74 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 73 65 74 74 69 6E 67 73 5F 61 70 70 6C 69 65 64 3E 74 72 75 65 3C 2F 73 65 74 74 69 6E 67 73 5F 61 70 70 6C 69 65 64 3E 3C 75 73 65 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 75 73 65 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 69 64 3E 74 72 75 65 3C 2F 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 69 64 3E 3C 73 65 6E 64 5F 74 6F 5F 65 6D 61 69 6C 3E 66 61 6C 73 65 3C 2F 73 65 6E 64 5F 74 6F 5F 65 6D 61	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			36 43 42 39 33 42 38 31 31 46 32 7D 3C 2F 69 64 3E 3C 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 70 61 73 73 77 6F 72 64 3E 66 61 6C 73 65 3C 2F 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 70 61 73 73 77 6F 72 64 3E 3C 61 73 6B 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 66 61 6C 73 65 3C 2F 61 73 6B 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 65 6E 74 3E 66 61 6C 73 65 3C 2F 73 65 6E 74 3E 3C 76 65 72 73 69 6F 6E 3E 37 30 32 32 30 3C 2F 76 65 72 73 69 6F 6E 3E 3C 70 75 62 6C 69 63 5F 6B 65 79 5F 6D 3E 3C 2F 70 75 62 6C 69 63 5F 6B 65 79 5F 6D 3E 3C 70 75 62 6C 69 63 5F 6B 65 79 5F 65 3E 3C 2F 70 75 62 6C 69 63 5F 6B 65 79 5F 65 3E 3C 70 61 73 73 77 6F 72 64 3E 3C 2F 70 61 73 73 77 6F 72 64 3E 3C 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 2F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 64 69 73 63 6C 61 69 6D 65 72 3E 3C 2F 64 69 73 63 6C 61 69 6D 65 72 3E 3C 6F 76 65 72 77 72 69 74 65 5F 69 64 5F 63 6F 64 65 3E 66 61 6C 73 65 3C 2F 6F 76 65 72 77 72 69 74 65 5F 69 64 5F 63 6F 64 65 3E 3C 6F 76 65 72 77 72 69 74 65 5F 69 64 3E 3C 64 69 73 63 6C 61 69 6D 65 72 3E 3C 2F 64 69 73 63 6C 61 69 6D 65 72 3E 3C 2F 6F 76 65 72 77 72 69 74 65 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 61 64 64 72 65 73 73 3E 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 6F 72 74 3E 35 36 35 35 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 6F 72 74 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 69 70 76 36 3E 66 61 6C 73 65 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 69 70 76 36 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 5F 70 69 6E 3E 66 61 6C 73 65 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 69 6E 3E 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 69 6E 3E 3C 63 6F 6D 70 75 74 65 72 5F 6E 61 6D 65 3E 3C 2F 63 6F 6D 70 75 74 65 72 5F 6E	69 6C 3E 3C 69 64 3E 75 42 3F 37 34 32 43 32 32 2D 36 35 45 41 2D 34 36 35 33 2D 39 43 34 38 2D 43 36 43 42 39 33 42 38 31 31 46 32 7D 3C 2F 69 64 3E 3C 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 70 61 73 73 77 6F 72 64 3E 66 61 6C 73 65 3C 2F 67 65 6E 65 72 61 74 65 5F 6E 65 77 5F 70 61 73 73 77 6F 72 64 3E 3C 61 73 6B 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 66 61 6C 73 65 3C 2F 61 73 6B 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 65 6E 74 3E 66 61 6C 73 65 3C 2F 73 65 6E 74 3E 3C 76 65 72 73 69 6F 6E 3E 37 30 32 32 30 3C 2F 76 65 72 73 69 6F 6E 3E 3C 70 75 62 6C 69 63 5F 6B 65 79 5F 6D 3E 3C 2F 70 75 62 6C 69 63 5F 6B 65 79 5F 6D 3E 3C 70 75 62 6C 69 63 5F 6B 65 79 5F 65 3E 3C 2F 70 75 62 6C 69 63 5F 6B 65 79 5F 65 3E 3C 70 61 73 73 77 6F 72 64 3E 3C 2F 70 61 73 73 77 6F 72 64 3E 3C 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 2F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 64 69 73 63 6C 61 69 6D 65 72 3E 3C 2F 64 69 73 63 6C 61 69 6D 65 72 3E 3C 6F 76 65 72 77 72 69 74 65 5F 69 64 5F 63 6F 64 65 3E 66 61 6C 73 65 3C 2F 6F 76 65 72 77 72 69 74 65 5F 69 64 5F 63 6F 64 65 3E 3C 6F 76 65 72 77 72 69 74 65 5F 69 64 3E 3C 64 69 73 63 6C 61 69 6D 65 72 3E 3C 2F 64 69 73 63 6C 61 69 6D 65 72 3E 3C 2F 6F 76 65 72 77 72 69 74 65 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 61 64 64 72 65 73 73 3E 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 6F 72 74 3E 35 36 35 35 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 6F 72 74 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 69 70 76 36 3E 66 61 6C 73 65 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 69 70 76 36 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 5F 70 69 6E 3E 66 61 6C 73 65 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 69 6E 3E 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 69 6E 3E 3C 63 6F 6D 70 75 74 65 72 5F 6E				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			61 6D 65 3E 3C 73 65 6C 66 5F 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 3C 2F 73 65 6C 66 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 6D 74 70 5F 73 65 74 74 69 6E 67 73 3E 3C 68 6F 73 74 3E 3C 2F 68 6F 73 74 3E 3C 70 6F 72 74 3E 35 38 37 3C 2F 70 6F 72 74 3E 3C 75 73 65 72 6E 61 6D 65 3E 3C 2F 75 73 65 72 6E 61 6D 65 3E 3C 70 61 73 73 77 6F 72 64 3E 3C 2F 70 61 73 73 77 6F 72 64 3E 3C 66 72 6F 6D 5F 65 6D 61 69 6C 3E 3C 2F 66 72 6F 6D 5F 65 6D 61 69 6C 3E 3C 75 73 65 5F 74 6C 73 3E 74 72 75 65 3C 2F 75 73 65 5F 74 6C 73 3E 3C 65 6D 61 69 6C 3E 3C 2F 65 6D 61 69 6C 3E 3C 73 75 62 6A 65 63 74 3E 3C 2F 73 75 62 6A 65 63 74 3E 3C 74 65 78 74 3E 3C 2F 74 65 78 74 3E 3C 2F 73 6D 74 70 5F 73 65 74 74 69 6E 67 73 3E 3C 2F 72 6D 73 5F 69 6E 65 74 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 0D 0A	74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 5F 70 69 6E 3E 66 61 6C 73 65 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 75 73 65 5F 70 69 6E 3E 3C 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 69 6E 3E 3C 2F 69 64 5F 63 75 73 74 6F 6D 5F 73 65 72 76 65 72 5F 70 6F 6D 70 75 74 65 72 5F 6E 61 6D 65 3E 3C 2F 63 6F 6D 70 75 74 65 72 5F 6E 61 6D 65 3E 3C 73 65 6C 66 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 3C 2F 73 65 6C 66 5F 69 64 65 6E 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 6D 74 70 5F 73 65 74 74 69 6E 67 73 3E 3C 68 6F 73 74 3E 3C 2F 68 6F 73 74 3E 3C 70 6F 72 74 3E 35 38 37 3C 2F 70 6F 72 74 3E 3C 75 73 65 72 6E 61 6D 65 3E 3C 2F 75 73 65 72 6E 61 6D 65 3E 3C 70 61 73 73 77 6F 72 64 3E 3C 2F 70 61 73 73 77 6F 72 64 3E 3C 66 72 6F 6D 5F 65 6D 61 69 6C 3E 3C 2F 66 72 6F 6D 5F 65 6D 61 69 6C 3E 3C 75 73 65 5F 74 6C 73 3E 74 72 75 65 3C 2F 75 73 65 5F 74 6C 73 3E 3C 65 6D 61 69 6C 3E 3C 2F 65 6D 61 69 6C 3E 3C 73 75 62 6A 65 63 74 3E 3C 2F 73 75 62 6A 65 63 74 3E 3C 74 65 78 74 3E 3C 2F 74 65 78 74 3E 3C 2F 73 6D 74 70 5F 73 65 74 74 69 6E 67 73 3E 3C 2F 72 6D 73 5F 69 6E 65 74 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 0D 0A				
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	General	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 70 6F 72 74 3E 35 36 35 30 3C 2F 70 6F 72 74 3E 3C 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 74 72 75 65 3C 2F 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 3C 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 74 72 75 65 3C 2F 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 3C 6C 61 6E 67 75 61 67 65 3E 4B 6F 72 65 61 6E 3C 2F 6C 61 6E 67 75 61 67 65 3E 3C 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 74 72 75 65 3C 2F 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 70 6F 72 74 3E 35 36 35 30 3C 2F 70 6F 72 74 3E 3C 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 74 72 75 65 3C 2F 68 69 64 65 5F 74 72 61 79 5F 69 63 6F 6E 5F 70 6F 70 75 70 5F 6D 65 6E 75 3E 3C 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 74 72 75 65 3C 2F 74 72 61 79 5F 6D 65 6E 75 5F 68 69 64 65 5F 73 74 6F 70 3E 3C 6C 61 6E 67 75 61 67 65 3E 4B 6F 72 65 61 6E 3C 2F 6C 61 6E 67 75 61 67 65 3E 3C 63 61 6C 6C 62 61 63 6B 5F	success or wait	1	4DD51F	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			6F 6E 6E 65 63 74 3E 3C 63 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 3C 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 37 65 69 36 75 6A 77 78 39 4B 41 3D 3C 2F 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 3C 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 3C 70 72 6F 74 65 63 74 5F 69 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 69 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 3C 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 66 61 6C 73 65 3C 2F 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 3C 75 73 65 5F 69 70 5F 76 5F 36 3E 74 72 75 65 3C 2F 75 73 65 5F 69 70 5F 76 5F 36 3E 3C 6C 6F 67 5F 75 73 65 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 3E 3C 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 3C 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 2F 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 2F 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 73 69 64 5F 69 64 3E 34 35 33 32 34 2E 34 30 31 30 31 33 37 30 33 37 3C 2F 73 69 64 5F 69 64 3E 3C 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 3C 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 74 72 75 65 3C 2F 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 3C 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 3C 6E 6F 74 69 66 79 5F 70 6C 61 79 5F 73 6F 75 6E 64 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 70 6C 61 79 5F 73 6F 75 6E 64 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 2D 31	61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 74 72 75 65 3C 2F 63 61 6C 6C 62 61 63 6B 5F 61 75 74 6F 5F 63 6F 6E 6E 65 63 74 3E 3C 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 61 6C 6C 62 61 63 6B 5F 63 6F 6E 6E 65 63 74 5F 69 6E 74 65 72 76 61 6C 3E 3C 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 37 65 69 36 75 6A 77 78 39 4B 41 3D 3C 2F 70 61 73 73 77 6F 72 64 5F 64 61 74 61 3E 3C 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 63 61 6C 6C 62 61 63 6B 5F 73 65 74 74 69 6E 67 73 3E 3C 70 72 6F 74 65 63 74 5F 69 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 74 72 75 65 3C 2F 70 72 6F 74 65 63 74 5F 69 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 3C 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 6C 65 67 61 63 79 5F 63 61 70 74 75 72 65 3E 3C 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 66 61 6C 73 65 3C 2F 64 6F 5F 6E 6F 74 5F 63 61 70 74 75 72 65 5F 72 64 70 3E 3C 75 73 65 5F 69 70 5F 76 5F 36 3E 74 72 75 65 3C 2F 75 73 65 5F 69 70 5F 76 5F 36 3E 3C 6C 6F 67 5F 75 73 65 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 3E 3C 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 66 61 6C 73 65 3C 2F 6C 6F 67 5F 75 73 65 5F 77 69 6E 64 6F 77 73 3E 3C 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 2F 63 68 61 74 5F 63 6C 69 65 6E 74 5F 73 65 74 74 69 6E 67 73 3E 3C 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 2F 61 75 74 68 5F 6B 65 79 5F 73 74 72 69 6E 67 3E 3C 73 69 64 5F 69 64 3E 34 35 33 32 34 2E 34 30 31 30 31 33 37 30 33 37 3C 2F 73 69 64 5F 69 64 3E 3C 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 73 68 6F 77 5F 70 61 6E 65 6C 3E 3C 6E 6F 74 69 66 79 5F 63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 74 72 75 65 3C 2F 6E 6F 74 69 66 79 5F				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			3C 2F 6E 6F 74 69 66 79 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 3C 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 37 37 75 2F 50 44 39 34 62 57 77 67 64 6D 56 79 63 32 6C 76 62 6A 30 69 4D 53 34 77 49 69 42 6C 62 6D 4E 76 5A 47 6C 75 5A 7A 30 69 56 56 52 47 4C 54 67 69 50 7A 34 4E 43 6A 78 77 63 6D 39 34 65 56 39 7A 5A 58 52 30 61 57 35 6E 63 79 42 32 5A 58 4A 7A 61 57 39 75 50 53 49 33 4D 44 49 79 4D 43 49 2B 50 48 56 7A 5A 56 39 77 63 6D 39 34 65 54 35 6D 59 57 78 7A 5A 54 77 76 64 58 4E 6C 58 33 42 79 62 33 68 35 50 6A 78 77 63 6D 39 34 65 56 39 30 65 58 42 6C 50 6A 41 38 4C 33 42 79 62 33 68 35 58 33 52 35 63 47 55 2B 50 47 68 76 63 33 51 2B 50 43 39 6F 62 33 4E 30 50 6A 78 77 62 33 4A 30 50 6A 67 77 4F 44 41 38 4C 33 42 76 63 6E 51 2B 50 47 35 6C 5A 57 52 66 59 58 56 30 61 44 35 6D 59 57 78 7A 5A 54 77 76 62 6D 56 6C 5A 46 39 68 64 58 52 6F 50 6A 78 75 64 47 31 73 58 32 46 31 64 47 67 2B 5A 6D 46 73 63 32 55 38 4C 32 35 30 62 57 78 66 59 58 56 30 61 44 34 38 64 58 4E 6C 63 6D 35 68 62 57 55 2B 50 43 39 31 63 32 56 79 62 6D 46 74 5A 54 34 38 63 47 46 7A 63 33 64 76 63 6D 51 2B 50 43 39 77 59 58 4E 7A 64 32 39 79 5A 44 34 38 5A 47 39 74 59 57 6C 75 50 6A 77 76 5A 47 39 74 59 57 6C 75 50 6A 77 76 63 48 4A 76 65 48 6C 66 63 32 56 30 64 47 6C 75 5A 33 4D 2B 44 51 6F 3D 3C 2F 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 3C 61 64 64 69 74 69 6F 6E 61 6C 3E 3C 2F 61 64 64 69 74 69 6F 6E 61 6C 3E 3C 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 66 61 6C 73 65 3C 2F 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74	63 68 61 6E 67 65 5F 74 72 61 79 5F 69 63 6F 6E 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 68 69 6E 74 3E 66 61 6C 73 65 3C 2F 6E 6F 74 69 66 79 5F 62 61 6C 6C 6F 6E 5F 68 69 6E 74 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 73 65 74 74 69 6E 67 73 3E 3C 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 78 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 2D 31 3C 2F 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 79 3E 3C 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 3C 6E 6F 74 69 66 79 5F 70 61 6E 65 6C 5F 73 65 74 74 69 6E 67 73 3E 37 37 75 2F 50 44 39 34 62 57 77 67 64 6D 56 79 63 32 6C 76 62 6A 30 69 4D 53 34 77 49 69 42 6C 62 6D 4E 76 5A 47 6C 75 5A 7A 30 69 56 56 52 47 4C 54 67 69 50 7A 34 4E 43 6A 78 77 63 6D 39 34 65 56 39 7A 5A 58 52 30 61 57 35 6E 63 79 42 32 5A 58 4A 7A 61 57 39 75 50 53 49 33 4D 44 49 79 4D 43 49 2B 50 48 56 7A 5A 56 39 77 63 6D 39 34 65 54 35 6D 59 57 78 7A 5A 54 77 76 64 58 4E 6C 58 33 42 79 62 33 68 35 50 6A 78 77 63 6D 39 34 65 56 39 30 65 58 42 6C 50 6A 41 38 4C 33 42 79 62 33 68 35 58 33 52 35 63 47 55 2B 50 47 68 76 63 33 51 2B 50 43 39 6F 62 33 4E 30 50 6A 78 77 62 33 4A 30 50 6A 67 77 4F 44 41 38 4C 33 42 76 63 6E 51 2B 50 47 35 6C 5A 57 52 66 59 58 56 30 61 44 35 6D 59 57 78 7A 5A 54 77 76 62 6D 56 6C 5A 46 39 68 64 58 52 6F 50 6A 78 75 64 47 31 73 58 32 46 31 64 47 67 2B 5A 6D 46 73 63 32 55 38 4C 32 35 30 62 57 78 66 59 58 56 30 61 44 34 38 64 58 4E 6C 63 6D 35 68 62 57 55 2B 50 43 39 31 63 32 56 79 62 6D 46 74 5A 54 34 38 63 47 46 7A 63 33 64 76 63 6D 51 2B 50 43 39 77 59 58 4E 7A 64 32 39 79 5A 44 34 38 5A 47 39 74 59 57 6C 75 50 6A 77 76 5A 47 39 74 59 57 6C 75 50 6A 77 76 63 48 4A 76 65 48 6C 66 63 32 56 30 64 47 6C 75 5A 33 4D 2B 44 51 6F 3D 3C 2F 70 72 6F 78 79 5F 73 65 74 74 69 6E 67 73 3E 3C 61 64 64 69 74 69 6F 6E 61 6C 3E 3C 64 69				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 77 69 74 68 5F 74 69 6D 65 6F 75 74 3E 3C 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 3C 2F 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 3C 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 30 3C 2F 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 66 61 6C 73 65 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 3C 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 3C 2F 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 3E 0D 0A	73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 66 61 6C 73 65 3C 2F 64 69 73 61 62 6C 65 5F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 66 61 6C 73 65 3C 2F 73 61 66 65 5F 6D 6F 64 65 5F 73 65 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 74 72 75 65 3C 2F 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 3C 73 68 6F 77 5F 69 64 5F 6E 6F 74 69 66 69 63 61 74 69 6F 6E 5F 72 65 71 75 65 73 74 3E 3C 69 6E 74 65 67 72 61 74 65 5F 66 69 72 65 77 61 6C 6C 5F 61 74 5F 73 74 61 72 74 75 70 3E 3C 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 30 3C 2F 63 6C 69 70 62 6F 61 72 64 5F 74 72 61 6E 73 66 65 72 5F 6D 6F 64 65 3E 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3E 66 61 6C 73 65 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 3C 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 36 30 3C 2F 63 6C 6F 73 65 5F 73 65 73 73 69 6F 6E 5F 69 64 6C 65 5F 69 6E 74 65 72 76 61 6C 3E 3C 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 66 61 6C 73 65 3C 2F 73 68 6F 77 5F 63 6F 6E 6E 65 63 74 69 6F 6E 5F 61 6C 65 72 74 5F 66 6F 72 5F 61 6C 6C 3E 3C 2F 67 65 6E 65 72 61 6C 5F 73 65 74 74 69 6E 67 73 3E 0D 0A				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Usoris\Remote Utilities Host\Host\Parameters	InternetId	binary	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 72 6D 73 5F 69 6E 74 65 72 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 2F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 75 73 65 5F 69 6E 65 74 5F 63 6F 6E 6E 65 63 74 69 6F 6E 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 69 6E 65 74 5F 63 6F 6E 6E 65 63 74 69 6F 6E 3E 3C 69 6E 65 74 5F 73 65 72 76 65 72 3E 3C 2F 69 6E 65 74 5F 73 65 72 76 65 72 3E 3C 75 73 65 5F 63 75 73 74 6F 6D 5F 69 6E 65 74 5F 73 65 72 76 65 72 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 63 75 73 74 6F 6D 5F 69 6E 65 74 5F 73 65 72 76 65 72 3E 3C 69 6E 65 74 5F 69 64 5F 70 6F 72 74 3E 35 36 35 35 3C 2F 69 6E 65 74 5F 69 64 5F 70 6F 72 74 3E 3C 75 73 65 5F 69 6E 65 74 5F 69 64 5F 69 70 76 36 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 69 6E 65 74 5F 69 64 5F 69 70 76 36 3E 3C 69 6E 65 74 5F 69 64 5F 75 73 65 5F 70 69 6E 3E 66 61 6C 73 65 3C 2F 69 6E 65 74 5F 69 64 5F 75 73 65 5F 70 69 6E 3E 3C 69 6E 65 74 5F 69 64 5F 70 69 6E 3E 3C 2F 69 6E 65 74 5F 69 64 5F 70 69 6E 3E 3C 2F 72 6D 73 5F 69 6E 74 65 72 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 0D 0A	EF BB BF 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0D 0A 3C 72 6D 73 5F 69 6E 74 65 72 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 20 76 65 72 73 69 6F 6E 3D 22 37 30 32 32 30 22 3E 3C 69 6E 74 65 72 6E 65 74 5F 69 64 3E 33 35 30 2D 37 30 30 2D 34 38 39 2D 37 30 39 3C 2F 69 6E 74 65 72 6E 65 74 5F 69 64 3E 3C 75 73 65 5F 69 6E 65 74 5F 63 6F 6E 6E 65 63 74 69 6F 6E 3E 3C 69 6E 65 74 5F 73 65 72 76 65 72 3E 3C 2F 69 6E 65 74 5F 73 65 72 76 65 72 3E 3C 75 73 65 5F 63 75 73 74 6F 6D 5F 69 6E 65 74 5F 73 65 72 76 65 72 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 63 75 73 74 6F 6D 5F 69 6E 65 74 5F 73 65 72 76 65 72 3E 3C 69 6E 65 74 5F 70 6F 72 74 3E 35 36 35 35 3C 2F 69 6E 65 74 5F 70 6F 72 74 3E 3C 75 73 65 5F 69 6E 65 74 5F 69 64 5F 69 70 76 36 3E 66 61 6C 73 65 3C 2F 75 73 65 5F 69 6E 65 74 5F 69 64 5F 69 70 76 36 3E 3C 69 6E 65 74 5F 69 64 5F 75 73 65 5F 70 69 6E 3E 66 61 6C 73 65 3C 2F 69 6E 65 74 5F 69 64 5F 75 73 65 5F 70 69 6E 3E 3C 69 6E 65 74 5F 69 64 5F 70 69 6E 3E 3C 2F 69 6E 65 74 5F 69 64 5F 70 69 6E 3E 3C 2F 72 6D 73 5F 69 6E 74 65 72 6E 65 74 5F 69 64 5F 73 65 74 74 69 6E 67 73 3E 0D 0A	success or wait	1	4DD51F	RegSetValueExW

Analysis Process: rutserv.exe PID: **8008**, Parent PID: **7876**

General

Target ID:	10
Start time:	09:37:20
Start date:	02/02/2024
Path:	C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" -firewall
Imagebase:	0x340000
File size:	21'148'984 bytes
MD5 hash:	652C2A693B333504A3879460D0AF7224
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	Borland Delphi
Reputation:	low
Has exited:	true

Analysis Process: rfusclient.exe PID: **8048**, Parent PID: **7876**

General	
Target ID:	11
Start time:	09:37:21
Start date:	02/02/2024
Path:	C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe
Imagebase:	0x650000
File size:	10'931'000 bytes
MD5 hash:	6AAE165F3B1575DB887A0370CFC80083
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low
Has exited:	false

Analysis Process: rfusclient.exe PID: **8068**, Parent PID: **7876**

General	
Target ID:	12
Start time:	09:37:21
Start date:	02/02/2024
Path:	C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe" /tray
Imagebase:	0x650000
File size:	10'931'000 bytes
MD5 hash:	6AAE165F3B1575DB887A0370CFC80083
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Reputation:	low
Has exited:	false

Analysis Process: rfusclient.exe PID: **5016**, Parent PID: **8048**

General	
Target ID:	15
Start time:	09:37:29
Start date:	02/02/2024
Path:	C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe" /tray
Imagebase:	0x650000
File size:	10'931'000 bytes
MD5 hash:	6AAE165F3B1575DB887A0370CFC80083
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Reputation:	low

Has exited:	true

Disassembly

No disassembly