ID: 1317431
Sample Name: Hu25VEa8Dr
Cookbook: default.jbs
Time: 06:00:34
Date: 01/10/2023
Version: 38.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report Hu25VEa8Dr.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 5
Yara Signatures 5
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Compliance 5
Networking 5
Data Obfuscation 6
Boot Survival 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 12
Private 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\ProgramData\Local Settings\Temp\msoiruj.bat 13
C:\Users\user\AppData\Local\Temp\0BBFF.tmp 14
C:\Users\user\AppData\Local\Temp\0BBFF.tmp:Zone.Identifier 14
C:\Users\user\AppData\Local\Temp\Firozedikami.dll 14
C:\Users\user\AppData\Local\Temp\Gozekeneka.dll 15
C:\Users\user\AppData\Local\Temp\Jahulocayedo.dll 15
C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe 16
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe 16
C:\Users\user\AppData\Local\Temp\Sahofivizu.exe 16
C:\Users\user\AppData\Local\Temp\Yumicebivud.rih 17
C:\Users\user\AppData\Local\Temp\Zojemilocan.dll 17
C:\Users\user\AppData\Local\Temp\naseropuxeq.dll 17
C:\Users\user\AppData\Local\Temp\natigezeholi.dll 18
C:\Users\user\AppData\Local\Temp\rikayolehofu.Xoc 18
C:\Users\user\AppData\Local\Temp\xuxokuxoka.dll 18
C:\Users\user\AppData\Local\Temp\yiduyevutog.dll 19
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171 19

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\R3PRUMZY.txt 19
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y4A6H5R0.txt 20
Static File Info 20
General 20
File Icon 20
Static PE Info 21
General 21
Entrypoint Preview 21
Rich Headers 22
Data Directories 22
Sections 22
Resources 23
Imports 23
Possible Origin 23
Network Behavior 23
Snort IDS Alerts 23
Network Port Distribution 24
TCP Packets 24
UDP Packets 24
ICMP Packets 25
DNS Queries 25
DNS Answers 25
HTTP Request Dependency Graph 26
Statistics 26
Behavior 26
System Behavior 26
Analysis Process: Hu25VEa8Dr.exePID: 2948, Parent PID: 1244 26
General 26
File Activities 26
Analysis Process: Sahofivizu.exePID: 920, Parent PID: 2948 27
General 27
File Activities 27
File Read 27
Analysis Process: Hu25VEa8Dr.exePID: 1724, Parent PID: 920 27
General 27
File Activities 27
File Created 27
File Deleted 27
Analysis Process: Hu25VEa8Dr.exePID: 2092, Parent PID: 1724 28
General 28
File Activities 28
File Created 28
File Deleted 28
File Written 28
File Read 29
Registry Activities 29
Key Value Created 29
Analysis Process: msiexec.exePID: 1948, Parent PID: 2092 38
General 38
File Activities 38
File Created 38
File Deleted 39
File Written 39
File Read 41
Analysis Process: Lohonibuhod.exePID: 1396, Parent PID: 1948 41
General 41
File Activities 42
File Read 42
Analysis Process: msiexec.exePID: 2748, Parent PID: 1396 42
General 42
File Activities 42
File Created 42
File Deleted 42
Analysis Process: msiexec.exePID: 2948, Parent PID: 2748 42
General 42
File Activities 43
Analysis Process: svchost.exePID: 1740, Parent PID: 2948 43
General 43
File Activities 43
File Created 43
File Deleted 44
File Written 44
File Read 45
Registry Activities 45
Key Created 45
Key Value Created 45
Disassembly 49

Windows Analysis Report

Hu25VEa8Dr.exe

Overview

General Information

Sample Name:	Hu25VEa8Dr.exe (renamed file extension from none to exe, renamed because original name is a hash value)
Original Sample Name:	9535a9bb1ae8…
Analysis ID:	1317431
MD5:	bc76bd7b332a…
SHA1:	c6858031315a…
SHA256:	9535a9bb1ae8…
Infos:	

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

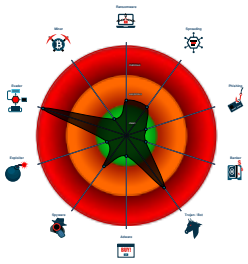
Gamarue

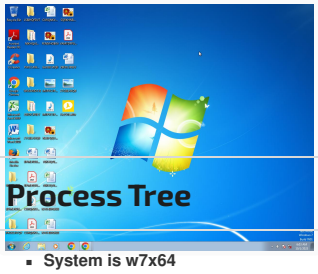
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Tries to download HTTP data from a…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Yara detected Gamarue
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic

Classification





- **System is w7x64**
- Hu25VEa8Dr.exe (PID: 2948 cmdline: C:\Users\user\Desktop\Hu25VEa8Dr.exe MD5: BC76BD7B332AA8F6AEDBB8E11B7BA9B6)
  - Sahofivizu.exe (PID: 920 cmdline: C:\Users\user\AppData\Local\Temp\Sahofivizu.exe" "C:\Users\user\Desktop\Hu25VEa8Dr.exe MD5: 7FE00CC4EA8429629AC0AC610DB51993)
    - Hu25VEa8Dr.exe (PID: 1724 cmdline: C:\Users\user\Desktop\Hu25VEa8Dr.exe MD5: BC76BD7B332AA8F6AEDBB8E11B7BA9B6)
      - Hu25VEa8Dr.exe (PID: 2092 cmdline: C:\Users\user\Desktop\Hu25VEa8Dr.exe MD5: BC76BD7B332AA8F6AEDBB8E11B7BA9B6)
        - msiexec.exe (PID: 1948 cmdline: "C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe" MD5: B3657BCFE8240BC0985093A0F8682703)
          - Lohonibuhod.exe (PID: 1396 cmdline: "C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe" "C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe" MD5: 44902781C1865978B17F396DB51D85E1)
            - msiexec.exe (PID: 2748 cmdline: "C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe" MD5: B3657BCFE8240BC0985093A0F8682703)
              - msiexec.exe (PID: 2948 cmdline: "C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe" MD5: B3657BCFE8240BC0985093A0F8682703)
  - svchost.exe (PID: 1740 cmdline: C:\Windows\syswow64\svchost.exe MD5: 54A47F6B5E09A77E61649109C6A08866)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Andromeda, Gamarue, B106-Gamarue, B67-SS-Gamarue		• Operation C-Major	http://blog.morphisec.com/andromeda-tactics-analyzedhttp://resources.infosecinstitute.com/andromeda-bot-analysis-part-two/http://resources.infosecinstitute.com/andromeda-bot-analysis/http://www.0xebfe.net/blog/2013/03/30/fooled-by-andromeda/https://blog.avast.com/andromeda-under-the-microscope	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.andromeda

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: svchost.exe PID: 1740	JoeSecurity_Gamarue	Yara detected Gamarue	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Known Sinkhole Response Kryptos Logic - Source IP: 147.75.61.38 - Destination IP: 192.168.2.22

Timestamp:	147.75.61.38192.168.2.2280491662031515 10/01/23-06:01:37.455932
SID:	2031515
Source Port:	80
Destination Port:	49166
Protocol:	TCP
Classtype:	Misc activity

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

System process connects to network (likely due to code injection or exploit)

Tries to download HTTP data from a sinkholed server

Snort IDS alert for network traffic

Contains functionality to check if Internet connection is working

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Boot Survival

Creates an undocumented autostart registry key

Malware Analysis System Evasion

Contain functionality to detect virtual machines

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Stealing of Sensitive Information

Yara detected Gamarue

Remote Access Functionality

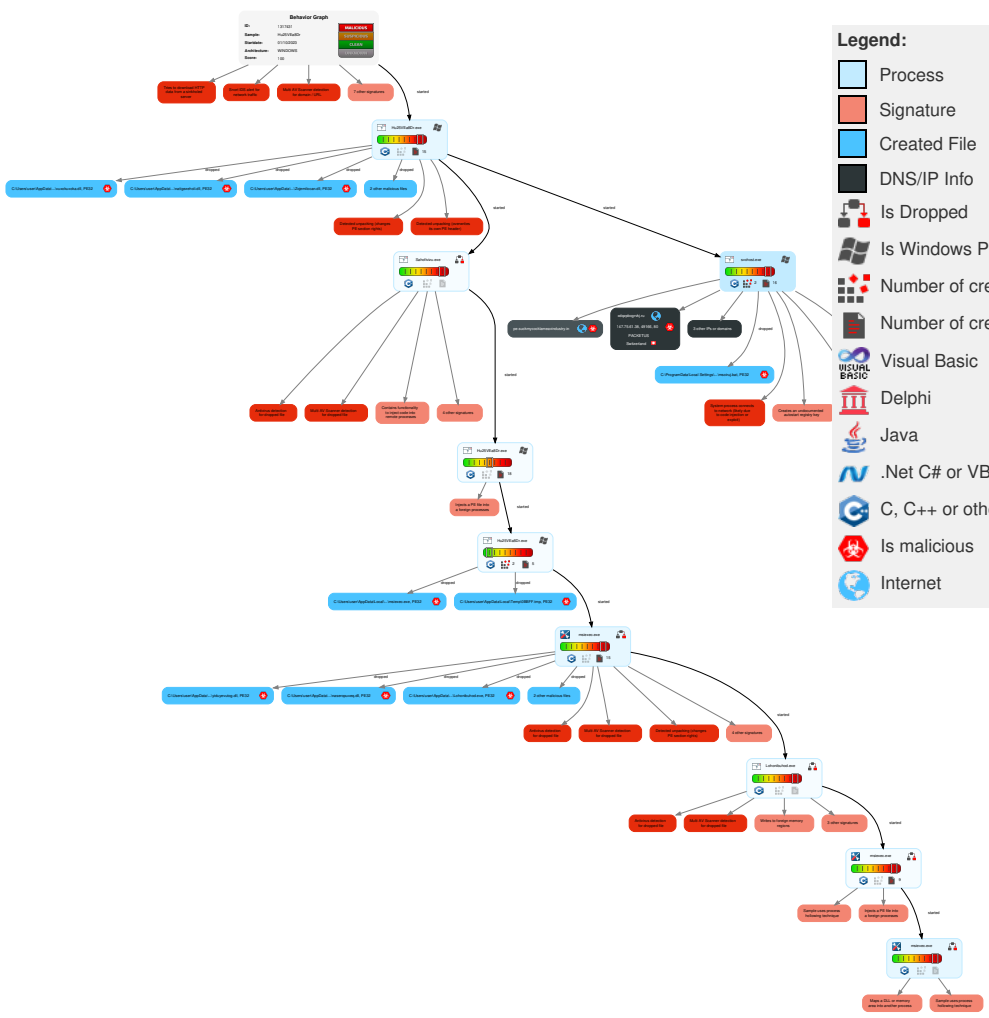
Yara detected Gamarue

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Obfuscated Files or Information	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	1 Registry Run Keys / Startup Folder	7 1 1 Process Injection	2 1 Software Packing	LSASS Memory	1 Peripheral Device Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	Security Account Manager	1 System Network Connections Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Masquerading	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Modify Registry	LSA Secrets	1 1 6 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 6 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	7 1 1 Process Injection	DCSync	1 3 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	2 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

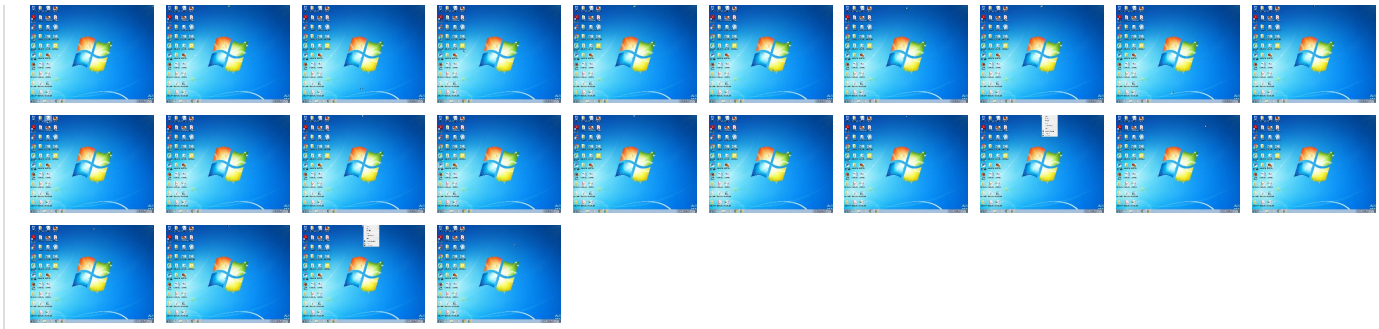
Behavior Graph



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
Hu25VEa8Dr.exe	96%	ReversingLabs	Win32.Backdoor.Andromeda	
Hu25VEa8Dr.exe	82%	Virustotal		Browse
Hu25VEa8Dr.exe	100%	Avira	TR/AD.Gamarue.njjtd	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Gozekeneka.dll	100%	Avira	HEUR/AGEN.1358866	
C:\Users\user\AppData\Local\Temp\0BBFF.tmp	100%	Avira	TR/AD.Gamarue.njjtd	
C:\Users\user\AppData\Local\Temp\xuxokuxoka.dll	100%	Avira	TR/Symmi.17001.30	
C:\Users\user\AppData\Local\Temp\naseropuxeq.dll	100%	Avira	TR/Graftor.75972.7	
C:\Users\user\AppData\Local\Temp\yiduyevutog.dll	100%	Avira	TR/Symmi.17001.22	
C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe	100%	Avira	TR/Agent.hwpf	
C:\Users\user\AppData\Local\Temp\natigezeholi.dll	100%	Avira	HEUR/AGEN.1328724	
C:\ProgramData\Local Settings\Temp\msoiruj.bat	100%	Avira	TR/AD.Gamarue.djauj	
C:\Users\user\AppData\Local\Temp\Sahofivizu.exe	100%	Avira	HEUR/AGEN.1344339	
C:\Users\user\AppData\Local\Temp\Jahulocayedo.dll	100%	Avira	TR/Symmi.17001.23	
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	100%	Avira	TR/AD.Gamarue.djauj	
C:\Users\user\AppData\Local\Temp\Zojemilocan.dll	100%	Avira	HEUR/AGEN.1322941	
C:\ProgramData\Local Settings\Temp\msoiruj.bat	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	100%	Joe Sandbox ML		
C:\ProgramData\Local Settings\Temp\msoiruj.bat	87%	ReversingLabs	Win32.Backdoor.Andromeda	
C:\ProgramData\Local Settings\Temp\msoiruj.bat	85%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\0BBFF.tmp	96%	ReversingLabs	Win32.Backdoor.Andromeda	
C:\Users\user\AppData\Local\Temp\0BBFF.tmp	82%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Firozedikami.dll	59%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\Firozedikami.dll	59%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Gozekeneka.dll	77%	ReversingLabs	Win32.Trojan.Tiggre	
C:\Users\user\AppData\Local\Temp\Gozekeneka.dll	75%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Jahulocayedo.dll	71%	ReversingLabs	Win32.Trojan.Ursu	
C:\Users\user\AppData\Local\Temp\Jahulocayedo.dll	66%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe	76%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe	77%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	87%	ReversingLabs	Win32.Backdoor.Andromeda	
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	85%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Sahofivizu.exe	57%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\Sahofivizu.exe	61%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Zojemilocan.dll	64%	ReversingLabs	Win32.Backdoor.Andromeda	
C:\Users\user\AppData\Local\Temp\Zojemilocan.dll	74%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\naseropuxeq.dll	59%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\naseropuxeq.dll	71%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\natigezeholi.dll	78%	ReversingLabs	Win32.Trojan.Ursu	
C:\Users\user\AppData\Local\Temp\natigezeholi.dll	76%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\xuxokuxoka.dll	67%	ReversingLabs	Win32.Trojan.Symmi	
C:\Users\user\AppData\Local\Temp\xuxokuxoka.dll	67%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\yiduyevutog.dll	71%	ReversingLabs	Win32.Trojan.Ursu	
C:\Users\user\AppData\Local\Temp\yiduyevutog.dll	73%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
xdqzpbcgrvkj.ru	19%	Virustotal		Browse
anam0rph.su	11%	Virustotal		Browse
pe.suckmycocklameavindustry.in	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pe.suckmycocklameavindustry.in/	0%	Avira URL Cloud	safe	
http://orzdwjtvmein.in/in.php	100%	Avira URL Cloud	malware	
http://bdcrqgonzmwuehky.nl/in.php	100%	Avira URL Cloud	malware	
http://pe.suckmycocklameavindustry.in/DOS_STUBhttp://sc.suckmycocklameavindustry.in/ImageBasehttp://	0%	Avira URL Cloud	safe	
http://orzdwjtvmein.in/in.php	11%	Virustotal		Browse
http://pe.suckmycocklameavindustry.in/dtkdvjezlgdvslgbvqqjiiheaxroigffC:	0%	Avira URL Cloud	safe	
http://pe.suckmycocklameavindustry.in/	7%	Virustotal		Browse
http://pe.suckmycocklameavindustry.in/dtkdvjezlgdvslgbvqqjiiheaxroigff6Tl	0%	Avira URL Cloud	safe	
http://somicrososoft.ru/in.php	100%	Avira URL Cloud	malware	
http://pe.suckmycocklameavindustry.in/DOS_STUBhttp://sc.suckmycocklameavindustry.in/ImageBasehttp://	3%	Virustotal		Browse
http://img.suckmycocklameavindustry.in/	0%	Avira URL Cloud	safe	
http://xdqzpbcgrvkj.ru/in.php	100%	Avira URL Cloud	malware	
http://bdcrqgonzmwuehky.nl/in.php	11%	Virustotal		Browse
http://somicrososoft.ru/in.php	14%	Virustotal		Browse
http://anam0rph.su/in.php	100%	Avira URL Cloud	malware	
http://xdqzpbcgrvkj.ru/in.phphttp://anam0rph.su/in.phphttp://orzdwjtvmein.in/in.phphttp://ygiudewsqh	100%	Avira URL Cloud	malware	
http://img.suckmycocklameavindustry.in/	4%	Virustotal		Browse
http://sc.suckmycocklameavindustry.in/	0%	Avira URL Cloud	safe	
http://ygiudewsqhct.in/in.php	100%	Avira URL Cloud	malware	
http://anam0rph.su/in.php	13%	Virustotal		Browse
http://xdqzpbcgrvkj.ru/in.phphttp://anam0rph.su/in.phphttp://orzdwjtvmein.in/in.phphttp://ygiudewsqh	14%	Virustotal		Browse
http://ygiudewsqhct.in/in.php	13%	Virustotal		Browse
http://pe.suckmycocklameavindustry.in/dtkdvjezlgdvslgbvqqjiiheaxroigff	0%	Avira URL Cloud	safe	
http://xdqzpbcgrvkj.ru/in.php	17%	Virustotal		Browse
http://sc.suckmycocklameavindustry.in/	7%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pe.suckmycocklameavindustry.in	34.29.71.138	true	true	• 7%, Virustotal, Browse	unknown
xdqzpbcgrvkj.ru	147.75.61.38	true	true	• 19%, Virustotal, Browse	unknown
anam0rph.su	unknown	unknown	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

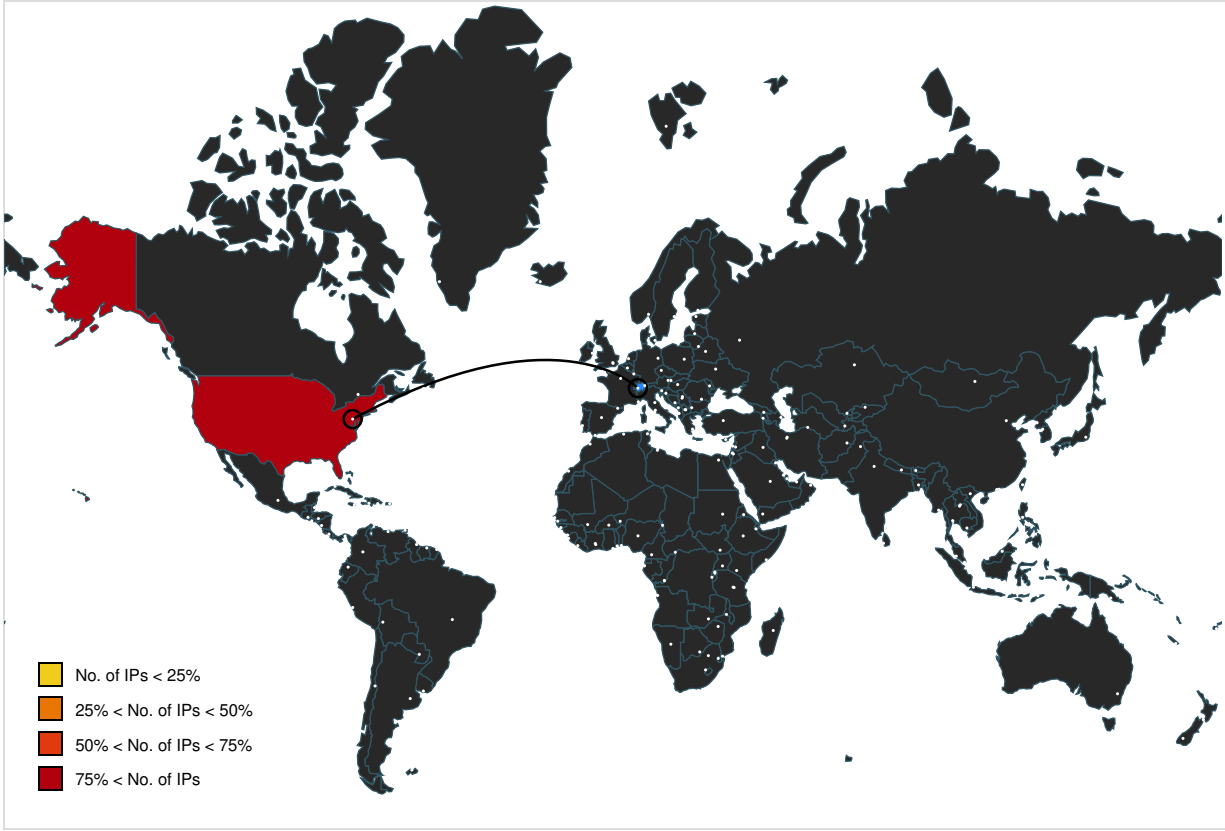
Name	Malicious	Antivirus Detection	Reputation
http://xdqzpbcgrvkj.ru/in.php	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://pe.suckmycocklameavindustry.in/dtkdvjezlgdvslgbvqqjiiheaxroigff	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://pe.suckmycocklameavindustry.in/	svchost.exe	false	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://orzdwjtvmein.in/in.php	svchost.exe, svchost.exe, 00000009.00000002.381446071.0000000000020000.00000040.00001000.00020000.00000000.sdmp	false	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	msiexec.exe, msiexec.exe, 00000005.00000002.353292307.0000000000409000.00000004.00000001.01000000.0000000A.sdmp, msiexec.exe, 00000005.00000000.351213851.0000000000409000.00000008.00000001.01000000.0000000A.sdmp, msiexec.exe, 00000007.00000000.364458175.0000000000409000.00000008.00000001.01000000.0000000A.sdmp, msiexec.exe, 00000008.00000000.365114158.0000000000409000.00000008.00000001.01000000.0000000A.sdmp, Hu25VEa8Dr.exe, 0BBFF.tmp.4.dr, msoiruj.bat.9.dr, msiexec.exe.4.dr	false		high
http://bdcrqgonzmwuehky.nl/in.php	svchost.exe, svchost.exe, 00000009.00000002.381446071.0000000000020000.00000040.00001000.00020000.00000000.sdmp	false	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://pe.suckmycocklameavindustry.in/DOS_STUBhttp://sc.suckmycocklameavindustry.in/ImageBasehttp://	svchost.exe, 00000009.00000003.373478974.0000000000130000.00000040.00001000.00020000.00000000.sdmp, svchost.exe, 00000009.00000002.381475492.00000000001E0000.00000040.00001000.00020000.00000000.sdmp	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://pe.suckmycocklameavindustry.in/dtkdvjezlgdvslgbvqqjiiheaxroigffC:	svchost.exe, 00000009.00000002.381503603.00000000004D4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000009.00000002.381500240.000000000044A000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://pe.suckmycocklameavindustry.in/dtkdvjezlgdvslgbvqqjiiheaxroigff6Tl	svchost.exe, 00000009.00000002.381503603.0000000000484000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://somicrososoft.ru/in.php	svchost.exe, svchost.exe, 00000009.00000002.381446071.0000000000020000.00000040.00001000.00020000.00000000.sdmp	false	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://img.suckmycocklameavindustry.in/	svchost.exe	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://nsis.sf.net/	Hu25VEa8Dr.exe, 00000003.00000002.350134891.0000000002120000.00000004.00000020.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	Hu25VEa8Dr.exe, 0BBFF.tmp.4.dr, msoiruj.bat.9.dr, msiexec.exe.4.dr	false		high
http://anam0rph.su/in.php	svchost.exe, svchost.exe, 00000009.00000002.381446071.0000000000020000.00000040.00001000.00020000.00000000.sdmp	false	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://xdqzpbcgrvkj.ru/in.phphttp://anam0rph.su/in.phphttp://orzdwjtvmein.in/in.phphttp://ygiudewsqh	svchost.exe, 00000009.00000002.381446071.0000000000020000.00000040.00001000.00020000.00000000.sdmp	false	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://sc.suckmycocklameavindustry.in/	svchost.exe	false	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ygiudewsqhct.in/in.php	svchost.exe, svchost.exe, 00000009.00000002.381446071.0000000000020000.00000040.00001000.00020000.00000000.sdmp	false	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.29.71.138	pe.suckmycocklameavindustry.in	United States		2686	ATGS-MMD-ASUS	true
147.75.61.38	xdqzpbcgrvkj.ru	Switzerland		54825	PACKETUS	true

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	38.0.0 Beryl
Analysis ID:	1317431
Start date and time:	2023-10-01 06:00:34 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	13
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 file name:	Hu25VEa8Dr.exe (renamed file extension from none to exe, renamed because original name is a hash value)
Original Sample Name:	9535a9bb1ae8f620d7cbd7d9f5c20336b0fd2c78d1a7d892d76e4652dd8b2be7

Detection:	MAL
Classification:	mal100.troj.evad.winEXE@17/19@7/3
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe
- Excluded IPs from analysis (whitelisted): 209.197.3.8, 8.252.14.254, 67.26.203.254, 8.253.135.120, 8.252.139.254, 8.252.140.126, 20.72.235.82
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, redir.update.msft.com.trafficmanager.net, www.update.microsoft.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:01:19	API Interceptor	8x Sleep call for process: Hu25VEa8Dr.exe modified
06:01:26	API Interceptor	1x Sleep call for process: msiexec.exe modified
06:01:35	API Interceptor	42x Sleep call for process: svchost.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:\ProgramData\Local Settings\Temp\msoiruj.bat

Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	88209
Entropy (8bit):	7.192271927525946
Encrypted:	false

SSDEEP:	1536:cpgpHzb9dZVX9fHMvG0D3XJz0MAuV9wWGm1FJaThXPF5zRRn55NATTeIIQ:qgXdZt9P6D3XJYMHV9wWGkEZ7Fx55NCr
MD5:	B3657BCFE8240BC0985093A0F8682703
SHA1:	4E19F1CC04645356FD523E67655E5D76A19A86BA
SHA-256:	5F4B0AA22CE65B30FB232421673FAD4C1269709282O7ADE256D3BFEE33DC3687
SHA-512:	71C06203020C5C5BCB1C9F8383544BF270C5D7FAC1E732FEC1F78820BBF91A6DB5888FF57D782A05D49A960351B5436966C78974C60B40908099603118C56B15
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 87% • Antivirus: Virustotal, Detection: 85%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i..iw..iu..i...i..id..i!..i...i...it..iRichu..i.....PE..L.....K.....^.....0.....p....@.....t.....p..X?.....p.....text...L\.....^..... ..`.rdata.....p.....b.....@..@.data...X\.....v.....@....ndata.....rsrc...X?...p...@...z.....@..@.....

C:\Users\user\AppData\Local\Temp\0BBFF.tmp

Process:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	196227
Entropy (8bit):	7.67760121359675
Encrypted:	false
SSDEEP:	3072:ugXdZt9P6D3XJ3TCM/vosUE2L/TLqtAyD2XXhtksIae31fXJHhKgzyJtdeV:ue34p/vr6yrC2sJe35ZBKg0dW
MD5:	BC76BD7B332AA8F6AEDBB8E11B7BA9B6
SHA1:	C6858031315A50EC87E37966291EC69B64600EFB
SHA-256:	9535A9BB1AE8F620D7CBD7D9F5C20336B0FD2C78D1A7D892D76E4652DD8B2BE7
SHA-512:	C74A8A893D0D91EF9423C75C14E701102F01D46B4638D7E3184C95BFD4FF29F9CAB71FE5DE45E8E201DCDB8DF77E952A18E32BFED5014B9C8155C189825F379
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 96% • Antivirus: Virustotal, Detection: 82%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i..iw..iu..i...i..id..i!..i...i...it..iRichu..i.....PE..L.....K.....^.....0.....p....@.....t.....p...C.....p.....text...L\.....^..... ..`.rdata.....p.....b.....@..@.data...X\.....v.....@....ndata.....rsrc....C...p...D...z.....@..@.....

C:\Users\user\AppData\Local\Temp\0BBFF.tmp:Zone.Identifier

Process:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Reputation:	low
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\Firozedikami.dll

Process:	C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3584

Entropy (8bit):	2.4737941425256986
Encrypted:	false
SSDEEP:	24:ev1GSN60lFZCJdYvP/yYhqlVrfRgtaU40Zfxw6XgE:q0LZCDYHJrftofXg
MD5:	775A98111E9A1142F44EE78ABD0C37AA
SHA1:	1566C2070880FD0A7533AB34F19C9DF13E166F30
SHA-256:	855C6ECC9D9B3BA70B1E4D6F1CECC9AE88F9A36E62338C0C9000CEF28EA85F85
SHA-512:	B154DCCBEC5D4F236C66B1FC045A886C4CBB8DF6CD11FCF7FF48101AE233AD0E8494240144013 48F7815C788EAE366A1FD681449E534FBD4554475507718E22
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 59% • Antivirus: Virustotal, Detection: 59%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..._..._..._.).U..._...^..._.).T..._.).[..._.Rich..._.....PE..L. ...xGQ.....!.....f..... .....P..... ..P.... ..(.....@..P..... .....text... ....`.rdata..... .....@..@.data...H....0.....@....reloc..v....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\Gozekeneka.dll

Process:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.3074171093110873
Encrypted:	false
SSDEEP:	48:CXqWBMk6A7qZ2LcYKEbcqNCCC81iBtYf86SyuUH5npNpRppv5D:Cqv2cOCCC81Aw8hyBnNvv
MD5:	7AC02E7E2C7EC30BFC8C946D12DF26A0
SHA1:	079FF9DBFC5AF1D4DC569203847F50A8B30B5056
SHA-256:	71CFBE0622AEA1248EFF7CA09095493B3D47DF40E0936493B098D770551213F3
SHA-512:	DAC09E5CA0BDA7A9094A34F17B6606767B4A1E308148BFC1AC7E1C0AA55404C4AA50366C8F5F9BC2D225BE88D9290CCB7F55AECF71CB400528538367A2E2CA 3F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 77% • Antivirus: Virustotal, Detection: 75%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....IMr..,...,...,...0...,...3...,...,...,...o3...,...3...,...*...,...3...,..Rich,..... .....PE..L.....GQ.....!..... .....`..... ..J... ..<....@..X.....P..d..... .. ..... .....text...B..... ..`.rdata..*.... .....@..@.data...x....0.....@....rsrc...X....@.....@..@.reloc.....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\Jahulocayedo.dll

Process:	C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7221735995832015
Encrypted:	false
SSDEEP:	48:CXqWBMkLSPowUXULXfCmY6ULcYKEbc2VsTgt0fJdkp9uUH5nr3dppfO9:CqN7UXULXffY6EcSMJdkrBV3F29
MD5:	213FF346767B1B7C2AF9EC4EF51A7267
SHA1:	66D9FE22F0403E52EFFCCE675DEB8D674C11AF5D
SHA-256:	F227C46CCD589B9F48F066F0901DFF6A772B332E725BA0030A273B5B5A8BC41C
SHA-512:	B91E4D76F17B9245AE97FD7D7FB44E307C8A2A0C043FD212BAA7C4EEE946729A43CEF72F77344EA52BA6C9934CE01F85F6E839CC00BEB4ABEABDCF4B32644 206
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 71% • Antivirus: Virustotal, Detection: 66%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....IMr..,...,...,...0...,...3...,...,...,...o3...,...3...,...*...,...3...,..Rich,..... .....PE..L....xGQ.....!.....O..... .....`..... ..K... ..<....@..`.....P..|..... .. ..text..... ..`.rdata..+.... .....@..@.data.....0.....@....rsrc...`....@.....@..@.reloc.....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe

Process:	C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19968
Entropy (8bit):	4.009299462345418
Encrypted:	false
SSDEEP:	96:kinIPI95bH6bfG6rg0cbqiJrlUoynNmwIvc0NFSH:XnD5bGVrlHiJrlUoynNmwIvN4
MD5:	44902781C1865978B17F396DB51D85E1
SHA1:	D1EBC2238FCA1CFFCABBD692E9AF4D3121396983
SHA-256:	667FFD6F177DD67F4928DDE38378C5E500984CE40ED73BB6F1B3EE997B513403
SHA-512:	D60828174B1D042A4541FD26D4AF2DEABD44BB862C416B31BE28DE0B133FC9E2569389CDD0185B70819080B5AF0F54CFC72F7B96808CEE7FFB7C4C7E3E7647 4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 76% • Antivirus: Virustotal, Detection: 77%, Browse
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........B.v.#.%.#.%.#.%.?.%.#.%N?.%.#.%%<.%.#.%%<.%.#.%.<.% .#.%.#.%.#.%%<.%.#.%u%.%.#.%Rich.#.%................PE..L....xGQ.....................@............... ....@... ....@..H7................ ....text...0........................... ..`.rdata..t.... ....@..@.data........0......................@....rsrc...H7...@...8........... ......@..@.. ....

C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe

Process:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	88209
Entropy (8bit):	7.192271927525946
Encrypted:	false
SSDEEP:	1536:cpgpHzb9dZVX9fHMvG0D3XJz0MAuV9wWGm1FJaThXPF5zRRn55NATTeIlQ:qgXdZt9P6D3XJYMHV9wWGkEZ7Fx55NCr
MD5:	B3657BCFE8240BC0985093A0F8682703
SHA1:	4E19F1CC04645356FD523E67655E5D76A19A86BA
SHA-256:	5F4B0AA22CE65B30FB232421673FAD4C126970928207ADE256D3BFEE33DC3687
SHA-512:	71C06203020C5C5BCB1C9F8383544BF270C5D7FAC1E732FEC1F78820BBF91A6DB5888FF57D782A05D49A960351B5436966C78974C60B40908099603118C56B15
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 87% • Antivirus: Virustotal, Detection: 85%, Browse
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......1..:u..iu..iu..i..iw..iu..i...i..id..i!..i...i...it..iRichu..i.........................PE..L. .....K.................^...........0.......p....@..t.......p..X?...p...............................text... L\.......^.................. ..`.rdata.......p.......b.............@..@.data...X\...........v.............@....ndata...................................rsrc...X?...p...@...z.............@..@...................................... ....

C:\Users\user\AppData\Local\Temp\Sahofivizu.exe

Process:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.1878975851833986
Encrypted:	false
SSDEEP:	192:1AFmqdxP1oynRg94DELe9vZ/wJcVuhWEx:yFL1Q9eR6hTx
MD5:	7FE00CC4EA8429629AC0AC610DB51993
SHA1:	5B2B4BF75EF99D03D3EA3A778E0BD0B124C5E70B
SHA-256:	9827E20FFED86C23DD493845F03A9041977C5CF0E5DA14EDFEB7EDADFAA34508
SHA-512:	F1E919C53E6829447F03AAFEDFC0128CEC4F03C21CC127A26C9CB336D42DEBF94703C9939976EE9B74F629C6713CB571F178D500503BE88E8A2D770AA2843BI 5
Malicious:	**true**

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 57% • Antivirus: Virustotal, Detection: 61%, Browse
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........v..%..%..%T..%..%?..%..%?..%..%...%..%..%..%?..%. .%o.%..%Rich..%................PE..L.....GQ.....................V......6........ ....@.. ....P...;.. ....text.............................. ..`.rdata....... ....@..@.data........0......................@....rsrc....;...P...<.................@..@... ....

C:\Users\user\AppData\Local\Temp\Yumicebivud.rih

Process:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	7.980181192486164
Encrypted:	false
SSDEEP:	1536:gVbB3S+6LC/SQd6sTGmGEWx+JWgxhfCvWYjo/pk2X+FMCZTtkUn4rEeaMj31e5+P:KhTSQ0omUyD2X8htksIae31fX9cnheF7
MD5:	0F12B3226FE28398608E4F48B3FAFCA2
SHA1:	38B5BFD50DF9775C8ED379A0FA5F43979411E252
SHA-256:	7637E855C4F59DDFE01C9857FBDFF59036177BC1B439B4B0A24E14BC2E3E509A
SHA-512:	089DBFF0BFB72F3925E67055D45D357602D999AFAF7E82238AF18A2D3C86C9B1C37672C049E14939B3E414B11875DD70EF31F72D29B3ADA68D826081B5C347A
Malicious:	false
Reputation:	low
Preview:	a\JFBTTs[YWQrM82758275827g]ABX]f_G]SS5827582758275827^]@YPT...\^[58275827582758275kWCaP@RT\qX[LWOA8275827582yAm\ZTHd^PO}Qf]QC\W\75 827582pPLf_G]SSvW\CP@F758275827582pPL.XQM^RsQ^R{Y_Rt82758275827gL^mPJ]zPU]EL8275827582758\CQT^.QT^75827582758275.WCeJ]Tt\VEPKA7582 7582{ZYV{\Z@VGAs758275827582758a_YOSG\.V[Y82758275827582758 2`GQFReJ]TPKAzPU]EL82758275.WCvW_ZTVV{\VWv58275827eYF_r]FvG_Av582758275 827vJWVA]bEZ[WDFy2758275827582758275uh.5;275<275..75.2758275x27582758275827582758275827582758275.2756-.;8.>...6y..c]QA.EJ]PGY_.VY\YZL.UP.@B[. [Y.|}d.U]SP.?:?.2758275.....O...O...O..7P...O..\S...O..7P...O...O...O..P...O...O...O..7P...O..gI...O..j[T].O..82758275hw75t345..pd82758275.284331582758.658275. .758"758"7582w58"758075<2758275<27582758.5586758275:27582'58"7582'58"758275(27582758275<#75.2758.75..658275827582758275827582758275827582758 27582758275827582758275827582758275827582758"75.27582758275827582758275827582758275.@STLS75d4758"758:75867582758275827582758275x27u.VVAY275.?758.758<758>7 5827582758275x27..@DG[275..658.758.658(

C:\Users\user\AppData\Local\Temp\Zojemilocan.dll

Process:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	2.9848615810105574
Encrypted:	false
SSDEEP:	24:eFGSWUcWLuSDlkGPfe58//zYVVfiRHtaU4VExxSIVSPAEVlcr7:iWGLvybcMDfXtVe4PAylcr
MD5:	3ED0F4B16841CCF3C6D613E77BCEF3CD
SHA1:	751E4846DB47CCF5F94DB4CA198E96E77A7032E7
SHA-256:	A9B7526FE7C988F2219FA3B726DC2F771DE38C31593C3B8DAD3AC06E60135AC3
SHA-512:	6D44120D28AB5CA8164423C428EDDBF488C605A56F20794BB96618E8539AA50F9A24B9FD48E58001CEB95EC7932DC96BC48CB3F9C732FA0481F76C81F91CFF B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 64% • Antivirus: Virustotal, Detection: 74%, Browse
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..................y................y.....y.....Rich...........PE..L.....GQ...........!............. ...Q........ ....P..................................... !..O...$ ..<............................@..L.. ..$............................text.............................. .. `.rdata..o.... ....@..@.data...d....0.....................@....reloc..t....@......................@..B... ....

C:\Users\user\AppData\Local\Temp\naseropuxeq.dll

Process:	C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17408
Entropy (8bit):	6.090813739725965
Encrypted:	false
SSDEEP:	192:ZPtFv5PY4kJlbZxiDZmZBdZDETl/trQXYezGGK5vZgZa+HNgtt1ycHl0WqESzyyE:rgZOZmlGNZJ+ytLdKyyT20dX1o9Fn

MD5:	67A995C0B4C431BE506625F3674DC621
SHA1:	72C43092973661CA8E5225749EA6CD9CFC3423DC
SHA-256:	4BEA02228E8CA0854826D6A3BB0D8DC5E6F2828B344AEF8E2B811D06F8EB67AA
SHA-512:	9F85EF3E51C484C4B13484F04D3ECEA1CDF34ECE7DBB6BEF544DE63BD160FDE60360D76CC2B7509E07F5830FECA1829344597C21135FC5CF231B4FD2E92BA BD
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 59% • Antivirus: Virustotal, Detection: 71%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Pv.>%.>%.>%1.4%.>%Z.0%.>%..-%.>%.?%..>%1.5%.>%a.8% .>%1.:%.>%Rich.>%.....PE..L....xGQ.....!.....I.....@.....G..O....C..(....`..X.....p..... .....@.....text....*.....,..... ..`.rdata..._....@.....0.....@..@.data.....P.....8.....@....rsrc...X....`.....:.....@..@.reloc.....p.....>..... .....@..B.....

C:\Users\user\AppData\Local\Temp\natigezeholi.dll

Process:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17408
Entropy (8bit):	6.081723116162573
Encrypted:	false
SSDEEP:	192:MwPLlx5c4kJlbOxPDAE/mZBdZDEql+frQXYezGGK5vJgZa+HNgt/GI/x0mqESzyj:nsORXml/gDJuyt/RqyyuFX4o947Q
MD5:	F0C82EE96B56BF20D2B1CE93F7C0F941
SHA1:	432B3E4B9A1362D267630655DD44FEE58C49A2F0
SHA-256:	E6E1FA7A937C3CFA383C7A5CC5D1723E551A8AF62A03C7D8AF46504384D7993D
SHA-512:	0A342A87300C8BE6E1558A2729418A286F2770AE51960083289B25055659F27B3CC8870636660ECA67CC0C0A88D4E416B48B8ABFA0B709D434A953D6E59220D2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 78% • Antivirus: Virustotal, Detection: 76%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Xv.6%.6%.6%1.<%.6%Z.8%.6%..%%.6%.7%..6%1.=%.6%a.0% .6%1.2%.6%Rich.6%.....PE..L....GQ.....!.....N.....@.....F..O....C..(....`..`.....p..... .....@.....text....*.....,..... ..`.rdata..?....@.....0.....@..@.data.....P.....8.....@....rsrc...`....`.....:.....@..@.reloc..... ..p.....>.....@..B.....

C:\Users\user\AppData\Local\Temp\rikayolehofu.Xoc

Process:	C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	7.710087680990932
Encrypted:	false
SSDEEP:	384:1vPMrqX9DPfgkbWXqJNkNOYBNduseKKtCzkIPxOHPKRcadXpemop3gOrpNZ47vgJ:1vPeGDPfY6N8OYBNiwkIZcWcIpeXgqBJ
MD5:	45C8066C7A91E80794989C5BB03279CD
SHA1:	C16572FC6A2B7E5D2A5912CF175C9CDD7E4DDA78
SHA-256:	494A2F8CEB59B0A73B2CAE75A8016F1B5EED0355899A8FE27DE3ECF4856C89AC
SHA-512:	90136A41568E730749A954BD43D0EDBFE2BCFF53D67E16CF651830E1C028A5C866E0B462C88E67BDC627C8B016B56BDDC4794FF5BCF1F621A274A6007A244B A
Malicious:	false
Reputation:	low
Preview:	qFSQAWdD_VWGEq52460524eUAf\DUTVwY^AWLB0524605246`TF\qUAsFQCt2460524605\@R\Y.PZ\5246052460524`YGFAW\t^XYSpJ46052460524605 uQBd]@QWTv]ZBUMF4605246052_SB[WX...VXZ0524605246052460rW@u_X_UXTy[ZSq5246052460524qUAbFYStVPDUFA4605246052cDYAWdD_VWGE}P _[DI52460{FaX]TBb_UB}ReUVF]Y^52460524dDYhQD_xWYYBL24605246052g^\BSD_.Q^X605246052460524605`QEEXW`^BPSP60524605246|ZSPzYW@UDIt24605 246052460rW@{_QGXSv\^QxQXWu60524605246052460xh.635242052..05.4605246p52460524605246052460524605246052460.246>*.:6.<...1y..bX\A.FBZ UFW].QUX^ZF.TU.@AX.\\.r.f.YYTP.9;:.2460524.,...K...I...O..?W...M..PW...I..:P...H...M...K..V...O...H...M..;T...I..jI...H..dYVZ.K..24605246`p24z162...d24605246.5= 5=13246052h605246..246 524&0524v05"46072420524605646052460.2464524605046052$60%2460%24&052460%246052460520'05.4605.46.q24605246052 46052460524605246052460524605246052460524605246052460524605246052460524605"46.52460524605246052460524605246052.DTTFU60i4460%246852420524605246052 4v05r.RQAS460.?460.246>524:05246052460524v05..DCGQ460.v460.246v524,052460524605

C:\Users\user\AppData\Local\Temp\xuxokuxoka.dll

Process:	C:\Users\user\Desktop\Hu25VEa8Dr.exe

File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.080260047634796
Encrypted:	false
SSDEEP:	24:ev1GSqYDIuQyKxsq1X//oRVCR7tqU4xbaVZGy1Uua0wlqF4JNeS4G8Xq5S493Q00:qq4IBvsW/uTtx2OySuF30IN3T74
MD5:	81F429115E1AFD4A95DA0A8A73E4ACD1
SHA1:	520F4618A20E20E2ACC2382AF16CA244FE42B97E
SHA-256:	29D1AC834EDB48C1A75C90CF896EF27A53366BFECDEE7D65DDBB6621DC540200
SHA-512:	350994DB9C153E5CE2DD62D3C759378E0CD091F8FBD67E6D555FF34266C4BB5097FB376DC007D89EEDF939DA05BDBFFE00EF2A9A8EA2C0048C309702D1163619
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 67% • Antivirus: Virustotal, Detection: 67%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1.k.1.k.1.k..a.5.k.1.j.=.k..`.3.k...m.0.k..o.5.k.Rich1.k..... .....PE..L.....GQ.....!.....Q..... .....`.....!..M..., ..(....@.....P..P..... .,..... ....text..... ..`.rdata..M.... .....@..@.data...X....0.....@....rsrc.....@.....@..@.reloc.....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\yiduyevutog.dll

Process:	C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	2.9251612114551473
Encrypted:	false
SSDEEP:	24:ev1GSsGN+gg438JKANCE/mh7Vj3RotYU4sZfHtV1VdODXyIua0wJlRh1N7oRRC85:qsGtg43q3pgptgfHtA9uFmt/CCan+7
MD5:	E397A32C7C3ACA65A2A94D923F407B52
SHA1:	93C91BB1E8FDA9ECEC5A999BE0662A4E633D767F
SHA-256:	46B5B07EF3ADA0792C594D7FAAFF667DECF81E968908FADCD2F6020EACF400CD
SHA-512:	7BA018E72E51B78178E15A7BF940782815570D6D9A2E76A7C235877C5A447E3B8A91EF15E801D700D4857E0AA73589F526D34A8347D09A04A04F2D0AADE236A7
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 71% • Antivirus: Virustotal, Detection: 73%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....c.....Rich.....PE..L....xGQ.....!..... .....{..... .....`.....P!..N...4 ..<....@.....P..P..... ..4.....text..... ..`.rdata..... .....@..@.data...`....0.....@....rsrc.....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171

Process:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbWwWl:sZ
MD5:	3B7B4F5326139F48EFA0AAE509E2FE58
SHA1:	209A1CE7AF7FF28CCD52AE9C8A89DEE5F2C1D57A
SHA-256:	D47B073BF489AB75A26EBF82ABA0DAB7A484F83F8200AB85EBD57BED472022FC
SHA-512:	C99D99EA71E54629815099464A233E7617E4E118DD5B2A7A32CF41141CB9815DF47B0A40D1A9F89980C307596B53DD63F76DD52CF10EE21F47C635C5F68786B5
Malicious:	false
Reputation:	low
Preview:	.....user.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\R3PRUMZY.txt

Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	ASCII text
Category:	modified
Size (bytes):	99
Entropy (8bit):	4.623332970722682
Encrypted:	false
SSDEEP:	3:PfmYZLIRSzZfZJWEA1QWQRUvNxdQVeXvWA7dXviVPv:P+ILIR0lWn1QrmvN3A+Ngv
MD5:	CCF36D8632B95ACA87A55794AD9A3AF8
SHA1:	16586E00683427DC7C1090EDA5D575B103DDF8F1
SHA-256:	4A4EE293DAB048952EEC9CCDCECF457646FC7B4135CFAE76CB6ABD3C83E6C431
SHA-512:	5C3245D6B5110057BA3790184C3F26BC8F243F70456ED13A553521BCE2BAD7E4B46FE23631FD5CF6E04AF9B9660D5CAB7D0CCBC649A5B393F6B0E0368F66A2E8
Malicious:	false
Reputation:	low
Preview:	snkz.89.187.171.144.pe.suckmycocklameavindustry.in/.1536.1178451968.31320892.3507856880.31061020.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y4A6H5R0.txt

Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	157
Entropy (8bit):	4.591261443677953
Encrypted:	false
SSDEEP:	3:EngSc3dxZElO3dcYZLIRqTcTUJVecQVgVvXGOfZJWEA1QWQ7XiodQVeXvWA7dXvq:Egv3dxZEMcILIRqQYJ5QGFXZ/Wn1QrTs
MD5:	3931E58FFFBD0D2CF50ECFB0B0E77ACD
SHA1:	8D38511F7BA590D1F5F6482F83A6CB78F28065C5
SHA-256:	D5923F9CD92811609C2E5F53CB20FFC639A7480B4D5ECBC032A5826F5853DCF5
SHA-512:	EEB6205CA92955C3706215DB8942B2A3C3554BB7D3D6F171C4BDB2A944597609A2A5F7E3EB33E6CF5FA1DC1F155C3AC18CEC22419454AF9568CDD19DAB7D179
Malicious:	false
Reputation:	low
Preview:	btst.8894309f7f6b8698b45deaaa26bda18e|89.187.171.144|1696132900|1696132900|0|1|0.suckmycocklameavindustry.in/.9728.1178451968.31320892.3507856880.31061020.*.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.67760121359675
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Hu25VEa8Dr.exe
File size:	196'227 bytes
MD5:	bc76bd7b332aa8f6aedbb8e11b7ba9b6
SHA1:	c6858031315a50ec87e37966291ec69b64600efb
SHA256:	9535a9bb1ae8f620d7cbd7d9f5c20336b0fd2c78d1a7d892d76e4652dd8b2be7
SHA512:	c74a8a893d0d91ef9423c75c14e701102f01d46b4638d7e3184c95bfd4ff29f9cab71fe5de45e8e201dcdb8df77e952a18e32bfed5014b9c8155c189825f37e9
SSDEEP:	3072:ugXdZt9P6D3XJ3TCM/vosUE2L/TLqtAyD2XXhtksIae31fXJHhKgzyJtdeV:ue34p/vr6yrC2sJe35ZBKg0dW
TLSH:	6B14024364F582BFD6820432D5B92B79D77BCD8D438A7A470B447F21BA318D3C909E8A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....^.....

File Icon

Icon Hash:	9270c4ccc6741c42

Static PE Info

General

Entrypoint:	0x4030fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3CC [Sat Dec 5 22:50:52 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409160h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h
call dword ptr [004070B0h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [0042EC18h], eax
call 00007FEEC5176316h
mov dword ptr [0042EB64h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 00428F98h
call dword ptr [00407158h]
push 00409154h
push 0042E360h
call 00007FEEC5175FC9h
call dword ptr [004070ACh]
mov edi, 00434000h
push eax
push edi
call 00007FEEC5175FB7h
push ebx

Instruction
call dword ptr [0040710Ch]
cmp byte ptr [00434000h], 00000022h
mov dword ptr [0042EB60h], eax
mov eax, edi
jne 00007FEEC517372Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00434001h
push dword ptr [esp+14h]
push eax
call 00007FEEC5175AAAh
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007FEEC5173785h
cmp cl, 00000020h
jne 00007FEEC5173728h
inc eax
cmp byte ptr [eax], 00000020h
je 00007FEEC517371Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74b0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x37000	0x43f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x28c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c4c	0x5e00	False	0.6697140957446809	data	6.440105549497952	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.43359375	data	5.046835307909969	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c58	0x400	False	0.5849609375	data	4.801003752715384	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x37000	0x43f8	0x4400	False	0.16670496323529413	data	2.6375067972964095	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x37238	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States	0.09076763485477178
RT_ICON	0x397e0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States	0.14118198874296436
RT_ICON	0x3a888	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States	0.3891843971631206
RT_DIALOG	0x3acf0	0x100	data	English	United States	0.5234375
RT_DIALOG	0x3adf0	0x11c	data	English	United States	0.6056338028169014
RT_DIALOG	0x3af10	0x60	data	English	United States	0.7291666666666666
RT_GROUP_ICON	0x3af70	0x30	data	English	United States	0.8541666666666666
RT_VERSION	0x3afa0	0x184	MS Windows COFF Alpha object file	English	United States	0.5463917525773195
RT_MANIFEST	0x3b128	0x2cc	XML 1.0 document, ASCII text, with very long lines (716), with no line terminators	English	United States	0.5656424581005587

Imports

DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetTickCount, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, GetWindowsDirectoryA, SetFileTime, GetCommandLineA, SetErrorMode, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, GetVersion, CloseHandle, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, GetTempPathA
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, DestroyWindow, CreateDialogParamA, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
147.75.61.38192.168.2.22 80491662031515 10/01/23-06:01:37.455932	TCP	2031515	ET TROJAN Known Sinkhole Response Kryptos Logic	80	49166	147.75.61.38	192.168.2.22

Network Port Distribution

Total Packets: 19

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2023 06:01:37.211152077 CEST	49166	80	192.168.2.22	147.75.61.38
Oct 1, 2023 06:01:37.333363056 CEST	80	49166	147.75.61.38	192.168.2.22
Oct 1, 2023 06:01:37.333457947 CEST	49166	80	192.168.2.22	147.75.61.38
Oct 1, 2023 06:01:37.333792925 CEST	49166	80	192.168.2.22	147.75.61.38
Oct 1, 2023 06:01:37.455874920 CEST	80	49166	147.75.61.38	192.168.2.22
Oct 1, 2023 06:01:37.455931902 CEST	80	49166	147.75.61.38	192.168.2.22
Oct 1, 2023 06:01:37.455969095 CEST	80	49166	147.75.61.38	192.168.2.22
Oct 1, 2023 06:01:37.455986977 CEST	49166	80	192.168.2.22	147.75.61.38
Oct 1, 2023 06:01:37.456039906 CEST	49166	80	192.168.2.22	147.75.61.38
Oct 1, 2023 06:01:37.456289053 CEST	49166	80	192.168.2.22	147.75.61.38
Oct 1, 2023 06:01:37.578176022 CEST	80	49166	147.75.61.38	192.168.2.22
Oct 1, 2023 06:01:37.578208923 CEST	80	49166	147.75.61.38	192.168.2.22
Oct 1, 2023 06:01:37.578372002 CEST	80	49166	147.75.61.38	192.168.2.22
Oct 1, 2023 06:01:40.038088083 CEST	49167	80	192.168.2.22	34.29.71.138
Oct 1, 2023 06:01:40.212160110 CEST	80	49167	34.29.71.138	192.168.2.22
Oct 1, 2023 06:01:40.212265968 CEST	49167	80	192.168.2.22	34.29.71.138
Oct 1, 2023 06:01:40.212869883 CEST	49167	80	192.168.2.22	34.29.71.138
Oct 1, 2023 06:01:40.386900902 CEST	80	49167	34.29.71.138	192.168.2.22
Oct 1, 2023 06:01:40.386976957 CEST	80	49167	34.29.71.138	192.168.2.22
Oct 1, 2023 06:01:40.387012005 CEST	80	49167	34.29.71.138	192.168.2.22
Oct 1, 2023 06:01:40.387048006 CEST	49167	80	192.168.2.22	34.29.71.138
Oct 1, 2023 06:01:40.387104034 CEST	49167	80	192.168.2.22	34.29.71.138
Oct 1, 2023 06:01:40.404280901 CEST	49167	80	192.168.2.22	34.29.71.138
Oct 1, 2023 06:01:40.619858027 CEST	80	49167	34.29.71.138	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2023 06:01:20.029628992 CEST	138	138	192.168.2.22	192.168.2.255
Oct 1, 2023 06:01:37.098201990 CEST	57894	53	192.168.2.22	8.8.4.4
Oct 1, 2023 06:01:37.210273027 CEST	53	57894	8.8.4.4	192.168.2.22
Oct 1, 2023 06:01:37.456758976 CEST	57895	53	192.168.2.22	8.8.4.4
Oct 1, 2023 06:01:37.855343103 CEST	54821	53	192.168.2.22	8.8.8.8
Oct 1, 2023 06:01:38.076950073 CEST	53	57895	8.8.4.4	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2023 06:01:38.080461025 CEST	54719	53	192.168.2.22	8.8.8.8
Oct 1, 2023 06:01:38.604868889 CEST	53	54719	8.8.8.8	192.168.2.22
Oct 1, 2023 06:01:38.610348940 CEST	49881	53	192.168.2.22	8.8.8.8
Oct 1, 2023 06:01:38.857579947 CEST	54821	53	192.168.2.22	8.8.8.8
Oct 1, 2023 06:01:39.133213043 CEST	53	49881	8.8.8.8	192.168.2.22
Oct 1, 2023 06:01:39.134609938 CEST	137	137	192.168.2.22	192.168.2.255
Oct 1, 2023 06:01:39.871609926 CEST	54821	53	192.168.2.22	8.8.8.8
Oct 1, 2023 06:01:39.887109041 CEST	137	137	192.168.2.22	192.168.2.255
Oct 1, 2023 06:01:40.016741037 CEST	53	54821	8.8.8.8	192.168.2.22
Oct 1, 2023 06:01:40.026393890 CEST	53	54821	8.8.8.8	192.168.2.22
Oct 1, 2023 06:01:40.651536942 CEST	137	137	192.168.2.22	192.168.2.255
Oct 1, 2023 06:01:43.965873003 CEST	53	54821	8.8.8.8	192.168.2.22
Oct 1, 2023 06:03:19.729870081 CEST	138	138	192.168.2.22	192.168.2.255

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Oct 1, 2023 06:01:40.026474953 CEST	192.168.2.22	8.8.8.8	d024	(Port unreachable)	Destination Unreachable
Oct 1, 2023 06:01:43.965990067 CEST	192.168.2.22	8.8.8.8	d014	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 1, 2023 06:01:37.098201990 CEST	192.168.2.22	8.8.4.4	0x1234	Standard query (0)	xdqzpbcgrvkj.ru	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:37.456758976 CEST	192.168.2.22	8.8.4.4	0x1234	Standard query (0)	anam0rph.su	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:37.855343103 CEST	192.168.2.22	8.8.8.8	0xb02d	Standard query (0)	pe.suckmyc ocklameavi ndustry.in	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:38.080461025 CEST	192.168.2.22	8.8.8.8	0x82e1	Standard query (0)	anam0rph.su	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:38.610348940 CEST	192.168.2.22	8.8.8.8	0x2610	Standard query (0)	anam0rph.su	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:38.857579947 CEST	192.168.2.22	8.8.8.8	0xb02d	Standard query (0)	pe.suckmyc ocklameavi ndustry.in	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:39.871609926 CEST	192.168.2.22	8.8.8.8	0xb02d	Standard query (0)	pe.suckmyc ocklameavi ndustry.in	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
Oct 1, 2023 06:01:37.210273027 CEST	8.8.4.4	192.168.2.22	0x1234	No error (0)	xdqzpbcgrv kj.ru		147.75.61.38	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:37.210273027 CEST	8.8.4.4	192.168.2.22	0x1234	No error (0)	xdqzpbcgrv kj.ru		147.75.63.87	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:38.076950073 CEST	8.8.4.4	192.168.2.22	0x1234	Server failure (2)	anam0rph.su	none	none	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:38.604868889 CEST	8.8.8.8	192.168.2.22	0x82e1	Server failure (2)	anam0rph.su	none	none	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:39.133213043 CEST	8.8.8.8	192.168.2.22	0x2610	Server failure (2)	anam0rph.su	none	none	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:40.016741037 CEST	8.8.8.8	192.168.2.22	0xb02d	No error (0)	pe.suckmyc ocklameavi ndustry.in		34.29.71.138	A (IP address)	IN (0x0001)	false
Oct 1, 2023 06:01:40.026393890 CEST	8.8.8.8	192.168.2.22	0xb02d	No error (0)	pe.suckmyc ocklameavi ndustry.in		34.29.71.138	A (IP address)	IN (0x0001)	false

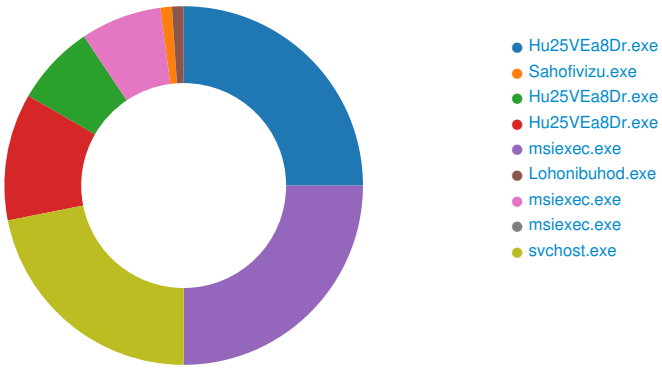
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 1, 2023 06:01:43.965873003 CEST	8.8.8.8	192.168.2.22	0xb02d	Server failure (2)	pe.suckmycocklameavindustry.in	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- xdqzpbcgrvkj.ru
- pe.suckmycocklameavindustry.in

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Hu25VEa8Dr.exe PID: **2948**, Parent PID: **1244**

General

Target ID:	0
Start time:	06:01:19
Start date:	01/10/2023
Path:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
Imagebase:	0x400000
File size:	196'227 bytes
MD5 hash:	BC76BD7B332AA8F6AEDBB8E11B7BA9B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Analysis Process: Sahofivizu.exe PID: **920**, Parent PID: **2948**

General

Target ID:	2
Start time:	06:01:19
Start date:	01/10/2023
Path:	C:\Users\user\AppData\Local\Temp\Sahofivizu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Sahofivizu.exe" "C:\Users\user\Desktop\Hu25VEa8Dr.exe
Imagebase:	0x400000
File size:	20'480 bytes
MD5 hash:	7FE00CC4EA8429629AC0AC610DB51993
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 57%, ReversingLabs • Detection: 61%, Virustotal, Browse
Reputation:	low
Has exited:	true

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Yumicebivud.rih	unknown	131072	success or wait	1	40147E	fread

Analysis Process: Hu25VEa8Dr.exe PID: **1724**, Parent PID: **920**

General

Target ID:	3
Start time:	06:01:24
Start date:	01/10/2023
Path:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
Imagebase:	0x400000
File size:	196'227 bytes
MD5 hash:	BC76BD7B332AA8F6AEDBB8E11B7BA9B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\{74865409-33C7-4D66-B1BE-5AF1BAA53947}	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4028E8	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Sahofivizu.exe	success or wait	1	402A67	DeleteFileA
C:\Users\user\AppData\Local\Temp\Zojemilocan.dll	success or wait	1	402A87	DeleteFileA
C:\Users\user\AppData\Local\Temp\Gozekeneka.dll	success or wait	1	402AA7	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\natigezeholi.dll	success or wait	1	402AC7	DeleteFileA
C:\Users\user\AppData\Local\Temp\xuxokuxoka.dll	success or wait	1	402AE7	DeleteFileA
C:\Users\user\AppData\Local\Temp\Yumicebivud.rih	success or wait	1	402B07	DeleteFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Hu25VEa8Dr.exe PID: **2092**, Parent PID: **1724**

General

Target ID:	4
Start time:	06:01:24
Start date:	01/10/2023
Path:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Hu25VEa8Dr.exe
Imagebase:	0x400000
File size:	196'227 bytes
MD5 hash:	BC76BD7B332AA8F6AEDBB8E11B7BA9B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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\MSI	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4016F7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40172C	CreateFileW
C:\Users\user\AppData\Local\Temp\0BBFF.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	401407	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\0BBFF.tmp\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert	success or wait	1	40141D	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0BBFF.tmp	success or wait	1	4014DF	DeleteFileW

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:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	0	88209	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 fd fd 3a 75 fd fd 69 75 fd fd 69 75 fd fd 69 fd b5 69 77 fd fd 69 75 fd fd 69 fd fd fd 69 fd b7 69 64 fd fd 69 21 fd fd 69 7f fd fd 69 fd fd fd 69 74 fd fd 69 52 69 63 68 75 fd fd 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 1a 4b 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 5e 00 00 00 fd 02 00 00 04 00	MZ@!L!This program cannot be run in DOS mode.$1:uiuiuiiwiuii idi!iiitiRichuiPELK^	success or wait	1	401747	WriteFile
C:\Users\user\AppData\Local\Temp\0BBFF.tmp	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 fd fd 3a 75 fd fd 69 75 fd fd 69 75 fd fd 69 fd b5 69 77 fd fd 69 75 fd fd 69 fd fd fd 69 fd b7 69 64 fd fd 69 21 fd fd 69 7f fd fd 69 fd fd fd 69 74 fd fd 69 52 69 63 68 75 fd fd 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 1a 4b 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 5e 00 00 00 fd 02 00 00 04 00	MZ@!L!This program cannot be run in DOS mode.$1:uiuiuiiwiuii idi!iiitiRichuiPELK^	success or wait	3	40141D	CopyFileW
C:\Users\user\AppData\Local\Temp\0BBFF.tmp:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	40141D	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0BBFF.tmp	unknown	196227	success or wait	1	401474	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft	00E35EEE	binary	50 4B 03 04 00 EC 00 00 01 71 00 00 D6 AD DB CD 9E C6 FC 27 21 0D ED 66 F7 28 A4 AC 2D 46 26 DB 6D F1 5C 58 C2 96 AB C2 37 59 25 77 2C E6 A3 81 85 3C 3A 83 59 FA 9F 4A F5 AA 11 92 C5 FD DE 4A E1 CE A8 87 4B 71 71 27 13 E3 F3 6F FF 10 2A	success or wait	1	401327	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			44 C5 6A D8 39 A0 66 EC 15 97 5E 9D FC F6 7E FE 18 43 F6 39 76 5B DF 7D 80 44 1F 53 03 1D 42 39 B7 4D 6E F1 6F 37 08 17 E2 A1 DC 23 43 5D 0F 42 21 C4 D7 0F DB 07 3C 74 FD 77 70 F5 EF 71 B0 C5 6A 30 54 BD D3 3C 63 43 92 08 14 93 C8 3E 6C 2A 32 B8 51 FC 46 37 BA F4 A0 E9 9E 6E 8D DD 42 75 EB 52 9F 4D A3 20 A1 52 A3 05 D7 A3 FD 30 02 04 EB F1 CD CC F8 E0 AF B0 10 A0 8D CD 21 CB 09 2F BD 4F D2 FA F6 32 9A ED DC DD 02 DC C5 DC DF DB 0D F1 93 5A C3 43 45 4D 20 15 83 4D 1B 61 FC AE 0A 70 04 17 C2 E6 58 41 B3 5B 4F 90 29 23 2B 14 F9 C9 3E B0 01 FD 44 1A 32 EA B2 5D EC 93 0A 97 86 4F 6D AE F1 96 E5 94 B4 AD 32 07 33 11 E8 44 7F A0 6E 12 0D 13 65 83 4E CE 84 C1 04 34 E4 B8 C3 C7 46 A0 D2 42 6C 1E 21 C3 BF 3E 95 BC 8F CF 18 52 EF 35 11 53 BA CE CD 56 DC BD C7 E6 34 47 30 70 85 2B 15 09 33 4B 5E E7 9C 49 41 76 D7 88 80 8F E3 9C 68 7B 2A E1 3E FE 35 3F A5 A5 13 BB 06 A3 A6 E4 6C 8D 7E 7F EF F8 68 73 10 EA D5 EB 57 DE 1C F8 46 5B 9A 72 6E C6 9E DA 59 07 85 06 D1 51 78 C6 F1 6F 96 44 59 72 44 36 6D 58 73 CC 95 73 57 FC 34 52 68 E4 1E 5C 68 EB AA 1F 4E 5B F2 72 CD DF 60 5D 40 75 EA C4 0D 2F 75 54 0B 00 72 5F 2A 1E DD 36 EB 90 CF 12 F3 03 65 9F E0 4C FE 5E 3C 40 31 BE 1B 25 12 86 E9 5A 9D 68 C0 C0 F9 C6 A2 B1 7C 26 B2 F3 DE 93 7B 41 3C 80 4D AF F9 F7 36 C2 63 F1 E1 48 5F 74 71 78 A9 D8 CB 05 D6 11 F6 94 22 6A 15 89 41 5A 69 FE 0C 76 33 AE CC 96 A1 78 E7 B3 81 BC 32 05 D2 B6 73 1A 7B 23 D8 E4 24 AB D0 01 38 B8 13 96 8B DD EA 3C 70 63 03 C2 9D DF AD 56 62 8A BB 9F B5 C7 31 84 78 E2 11 71 6E B3 EE C6 CF CB CF 88 B5 F0 B3 74 F6 21 5E 60 0B A4 5A BF 79 AA 67 E2 42 D5 59 BD 85 57 45 91 25 D0 3C 74 6C 64 00 AE 55 F7 6F 6B 06 07 56 E3 66 CA 0C A3 A3 85 EB 65 30 15 7A 33 4A 7C 14 40 0C 3C 10 B5 6C 17 78 91 48 51 BA 41 E2 B1 A6 E9 2C 3B 1A E5 D6 04 B1 74 26 87 D2 DC 63 88 B5 D5 00 F1 8C F6 63 39 71 05 69 7C 2D 51 52 9F 2B B3 5D 9A 57 04 32 E5 30 08 ED 33 2B DE D8 01 E5 53 4B CB 5A B6 5B 4A C6 F1 D0 16 F4 C6 F0 B0 27 68 24 DB EB 4E 49 E4 EF A4 63 A3 59 03 2A CB 27 41 DD 29 B1 DB 96 52 AA 39 46 17 6D 4B E5 B3 0D F4 0D EA 8C 94 29 2A 7B 19 09 2D 2B 75 18 B5 3C C4 4A AB 45 D6 9B 65 9A 98 74 65 CD 13 72 68 16 11 1F 7E 2D 61 0F 9F 87 3A 83 0E 68 5B 02 AC AA 12 08 B2 A4 4C FE 8D 24 3D 91 BD 24 A5 0C C8 15 CE ED F0 D3 8B 19 82 EB 73 84 5D 50 7B D0 74 68 23 29 EF CC 4F C1 9D D5 D1 98 8C F0 F0 E4 C3 CA 46 14 A1 9E FD 83 FB 7A AE D8 7B F1 31 C2 49 5F C9 B0 8B F5 A6 99 CA 39 AF 48 0D 19 DF 4B 33 D3 ED B0 17 EA 3A A4 D1 14 24 EA 74 89 09 1F 74 61 FE 6A E7 B2 F6 BA 34 E1 26 37 41 5C 55 79 1E 62 45 8A 99 2C A3 95 2E 3C 50 76 65 C0 B6 3B 85 24 D0 7A A2 47 94 D1 F9 06 EE 10 85 4B 6B 0A 97 77 0A 5A 58 9F C4 D8 EC 5D 56 0B 2B 1B 31 43 B9 3A E2 CF 08 A2 F3 C7 49 1F 6A 23 AC 01 D6 5F FD F8 DB D2 E9 97 E4 A6 2F 11 A1 02 91 FD DB F2 34 28 58 E0 1F CA 36 EA 38 D2 C5 C8 70 81 01 F7 AF 25 CF 08 19 37 95 6D DE 1A 76 31 52 5B 8D 7D 9B 37 56 1E B9 95 69 AB 00 FC 01 33 AF 38 C3 15 F7 A5 99 A0 30 79 9E 64 08 D2 E3 F5 A0 A3 0F E2 09 AE CB 4C 2C 4C 54 A6 A0 01 2C F9 00 AC 0E 32 20 E2 AD 90 D3 95 D0 99 79 A8 8A 78 21 46 1E 3F 3E C1 B4 AF E6 4D C1 B4 42 9D 2B AE 2F 69				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			75 B9 12 6B CD F5 E3 64 D3 13 8A 1A 11 29 A4 09 C2 7C 4E AD 3B 67 AD 37 55 0E 0A B3 85 F5 B2 57 56 C2 AB 69 C5 3D 16 2F FA 2F 40 DE 42 C8 6B E8 3A 09 39 A3 3A C2 DA 6E 97 4F 5A 46 00 90 A9 8A 63 27 6B 36 9D 7E 64 4C F3 76 0D 1D 8A F1 AA B4 43 82 34 6A BD 67 59 81 A4 ED 16 AE C9 0B 84 0A 84 A9 2D D9 D9 96 9E 19 49 AD E1 55 48 55 6F DE 58 1E 83 4C AC 3C DD 98 43 E9 95 3E DE A5 22 68 2A A6 C5 AF A5 6A B7 37 42 0F 30 8D EC F2 F6 0D 86 7F 5C D9 60 AE 6B 48 2C 9E 42 1D 9A 8F A4 CE 77 40 C6 52 C9 F7 D7 21 69 7D AD 74 A3 CE ED CC 33 8D A9 62 5E 3A 25 85 CE DF 32 B4 3B 0C 92 D6 F1 C2 C1 CA 31 95 72 B5 AC CF 4C F0 78 08 B9 AF BB 7B 7E 61 9D 68 BF 3A 32 F3 FD 35 4F 71 F2 48 61 70 D7 7C 9C C2 88 EC A3 0B F3 6E 6F 53 30 6C 39 97 5A FF 44 A5 F5 E1 E3 51 A4 D9 89 19 13 C7 04 71 A2 63 A4 3D FA 00 EC 6C 20 BA 71 B6 20 13 95 16 9B 04 CB 91 80 8B 27 DC 6E 77 CA F3 E5 5B 71 52 1C 66 05 D1 12 40 18 30 EF 4D CF 61 37 37 9A 48 40 B4 AF D4 CD A0 E8 F0 6B 6A B4 27 6D FA 3D BA C5 AE 07 7A 35 FE 55 A0 EA C1 ED 5C 6D E9 8F 06 4D BB 09 8D 00 46 6F 25 28 C4 4E 2B 16 99 FC 89 A0 65 AB 2F 22 BE 5D 3B 3E 00 87 A5 A6 68 72 6C 40 9D 93 E1 15 01 B5 FB C7 50 D3 B1 F4 37 51 EE 01 60 4A FB 82 E3 1E 92 7F A0 09 FA 34 62 E1 7E 64 7E 1F 11 20 DA 1E C1 FB ED C7 95 D9 CA C0 8F A6 15 68 65 B6 90 87 73 E8 4F 73 FE 15 08 C0 9E 83 81 78 5E 9E 5B 31 39 9B 49 B1 CB 30 B1 65 E5 29 D1 1D C2 36 60 F9 9F B4 1E 22 44 E3 D9 DF F8 85 EE 79 88 38 A5 A5 C6 54 89 DB 1F BF EA 37 62 A5 1A 08 DA 4D C3 42 12 C6 94 66 11 52 D8 62 B7 BD 80 A7 31 3A 02 7A C3 35 CF 55 82 FF 65 5E 21 F4 AF 61 F0 E7 01 67 C1 BD 10 1E 3A B4 18 7C 96 99 2A 02 F6 F2 DD A5 13 0D 2B 50 79 03 E6 F6 89 DB 20 0C D8 29 A2 F6 77 57 60 A4 2E 89 16 A4 EE 71 0A F3 9E 44 04 4C 9C 31 80 8E F5 64 E7 D3 E9 3F 3B FB 2E A4 B3 05 5A A6 DA 2F 83 C3 D7 2A CA 80 8E E7 B7 91 29 D7 D6 57 5C 30 A1 32 40 00 D0 66 98 E7 0D 69 45 CE 3C 71 F0 F6 E3 9C 95 0E D1 7D D5 01 A8 8C 4B 0B 52 01 DE C4 69 27 F7 08 F9 C1 43 A8 10 B1 20 83 91 96 1E E7 18 2F D3 0B 76 5D 50 24 44 E0 76 1C 9F 32 53 7C A8 BE 42 0E 0F F3 D8 FE 59 69 9C 12 5E 82 A3 0C F7 E2 15 9F 44 38 70 5C 43 7E 38 2F 2E 9F 9C E7 97 E6 23 66 DD D3 47 1F B7 8D 73 87 80 AE 20 C5 7F 13 15 7A 1C F8 FC 77 2F 9E 44 D9 4E 3B 72 E7 E6 79 64 C0 91 58 44 F9 6B 0F 1B 1E E7 89 65 C9 75 83 72 6B E1 5A E3 4E 02 D7 2B 2A 95 DE 29 4B AD 76 95 93 4A C2 E1 AD 81 DD C8 72 0A B7 D7 3A CF C3 1A 42 17 F2 A7 11 75 AA 21 DF 6B 03 D9 4E DF AF E6 6E E8 CA C1 36 27 6B 3A B2 5C 5B E7 0F 52 37 A9 38 54 C1 3A 81 7D 4F 1B BE DB 49 1A 90 1E 04 B6 64 7F B1 5C 09 6D 4B C2 CF 1E E1 42 C1 B1 27 6A 8A C9 4D 15 9F E7 34 97 A0 F1 E2 BE 7B 8E 24 E7 84 4D 46 C0 FF 2E FA C4 94 0E 49 F6 89 57 E3 11 6E BD 58 BA E1 E6 4A C2 3B 44 17 2D 65 1A 5D 2B 94 1F A8 02 8A 35 81 F7 D5 5C 4C EC B8 E8 49 BE FD AB 0B F8 A5 7D 9C FC 95 76 05 FD F8 B5 E8 03 45 40 92 75 F2 40 97 DE 50 E9 2D 98 E6 07 5F 5B 95 8A 59 96 B5 EF 7F 4F 03 A4 21 2B EA B3 A4 B8 18 F8 6A E3 14 5C 3D 55 9C 9C 55 9B 40 53 D1 A2 A6 47 E7 48 D5 F9 69 96 F4 9B 02 F2 16 A9 71 DC 76 7D 91 5D E3 ED 59 BD 63 42 DB FA C7 34 86 E0 F3 04 E7 92 4F 6D 2A 11 17 17 75 CE F7 06 EF 7B 6D 86 ED A4 93 34				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			A3 B6 86 AF E7 11 C7 32 CA B3 30 84 47 26 1A 64 21 B0 AB F9 C2 62 6A CC 1F 47 EF 25 D9 E2 96 89 10 8C C5 E2 60 CE CD 5E 0D 8C 30 7F 05 F5 11 F4 A3 CC 37 DE BC F2 BF 90 0D C7 CE F6 81 06 E5 62 53 CC C8 CA 30 5A 85 3E 66 04 05 B6 95 A4 A7 8D E9 6A AD 80 0F B8 C8 3B B1 15 0C EE CB AB 52 FD 26 5E CF 26 5A EF A9 C7 20 E6 7D D1 06 96 75 30 19 F2 64 44 64 28 E6 7D D7 B5 88 F1 B3 12 58 D7 05 60 3A 28 32 E1 D5 35 76 7A 73 90 6D 52 87 03 1E 34 6A 18 40 83 80 11 DE 02 A6 9C C7 09 E1 A3 85 3C E0 16 7D 05 94 B0 0F 3E 78 10 93 B6 7D 56 99 66 A2 D3 5B 95 7A 6A 19 E1 6A 15 78 BC 05 D9 3A 52 93 66 3B 6C 72 AA A9 FE 0B 8C 37 01 B2 1C A0 69 43 0F 49 2C 8A 55 35 2B 3D 0C DC E0 81 1C 5B 57 BA 33 F7 28 23 AB CA FF 45 55 12 82 95 85 AB 7C B2 8B 6F C8 39 42 24 50 A4 FD 7C 71 F1 7A BE 54 94 CA 76 CA FF 14 BE 68 29 C4 6A 83 96 07 90 7B 17 08 C5 7A A3 E2 DE 21 23 CD 11 38 A0 C3 6D BD 71 DB 48 CF 27 04 75 4A 8F 4B FB 04 F8 54 D5 AF 5A EE 2C E7 01 31 6F A0 42 39 DE A5 5A 2F B8 1A 19 58 F1 38 8F 97 5E 55 00 04 9B 36 1A B7 6B 24 93 BB 67 1E 6D 09 F8 CA DF A8 2B 94 73 A1 00 22 80 7A C7 50 E4 B6 0C C5 A5 13 75 70 F7 82 63 EE 28 D4 81 F7 42 85 73 5B 8E C4 2B 36 63 B0 A8 40 01 04 8A 31 9E F4 17 C8 6F 5F 64 C4 6F 86 36 B8 A2 D4 05 EB 9B C8 8E 3C 21 EA DB 88 B1 58 D9 00 5B 80 DD 8A FD 8C 4C 24 B2 A0 C4 8B 8B 2D 87 BF C3 F0 A7 4F A8 54 58 78 0D 36 C7 B2 38 34 F2 D7 67 31 0D C1 23 83 63 DA 36 BB 1D 44 17 2B 7C AB 26 09 06 21 42 41 13 7E 98 5E 3A 57 61 09 C4 C1 F9 BA 3B 1C 47 84 09 32 6A 77 70 72 FA 6F D8 53 6A E7 11 4B 3B D4 E2 58 7D 56 7F F7 AC 9E 37 FA C0 D2 7E 50 29 2D 1B A3 71 1C 3B E9 6A AB 95 B9 B7 00 EA 31 6A 7B C1 4B 2B D7 CF 6F 68 2F E2 95 1C D6 AC B6 A2 37 46 AA 3B 5E EB 84 67 68 AD 1F 32 25 4B 7E 80 14 99 25 6E A2 90 DA 22 FB 76 89 83 D9 89 45 77 C7 FE 5B 98 71 22 31 B1 53 CD 35 BC CE 1B FE 70 32 BC AC DB CE 9F 97 FC C8 61 35 FA 11 85 6A 5F FE B0 7B 59 0C 9B 2D EC C2 EC 6D EA 92 60 20 34 44 63 0D 5A 54 8E 68 E8 F8 B0 3C EB 00 9E 2E 39 2D 7E 23 92 A5 C5 C1 CE 87 07 EA 00 47 9B E1 96 B6 0F 12 AB 8A 39 6F F0 F4 F1 9F C6 F7 A1 4B E9 86 34 87 9B CA 20 A1 C7 8A BB 7F 67 32 7F 31 65 61 B0 A9 6F 8E 34 71 51 16 CB E8 AD 7D B4 4A 0A 11 38 96 AD 3E 76 A4 E4 00 8D D0 45 6B 94 7B B7 10 42 43 B6 EC CD 3A 31 82 D0 6F 09 3A 3B F5 28 9A F4 1F EF 92 23 FC AC 8E C4 87 20 BA 80 37 B7 94 3A 1C AC 88 C4 74 26 24 B2 EA 7F BA 17 08 E0 19 78 93 00 B3 8F 20 DC 7C FF 30 BA 33 04 75 08 02 A3 F2 F2 0A E9 A6 A5 5C E0 D3 FB 18 0F 4A 07 9D 41 BE C1 A5 15 B3 A2 81 22 06 E2 F9 CB 93 C0 3D 35 DA 7A 76 58 26 13 1C 81 88 11 09 90 CD 67 85 72 5C 5C 61 C2 E0 1C 4C 64 2E 99 69 DF B5 92 CC BF C6 8E E2 BE 95 A3 0C CF CF 3A B7 F3 49 EC 88 8A 7A B7 91 18 43 BD 4B C0 8E 71 65 8A DD 6C DE 19 84 B9 E2 7C 61 00 92 EA 32 53 52 C1 00 30 8A F7 4F E0 D1 40 A7 2D 83 31 27 C0 4C 9B 15 5D 27 01 CC AC A2 C9 90 54 1C 05 12 E2 6A 01 E4 88 EF 19 23 93 ED 6B AC 05 74 9C 13 4C 25 10 94 BD 6D C2 E4 5E A7 83 A9 98 6A 1A 7B 64 9D 25 87 57 27 81 1D F2 25 BD A5 6D D8 49 F1 FB 82 EF C5 8B 48 F3 48 C7 99 11 37 19 7F 07 D9 BE E9 5A 5B 84 3F AB 84 57 A6 60 80 F1 5E EC 48 CC B4 34 21 42 D2 26 7E 9D AB 30 CE A6 DE 96 B2 50 76 88 A4 EF E9 BB				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			[illegible] 3C 67 11 D4 B7 2F 51 7F 94 FA 36 1C D2 36 57 CC A0 A9 7E 86 0C AA C8 53 E7 41 EF F3 22 3C 67 2D 8D CE 85 21 97 F5 C2 A0 1E 25 E3 27 F5 C6 6F 93 7E D1 65 1C 09 90 E7 17 6D A7 0B 63 23 9F E2 EC 62 E7 5D AD 30 2A 1F 46 9E B4 F7 48 AB 90 F6 59 E1 ED DD B2 D5 41 DC 60 33 54 52 48 FB 9B A5 EE FD 94 7B 5D A3 AA 3B 19 55 9B F9 D4 8D E6 5D 48 F4 75 47 CF 87 7D 75 10 F6 A0 81 7B AB 94 C6 5C 14 64 86 79 E0 99 38 15 DC 1E C6 B0 05 D5 D8 7D EE 20 C1 9D E9 E5 F0 AE BE B1 10 F0 21 B7 8F 47 25 35 1C AF 20 A7 0F 8B 87 8A E5 BA F8 70 12 55 21 A6 F0 A4 64 C9 68 BA D6 68 03 3D 49 3B 0C B8 D9 80 D1 3E 05 3C C6 C6 62 6B AD E3 06 51 33 3A 33 83 22 A3 D2 21 B3 A9 8F 7F 71 FF F6 E0 70 40 A3 F4 6D 3C AC C6 40 7D 1F FB CA AD F3 3E 05 66 C4 53 3F BD E8 3E 02 15 8A 57 A9 3B C7 86 5C 8B 25 65 56 0F AA 5B 24 27 2B D5 2D 7E D8 CB 39 FD 47 98 C4 3B 16 30 A0 4C 6D D4 FE B9 2F CD 5F 0A 1E 81 F3 7B FA 26 77 8E 48 EB 02 1D E7 30 A5 A0 32 09 BD 11 2B 66 85 61 3C BE 1A FF CE 2C CC 42 05 F9 22 4B 43 DF C9 FC 80 9E 9A DD FF 43 3B 38 C3 19 9B 7B 4D 45 A9 6D 13 6F E8 3B C6 B7 6F 72 07 E7 15 95 F2 02 33 05 B0 AE 44 22 48 9C A4 E4 34 28 CD EC 29 9B 54 C8 BA 66 85 78 61 F6 28 41 88 43 27 A7 43 A9 6B 09 2D 8E 34 61 91 34 45 FC C2 D3 81 7C 8A B9 63 FC 48 93 B0 0A A9 3E 8D D0 E1 8B 30 D1 EC 63 65 46 61 0B D3 18 14 02 0D 51 D4 01 67 CF B9 0B 9B C7 D5 8E 52 09 0F DB 3A 1A FF B7 DA 6B 60 2A 92 C3 68 14 9E 90 A2 97 C6 64 1D 8C 3E B1 05 1B 28 53 E1 94 62 FC 63 F3 82 42 2A 5D D8 3E F3 D5 12 5B DA E7 AC B1 6E F0 77 A1 BA EE FA 96 23 A2 05 4C DC 50 9A 0C 58 8F 53 10 76 6E 67 41 E5 3C 86 4F E1 8F 59 7D 7C D9 2F AE 16 44 E8 D5 8E 65 57 1F 19 92 D5 F1 28 7E B4 5C 93 55 42 ED BB 6E 73 04 83 34 9B F4 AC 0A 02 3C 9F 6D 0C 3D 54 D6 19 C2 0D B5 DD C3 E5 76 8A CF 03 BC 74 0D 9F 41 6C 3A B0 79 41 73 F2 6A D9 4A AF B8 80 43 74 B9 04 7C F2 A6 EC 8F 91 32 A8 7E 85 C2 E6 1E AF 57 1A 25 B9 D1 4A 08 35 2D 18 F8 EA 9F 8B 49 40 7C 00 44 2B 25 EE 1A 18 B9 DD A0 5E 7A 45 D0 EA E0 1D 36 44 6D 67 99 8E 92 08 DA E5 6D 32 D3 AD 8F E2 14 E8 B3 51 30 E4 D4 DA 91 24 DD FD 12 13 76 2C B5 C7 F2 A6 75 50 DC 64 83 1D FE 87 2B 4C D9 BB 38 B0 2A 16 41 FD 13 37 8C E6 7F 0A FB 39 DB C0 71 E2 E2 F6 30 17 19 7D BA 0E 95 12 15 4C 9C 14 F0 1E 96 75 06 04 01 9B DC E5 7A D7 A7 FF BF 1E 45 5E EA 48 A3 BF B2 F0 56 B8 93 B3 BC B6 6E 60 CD 2F 0F 5E 80 67 77 25 0C 94 F5 19 E0 15 84 5E C0 56 0E 06 EE A6 7F 5F 59 AB 4E CC 27 A9 6B 20 51 02 FA F0 A5 53 1B 00 5F 05 F9 54 17 A8 AB B0 C9 AB C7 AE 61 A4 98 9D 76 3D 11 C4 3C 2A 29 3A 7B AC B9 8E BB 10 2F 85 1E 8F 72 9F 09 27 8E 9A 4B F6 10 54 AC FB 97 B2 EE 95 7C A5 BF A1 B0 1D B3 AF 4A 12 EA 14 21 67 51 1A 44 CF C8 6D 44 F5 CE 8A B0 C1 E2 2D E9 3D 68 54 64 FA 76 E7 EB 58 CD 9D 5E 7C BF 0E CF 02 17 1A E9 A8 49 D3 35 AC 8B 94 F5 C5 C1 80 26 69 33 40 A6 04 7E 2E 38 70 37 E5 71 23 E5 7F 18 E3 DD EE AF 87				
HKEY_CURRENT_USER\Software	ImageBase	binary	EC F9 AF 5F 22 5F 5F 5F 23 5F 5F 5F 5E 5E 5F 5F 97 5F 5F 5F 5F 5F 5F 5F 1F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 77 5F 5F 5F 2D 3E 99 2D 5F 93 28 6C 00 97 20 EB 6C 00 F3 C7 C8 D2 3F CF D1 CF C6 D1 C0	success or wait	1	4014B0	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			[illegible] [illegible] 3F C2 C0 CD CD CE D3 3F C1 C4 3F D1 D4 CD 3F C8 CD 3F E3 EE F2 3F CC CE C3 C4 0D 2C 2C 29 03 5F 5F 5F 5F 5F 5F 5F 10 97 A3 19 D4 78 49 C8 D4 78 49 C8 D4 78 49 C8 95 75 94 C8 D6 78 49 C8 D4 78 4A C8 4D 78 49 C8 95 75 96 C8 C3 78 49 C8 00 59 79 C8 DE 78 49 C8 91 7E 4B C8 D3 78 49 C8 F1 C8 C2 C7 D4 78 49 C8 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F EF E4 5F 5F EB 20 24 5F 6B 42 39 EA 5F 5F 5F 5F 5F 5F 5F 5F 7F 5F 2E 20 2A 20 25 5F 5F FD 5F 5F 5F A3 21 5F 5F 23 5F 5F 59 0F 5F 5F 5F 2F 5F 5F 5F CF 5F 5F 5F 5F 1F 5F 5F 2F 5F 5F 5F 21 5F 5F 23 5F 5F 5F 25 5F 5F 5F 23 5F 5F 5F 5F 5F 5F 5F 5F 9F 22 5F 5F 23 5F 5F 5F 5F 5F 5F 21 5F 5F DF 5F 5F 2F 5F 5F 2F 5F 5F 5F 5F 2F 5F 5F 2F 5F 5F 5F 5F 5F 5F 2F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 8F D3 5F 5F 93 5F 5F 5F 5F CF 22 5F 57 E2 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F CF 5F 5F AB 21 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 0D D3 C4 D7 D3 5F 5F 5F EB FB 5F 5F 5F 2F 5F 5F 5F FD 5F 5F 5F 23 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 3F 5F 5F FF 0D D1 C3 C0 D3 C0 5F 5F BB 31 5F 5F 5F CF 5F 5F 5F 33 5F 5F 5F C1 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 1F 5F 5F 1F 0D C3 C0 D3 C0 5F 5F 5F F7 FB 21 5F 5F AF 5F 5F 5F 23 5F 5F 5F D5 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 1F 5F 5F 9F 0D CD C3 C0 D3 C0 5F 5F 5F DF 5F 5F 5F 4F 21 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F DF 5F 5F 9F 0D D1 D2 D1 C2 5F 5F 5F 57 E2 5F 5F 5F CF 22 5F 5F E3 5F 5F 5F D9 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 1F 5F 5F 1F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F F4 AA 4B A2 4B FB A2 DC 2B 2E D3 0A A2 DC 2B E5 AA E4 33 D4 2C A2 E7 37 2F AA 2C C7 4A E1 5F A8 E7 23 EF 5E D4 2F 5E D4 2B 5E D4 27 5E 34 E7 D1 1F 5F 48 E1 20 5F 5F F2 F5 AA 14 CF 4A E1 5F AC [illegible]				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			E4 83 F6 EF 5E D4 27 5E 34 EB D1 1F 5F A2 C4 53 5F A8 E4 2B AC E4 43 EF 5E D4 27 5E 34 EF D1 1F 5F AA DC 4F A2 C4 4F 5F AA 3C E3 CF 1F 5F 48 DF 5F 5F 5F 2E 95 E5 F1 2E 95 F5 F5 2E 8E F4 47 AA 6E 0A EC 47 2E 8E 60 22 61 A8 EC 2F B8 56 5E 12 71 A9 4F 2E 95 E5 F0 2E 8E 60 2E 95 ED F4 2E 8E EC 47 22 60 AA 69 B8 56 5E 2E 95 F5 F3 2E 8E F4 47 A9 67 2E 95 E5 EF 2E 8E E4 2F 22 61 B8 56 5E 60 40 27 2E 95 9F 2A 67 AC E4 53 EF A8 EC 57 5E 34 E7 CF 1F 5F A2 E4 4F 23 A8 E4 33 EF AC E4 43 EF 5E D4 2B 5E 34 F3 D1 1F 5F 5E D4 33 5E 72 A2 E4 47 23 18 DC 47 2E AB D6 5E 5E 5E A2 DD F7 5E D3 C4 5E D5 13 5E 34 EB CF 1F 5F A4 9F A8 E4 33 D3 F4 AA DC 2B C9 20 F6 66 E4 43 2F 5F 5F 5F 66 E4 47 27 5F 5F 5F 5E 34 EF CF 1F 5F 5E D5 F7 F6 5E 34 F3 CF 1F 5F 5E D4 33 AA 14 F7 CF 1F 5F F6 5E 75 A8 E4 2B AC E4 43 C7 3F 27 5F 5F EF C9 5E C7 FF 42 E1 5F F6 5E 34 F7 D1 1F 5F 5E D4 2B F6 5E 75 5E D4 33 5E 72 AC E4 83 EF 5E D4 27 5E 34 FB D1 1F 5F FE FD 12 9F FA 68 61 2F 5F AA EB 03 23 80 A7 4A E1 5F AA 70 F2 C8 71 37 23 5F 5F F5 F6 AA F3 21 27 55 61 21 D3 EE AC D0 20 12 5E 1A 14 AB 4A E1 5F D2 E1 AA 6D C8 68 37 23 5F 5F AC E3 20 27 AA 27 55 60 21 D3 22 E6 4A 3D 55 60 23 D3 28 AA 6E EE A4 68 D3 3F 4A 2F 55 60 2F D4 2A AA 78 12 79 A2 42 20 12 78 A8 37 E5 24 37 23 5F 5F 1A 14 AB 4A E1 5F D1 69 FE FD FA 61 23 5F F4 AA 4B F0 F0 AA F4 27 F2 F5 AA 51 C8 55 37 23 5F 5F AA 3C A7 4A E1 5F 12 68 22 52 F6 A8 EC 5B A8 EC 57 AA E5 27 87 21 D3 2A 18 EC 2B D3 25 03 9D E1 A8 E5 27 1A 34 AB 4A E1 5F D2 E3 AA 61 C8 9F 37 23 5F 5F AC DB 37 27 AC E1 20 AA 2E 55 60 21 D3 29 C9 20 F1 47 84 5E 5E 5E AA 2E 55 60 23 D4 07 55 60 1F D3 22 5E E4 5B 55 60 20 D3 24 5E E4 5B 4A 22 5E E4 57 1A 24 AB 4A E1 5F AA 6F D1 9B 12 9F FE FD FA 68 61 27 5F A2 DC 5B 5F D3 52 A2 DC 57 5F D3 25 A2 ED 27 1F 4A 46 AA ED 27 DF 40 DE A2 68 20 A8 ED 27 4A 78 AA EB 03 23 80 A7 4A E1 5F F5 12 55 A2 58 3F D2 13 18 14 AB 4A E1 5F D5 0B AC EF 27 F6 AA 21 87 25 D4 31 12 5E E6 72 46 A4 D9 5B D3 23 2B 20 4A 21 03 5D A8 21 E5 A0 61 37 23 5F 5F 1A 14 AB 4A E1 5F D1 78 FE FD 61 23 5F F4 AA 4B A2 4B 2B 80 CF 4A E1 5F A2 C4 5B 5F F2 F5 24 B3 5F 5F 5F F6 AA 1C AB 4A E1 5F A8 E4 57 AA E4 57 12 7A 18 37 D3 EA 1A 7E D2 E4 AA 14 A7 4A E1 5F A2 65 27 AA 35 55 61 25 D4 07 AA E4 27 A4 9F D3 25 A2 1B B7 5F D3 3A AA EC 5B 12 9F 1F A2 41 20 72 7F AA ED 5B 02 67 AA 60 AA EC 5B 72 41 1A 61 D4 2A E2 A0 65 37 23 5F 5F 1A 7E D1 65 1A 7E D3 2C 5E E4 5B A2 E4 57 23 A2 DC 5B 3F D1 BE AA E4 5B FE FD FA 68 61 23 5F AA E3 03 23 A4 9F DC 30 1F 98 5F 4F E1 5F 60 7F 29 0A 67 F0 47 5C E4 5F 5F 61 23 5F F5 AA D3 03 27 4A C9 AA 65 AA 2C AF 4A E1 5F CA 9F 3B 22 60 A2 17 20 D3 FB EF 47 AB 5F 5F 5F 1C 5E 5E 5E DE D3 F4 EF 47 97 5E 5E 5E A4 9F D4 23 1F E5 4A 26 E7 AA 6D AA 4F 0A 60 A2 DB 03 2B 5F D3 0E 20 24 EB 42 E1 5F C9 5F 5E 14 13 42 E1 5F C7 0F D4 5F 5F 5E 14 EB 42 E1 5F 5E 34 0F D0 1F 5F EF C7 21 23 5F 5F 5E D3 03 37 5E 34 E3 D1 1F 5F A4 55 DC B1 12 9F FD 61 27 5F 97 5E 5E 5E DE 4A 54 AA E3 03 23 AA 2C CF 4A E1 5F C9 5F 5E D3 A0 CB 47 C8 5E 5E 5E 61 23 5F C7 DF BE 1F 5F 5E D3 03 27 47 D8 18 5F 5F 61 23 5F F4 AA 4B A0 4B 83 20 5F 5F 80				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			C7 4A E1 5F F2 F5 AA D4 27 F6 C9 26 F8 AC DC 77 A8 E4 6B 12 7A 52 84 AA E4 7B AA F4 7F AA 4F AA 59 60 45 29 98 5F 4F E1 5F A8 FC 5B 60 46 29 22 50 22 58 AC EC 7B A8 2C D7 BA 1F 5F AA EC 77 A2 60 5D A2 58 E0 2E A6 21 33 5F 5F 5E 03 AC BC 07 1F 5F F2 EF 47 32 18 5F 5F 48 D1 2C 5F 5F 5E 24 0B 42 E1 5F 18 FC 6B 2E A3 C2 2C 5F 5F F2 5E 34 57 D0 1F 5F 48 F6 2C 5F 5F EF 47 8F 5D 5E 5E E7 F2 EF 47 63 5D 5E 5E 48 6B 32 5F 5F F2 EF 47 78 17 5F 5F 48 94 32 5F 5F F2 47 5C 33 5F 5F A2 57 20 DE 22 12 9F 1F EF 5E 34 A7 CF 1F 5F 48 BA 32 5F 5F 5E D4 6B 5E 34 5B D0 1F 5F 48 AC 32 5F 5F 60 7F 21 18 FC 43 D4 01 AA A7 7F 4A E1 5F C9 20 A8 A7 3F 4B E1 5F 47 9F 33 5F 5F AA EC 7B A8 23 AC 7F 4A E1 5F 48 C2 32 5F 5F AA A7 3F 4B E1 5F A8 A7 7F 4A E1 5F 48 F1 32 5F 5F AA E4 43 AC 13 A4 7F 4A E1 5F 12 9F AA 2D 1A 6A 2E B3 9F 02 EC 47 AA E3 A4 7B A8 2D 48 1B 32 5F 5F 5E 13 B4 7F 4A E1 5F F5 48 6B 31 5F 5F AA 2C 0F 42 E1 5F AA 14 FF D1 1F 5F 1A 6A D3 26 F1 F0 5E 75 AA E4 7B AA 2C E3 42 E1 5F 1A 6A 2E A3 5E 31 5F 5F EF F0 5E 75 48 55 31 5F 5F C9 4F 47 F9 33 5F 5F 5E D4 7F EF 5E 34 A3 CF 1F 5F A4 9F 2E A4 7C 31 5F 5F 48 88 2F 5F 5F C9 4F 47 1B 33 5F 5F AA 57 F6 47 70 1E 5F 5F AA 4F 1A 52 D3 E1 C9 FB F5 47 F9 1E 5F 5F AA 4F F2 F6 A9 25 A7 3D A7 E4 2A 5E 34 DF CF 1F 5F A4 9F D4 3A 5E 34 DB CF 1F 5F 1C 96 5F 5F 5F D4 2A F6 5E 34 D7 CF 1F 5F 87 2F D4 22 5E E4 5B A9 E4 2A A7 25 E5 19 62 D4 9D 18 FC 7F D3 3D C9 45 47 2C 5D 5E 5E F6 C7 5F E7 E2 5F 47 4A E2 5F 5F F6 5E 34 D3 CF 1F 5F 48 FD 31 5F 5F C9 54 48 0F 2A 5F 5F F2 47 9B 32 5F 5F EF 47 66 E5 5F 5F 48 14 25 5F 5F C9 6F 47 89 32 5F 5F C9 7E AA 4F 47 80 32 5F 5F C9 32 AA 57 47 B7 32 5F 5F F6 F5 5E 34 CF CF 1F 5F A4 9F D3 26 C9 42 48 52 29 5F 5F 18 FC 43 2E A3 41 2E 5F 5F F5 47 A6 E5 5F 5F A4 9F 2E A3 73 2E 5F 5F F6 F5 47 6A 1F 5F 5F C9 43 48 6D 29 5F 5F F2 47 F9 32 5F 5F AA 4F AC E4 27 EF F6 C7 5F 23 5F 5F F5 5E 34 CB CF 1F 5F A4 9F D3 02 AA E4 27 1A 65 D5 04 17 37 D3 00 F5 47 E2 E5 5F 5F 1A 62 D3 2D A2 9F 0B EF 5E D4 27 47 17 E2 5F 5F 4A 28 66 E4 5B 20 5F 5F 5F A7 3E 18 FC 43 2E A4 82 30 5F 5F C7 5F 23 5F 5F F6 F6 5E 34 C7 CF 1F 5F 48 B0 30 5F 5F C9 5E 47 54 31 5F 5F AC EC 27 F0 F5 C7 5F 23 5F 5F F2 EF F2 5E 34 C3 CF 1F 5F A4 9F 2E A4 CE 30 5F 5F 48 2E 2E 5F 5F C9 4E 47 6D 31 5F 5F EF F5 47 42 1E 5F 5F 48 D1 5D 5E 5E C9 10 47 9A 31 5F 5F AA 4F AA E4 7B A2 7F 26 F5 A8 D4 57 A8 E4 27 47 3C 1D 5F 5F F5 9D DF BA 1F 5F A4 9F D3 27 F5 47 8C E1 5F 5F 4A 36 C7 5F E7 E2 5F F5 47 BF E1 5F 5F EF 47 AC 1C 5F 5F EF 47 8F E1 5F 5F F5 47 4F E3 5F 5F 9E DF 82 1F 5F A2 DC 27 22 DB 10 F5 47 D7 E4 5F 5F 12 68 1A 62 D3 2F AC EC 47 A2 9F 33 F0 EF 5E 34 FF CF 1F 5F AA 67 AA E4 27 A2 9F 5C 2C 5F 5F 5F DF 02 60 56 77 3A 9F 1F A8 E4 27 18 FC 27 D4 25 F5 47 5E 1D 5F 5F 12 9F A2 DC 27 20 2E B4 9F 1F EF C7 5F 5F 5F 1F F5 47 27 1E 5F 5F A2 57 5E A8 E4 6B D4 D5 18 FC 27 D4 F2 C7 5F 4F E1 5F F6 47 38 E1 5F 5F F5 C7 5F 4F E1 5F 47 2D E1 5F 5F 5E D4 4F C7 DF BE 1F 5F 47 02 E1 5F 5F F6 C7 5F 4F E1 5F 47 55 E0 5F 5F AA E4 7B 60 57 22 EF C7 DF BE 1F 5F 47 85 19 5F 5F A2 47 23 2E A3 F2 5E 5E 5E E7 D3 3A F5 C9 59 48 F6 5B 5E 5E 5E				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			D4 57 C9 41 47 C4 14 5F 5F A2 DC 27 21 48 F9 5C 5E 5E 5E 24 47 4A E1 5F 48 1A 2F 5F 5F 5E D4 57 C9 49 47 E6 14 5F 5F 5E 24 33 4B E1 5F F2 F2 5E D4 6B 5E D4 43 47 44 34 5F 5F 5E 2C 33 4B E1 5F A2 DC 47 5E AA 57 D4 25 A2 DC 4B 5E D3 31 AC E4 47 EF AC E4 47 F2 EF 5E D4 6B 5E 34 87 CF 1F 5F 5E D4 6B 5E 34 4B CF 1F 5F 1A 5A 2E AC 7D 2E 5F 5F A2 5E 5D D4 32 C9 48 F5 47 D3 E0 5F 5F 5E D4 57 F5 47 C4 E0 5F 5F 4A 27 C9 4D F5 47 C0 E0 5F 5F C7 2F 5F 3F 5F F5 48 10 28 5F 5F F2 4A 13 C9 10 47 33 30 5F 5F 5E D4 7B EF 47 41 18 5F 5F 1A 62 2E A3 C8 2C 5F 5F 1A E4 43 2E A3 E9 20 5F 5F 1A E4 4B 2E A4 A5 2E 5F 5F AA E4 4F 48 A8 2E 5F 5F C9 4F 47 41 2F 5F 5F 5E D4 7F EF 47 33 19 5F 5F 48 C8 2E 5F 5F C9 20 47 6C 2F 5F 5F EF 47 52 1F 5F 5F 48 A3 2A 5F 5F C9 21 47 BD 2F 5F 5F C9 22 A8 E4 27 47 B3 2F 5F 5F C9 20 AA 57 47 87 2F 5F 5F 18 FC 43 A8 E4 73 A7 3D D3 28 18 FC 27 2E A3 09 2E 5F 5F EF 47 9A 1F 5F 5F 1A 5A DC 27 22 57 2E A7 37 2E 5F 5F 1A 57 DD 21 AA 57 AA E4 73 22 66 EF F5 47 A6 1F 5F 5F AA DC 27 1A 5A 2E A3 5A 2D 5F 5F DC 2E F5 47 A9 1F 5F 5F 22 57 D8 24 A8 FC 27 AA 5A A0 5E 5F 23 5F 5F 2E AC 7D 2D 5F 5F A7 3B 16 48 75 2D 5F 5F C9 3F 47 19 2F 5F 5F C9 10 AA 4F 47 10 2F 5F 5F 18 FC 4B EF F5 D4 31 5E 34 4F CF 1F 5F A4 9F D4 CF AA E4 43 48 97 2D 5F 5F 5E 34 53 CF 1F 5F 4A 4B 12 5E E6 F6 47 26 2F 5F 5F C7 5F 23 5F 5F F5 EF A8 E4 27 5E 34 57 CF 1F 5F A4 9F D3 32 18 FC 43 D3 32 F5 5E D4 27 5E 34 53 CF 1F 5F A4 9F D4 24 A8 DC 5B A7 3D A7 BD 5E 22 5F 5F 48 C4 2D 5F 5F F2 47 8C 2E 5F 5F C9 20 AA 4F 47 83 2E 5F 5F 18 FC 4F D4 27 1A 4F DB 27 DD B5 4A 2D 1A 4F D2 27 AA E4 47 48 E7 2D 5F 5F D5 A5 AA E4 4B 48 1D 2D 5F 5F C9 20 47 D9 2E 5F 5F C9 21 AA 57 47 D0 2E 5F 5F AA 67 AA E4 47 A2 57 2B D6 CC 5E 03 A4 84 08 1F 5F 22 58 4A C1 0A 58 4A FD 2E 8E 6E AA 58 4A F6 1A 6A D3 E1 AA 66 B8 56 58 AA 57 4A E9 2A 58 4A E5 02 58 4A E1 12 58 4A 1D 12 9F 1A 5A 2E B3 9F 4A 46 1A 5A D4 2D 4A 27 12 5E 4A 0A 1A 5A D3 57 1A 6A D3 53 12 5E E6 4A 3D 1A 6A D3 28 AA 66 B8 56 58 AA 59 4A 30 12 5E 66 E4 5B 20 5F 5F 5F 4A 25 72 46 4A 21 72 5E F6 48 DB 59 5E 5E C9 20 47 29 2E 5F 5F C9 21 AA 57 47 43 2D 5F 5F EF F6 F5 5E 34 5F D1 1F 5F A2 63 2B 48 A4 2C 5F 5F AA E4 43 AA 1C DF 8E 1F 5F 1A 62 D3 E3 E7 1A 5A 2E A3 7E 25 5F 5F AA 1E 1A 62 D4 50 1A 5A 2E A3 70 25 5F 5F A2 66 23 9D DF BA 1F 5F F6 F5 47 72 1D 5F 5F 80 DF 8E 1F 5F A2 9F 23 EF F6 47 63 1D 5F 5F 80 DF 8E 1F 5F F5 A2 9F 23 EF 48 F9 2B 5F 5F 1A 72 D3 04 1A 5A 2E A3 58 29 5F 5F AC E6 23 EF F5 47 BE 1D 5F 5F AA 26 F6 82 DF 8E 1F 5F 5E 34 5B CF 1F 5F 48 2A 2C 5F 5F C7 23 23 5F 5F C9 1F 5E 34 5F D0 1F 5F 5E D4 7B AA 4F AC E5 23 EF 47 B2 1D 5F 5F 80 DF 8E 1F 5F A8 25 A8 14 DF 8E 1F 5F 48 7D 2B 5F 5F C9 22 47 04 2D 5F 5F C9 23 A8 E4 6B 47 3A 2D 5F 5F 55 E4 4F 20 A8 E4 27 D3 29 C9 12 47 07 2D 5F 5F A8 E4 6B 55 E4 4F 21 D3 29 C9 E3 47 37 2D 5F 5F A8 E4 27 A2 DC 77 00 C9 20 D4 E3 47 4A 2C 5F 5F C9 21 AA 57 47 41 2C 5F 5F AA EC 4F 60 58 21 D3 3D AC					

Analysis Process: msiexec.exe PID: **1948**, Parent PID: **2092**

General

Target ID:	5
Start time:	06:01:25
Start date:	01/10/2023
Path:	C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe"
Imagebase:	0x400000
File size:	88'209 bytes
MD5 hash:	B3657BCFE8240BC0985093A0F8682703
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 87%, ReversingLabs • Detection: 85%, Virustotal, Browse
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 | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4030ED	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nscC10E.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405745	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\rikayolehofu.Xoc	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40570F	CreateFileA
C:\Users\user\AppData\Local\Temp\Jahulocayedo.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40570F	CreateFileA
C:\Users\user\AppData\Local\Temp\naseropuxeq.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40570F	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Firozedikami.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40570F	CreateFileA
C:\Users\user\AppData\Local\Temp\yiduyevutog.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40570F	CreateFileA
C:\Users\user\AppData\Local\Temp\nshC12E.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405745	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40570F	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nscC10E.tmp	success or wait	1	403273	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rikayolehofu.Xoc	0	18958	71 46 53 51 41 57 64 44 5f 56 57 47 45 71 35 32 34 36 30 35 32 34 65 55 41 66 5c 44 55 54 56 77 59 5e 41 57 4c 42 30 35 32 34 36 30 35 32 34 36 60 54 46 5c 71 55 41 73 46 51 43 74 32 34 36 30 35 32 34 36 30 35 5c 40 52 5c 59 1c 50 5a 5c 35 32 34 36 30 35 32 34 36 30 35 32 34 60 59 47 46 41 57 5c 74 5e 58 59 53 70 4a 34 36 30 35 32 34 36 30 35 32 34 36 30 35 75 51 42 64 5d 40 51 57 54 76 5d 5a 42 55 4d 46 34 36 30 35 32 34 36 30 35 32 5f 53 42 5b 57 58 05 02 1b 56 58 5a 30 35 32 34 36 30 35 32 34 36 30 35 32 34 36 30 72 57 40 75 5f 58 5f 55 58 54 79 5b 5a 53 71 35 32 34 36 30 35 32 34 36 30 35 32 34 71 55 41 62 46 59 53 74 56 50 44 55 46 41 34 36 30 35 32 34 36 30 35 32 63 44 59 41 57 64 44 5f 56 57 47 45 7d 50 5f 5b 44 49 35 32 34 36 30 7b 46 61 58 5d 54	qFSQAWdD_VWGEq524 60524eUAf\DUT VwY^AWLB0524605246` TF\qUAsFQCt 2460524605\@R\YPZ\52 4605246052 4`YGFAW\t^XYSpJ46052 460524605u QBd]@QWTv]ZBUMF46 05246052_SB[W XVXZ0524605246052460 rW@u_X_UXT y[ZSq5246052460524qU AbFYStVPDU FA4605246052cDYAWd D_VWGE}P_[DI 52460{FaX]T	success or wait	2	402FD6	WriteFile
C:\Users\user\AppData\Local\Temp\Jahulocayedo.dll	0	4608	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 49 4d 72 fd 0d 2c 1c fd 0d 2c 1c fd 0d 2c 1c fd fd 30 12 fd 0f 2c 1c fd fd 33 16 fd 09 2c 1c fd 0d 2c 1d fd 05 2c 1c fd 6f 33 0f fd 0e 2c 1c fd fd 33 17 fd 0f 2c 1c fd fd 2a 1a fd 0c 2c 1c fd fd 33 18 fd 0e 2c 1c fd 52 69 63 68 0d 2c 1c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 78 47 51 00 00 00 00 00 00 00 00 fd 00 0e	MZ@!L!This program cannot be run in DOS mode.$lMr,,,0,3,,,o3 ,3,*,3,Rich,PELxGQ	success or wait	1	402FD6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\naseropuxeq.dll	0	17408	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 50 76 41 3e 25 41 3e 25 41 3e 25 31 fd 34 25 c1 3e 25 5a fd 30 25 01 3e 25 fd fd 2d 25 81 3e 25 41 3f 25 fd fd 3e 25 31 fd 35 25 81 3e 25 61 fd 38 25 01 3e 25 31 fd 3a 25 01 3e 25 52 69 63 68 41 3e 25 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 78 47 51 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 2c 00 00 00 1e 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Pv>%>%>%14%>%Z0%>%-%>%?%>%15%>%a8%>%1:%>%Rich>%PELxGQ!,	success or wait	1	402FD6	WriteFile
C:\Users\user\AppData\Local\Temp\Firozedikami.dll	0	3584	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 31 fd fd fd 5f fd fd fd 5f fd fd fd 5f fd 29 fd 55 fd 70 5f fd fd fd 5e fd 70 5f fd 29 fd 54 fd f0 5f fd 29 fd 5b fd 70 5f fd 52 69 63 68 fd fd 5f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 78 47 51 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 04 00 00 00 06 00 00 00 00 00 00 66 11 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$1___)U_^_)T_)[_Rich_PELxGQ!f	success or wait	1	402FD6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yiduyevutog.dll	0	4608	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 45 cd fd 01 fd fd 01 fd fd 01 fd fd fd fd 05 fd fd 01 fd fd 0c fd fd 63 fd fd 02 fd fd fd fd 03 fd 79 fd fd 00 fd fd fd fd 02 fd fd 52 69 63 68 01 fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 78 47 51 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 04 00 00 00 0a 00 00 00 00 00 00 7b 11 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$EcRichPELxGQ!{	success or wait	1	402FD6	WriteFile
C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe	0	19968	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 42 fd 76 fd 23 fd 25 fd 23 fd 25 fd 23 fd 25 fd 3f fd 25 fd 23 fd 25 4e 3f fd 25 fd 23 fd 25 25 3c fd 25 fd 23 fd 25 25 3c fd 25 fd 23 fd 25 fd 3c fd 25 fd 23 fd 25 fd 23 fd 25 fd 23 fd 25 25 3c fd 25 fd 23 fd 25 75 25 fd 25 fd 23 fd 25 52 69 63 68 fd 23 fd 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 78 47 51 00 00 00 00 00 00 00 00 fd 00 0f	MZ@!L!This program cannot be run in DOS mode.$Bv#%#%#%?%#%N?%#%%<%#%%<%#%<%#%#%#%%<%#%u%%#%Rich#%PELxGQ	success or wait	1	402FD6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	unknown	512	success or wait	94	40309A	ReadFile
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	unknown	4	success or wait	1	40309A	ReadFile
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	unknown	4	success or wait	6	40309A	ReadFile

Analysis Process: Lohonibuhod.exe PID: **1396**, Parent PID: **1948**

General

Target ID:	6
Start time:	06:01:26
Start date:	01/10/2023
Path:	C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe" "C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe"
Imagebase:	0x400000

File size:	19'968 bytes
MD5 hash:	44902781C1865978B17F396DB51D85E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 76%, ReversingLabs • Detection: 77%, Virustotal, Browse
Reputation:	low
Has exited:	true

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rikayolehofu.Xoc	unknown	24576	success or wait	1	2210A3	ReadFile

Analysis Process: msiexec.exe PID: 2748, Parent PID: 1396

General

Target ID:	7
Start time:	06:01:31
Start date:	01/10/2023
Path:	C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe"
Imagebase:	0x400000
File size:	88'209 bytes
MD5 hash:	B3657BCFE8240BC0985093A0F8682703
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\{869EE0AC-9F81-4D49-81EA-C21890B3CCC9}	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4028E8	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Lohonibuhod.exe	success or wait	1	402A67	DeleteFileA
C:\Users\user\AppData\Local\Temp\Firozedikami.dll	success or wait	1	402A87	DeleteFileA
C:\Users\user\AppData\Local\Temp\Jahulocayedo.dll	success or wait	1	402AA7	DeleteFileA
C:\Users\user\AppData\Local\Temp\naseropuxeq.dll	success or wait	1	402AC7	DeleteFileA
C:\Users\user\AppData\Local\Temp\yiduyevutog.dll	success or wait	1	402AE7	DeleteFileA
C:\Users\user\AppData\Local\Temp\rikayolehofu.Xoc	success or wait	1	402B07	DeleteFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 2948, Parent PID: 2748

General

Target ID:	8
Start time:	06:01:31
Start date:	01/10/2023
Path:	C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe"
Imagebase:	0x400000
File size:	88'209 bytes
MD5 hash:	B3657BCFE8240BC0985093A0F8682703
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
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: svchost.exe PID: **1740**, Parent PID: **2948**

General

Target ID:	9
Start time:	06:01:31
Start date:	01/10/2023
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\svchost.exe
Imagebase:	0xcd0000
File size:	20'992 bytes
MD5 hash:	54A47F6B5E09A77E61649109C6A08866
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Local Settings	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	21A3D	CreateDirectoryW
C:\ProgramData\Local Settings\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	21A54	CreateDirectoryW
C:\PROGRA~3\LOCALS~1\Temp\msoiruj.bat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	21B36	CreateFileW
C:\Users\user\AppData\Local\Temp\0E698.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	1E14E7	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1E158F	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1E158F	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1E158F	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1E158F	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1E158F	URLDownloadToFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1E158F	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1E158F	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1E158F	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1E158F	URLDownloadToFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	success or wait	1	20AE7	DeleteFileW

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\Local Settings\Temp\msoiruj.bat	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 fd fd 3a 75 fd fd 69 75 fd fd 69 75 fd fd 69 fd b5 69 77 fd fd 69 75 fd fd 69 fd fd fd 69 fd b7 69 64 fd fd 69 21 fd fd 69 7f fd fd 69 fd fd fd 69 74 fd fd 69 52 69 63 68 75 fd fd 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 1a 4b 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 5e 00 00 00 fd 02 00 00 04 00	MZ@!L!This program cannot be run in DOS mode.$1:uiuiuiiwiuii idi!iiitiRichuiPELK^	success or wait	3	21B77	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	unknown	32768	success or wait	3	21B5A	ReadFile
C:\Users\user\AppData\Local\Temp\MSI\msiexec.exe	unknown	32768	end of file	1	21B5A	ReadFile
C:\Users\user\AppData\Local\Temp\0E698.tmp	unknown	0	success or wait	1	1E1631	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\software\Wow6432Node\microsoft\windows\currentversion\Policies\Explorer\Run	success or wait	1	21C18	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	14108	unicode	C:\PROGRA~3\LOCALS~1\Temp\msoiruj.bat	success or wait	1	21C85	RegSetValueExW
HKEY_CURRENT_USER\Software	IMAGE_FILE_HEADER	binary	D9 CC 9A 6A 17 6A 6A 6A 16 6A 6A 6A 6B 6B 6A 6A A2 6A 6A 6A 6A 6A 6A 6A 2A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 72 6A 6A 6A 18 0B AC 18 6A A6 1D 59 35 A2 15 DE 59 35 C6 F2 FD E7 0A FA E4 FB F3 E4 F5 F9 0A F7 F5 F8 F8 FB E6 0A F4 F1 0A E4 E1 F8 0A FD F8 0A D6 DB C7 0A F9 FB F6 F1 38 19 19 1C 36 6A 6A 6A 6A 6A 6A 6A 41 FF 57 DD 85 1C B9 0C 85 1C B9 0C 85 1C B9 0C 68 01 BD 0C 87 1C B9 0C 68 01 B3 0C 81 1C B9 0C 82 E4 28 0C 80 1C B9 0C 85 1C BE 0C 8B 1C B9 0C 9C 83 14 0C 84 1C B9 0C 9C 83 20 0C 9A 1C B9 0C 9C 83 3A 0C 9A 1C B9 0C C4 FD F7 F2 85 1C B9 0C 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A DA D1 6A 6A DE 15 16 6A 99 F6 D7 C5 6A 6A 6A 6A 6A 6A 6A 4A 6A 14 35 1F 15 1C 6A 6A 16 6A 6A 6A 1C 6A 6A 6A 6A 6A 6A BF 1A 6A 6A 6A 1A 6A 6A 6A 0A 6A 6A 6A 6A 6A 1A 6A 1A 6A 6A 6A 14 6A 6A 11 6A 15 6A 6A 6A 6A 6A 11 6A 15 6A 6A 6A 6A 6A 6A DA 6A 6A 6A 16 6A 6A 6A	success or wait	1	1E1568	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			6A 6A 6A 14 6A 2A 15 6A 6A 1A 6A 6A 1A 6A 6A 6A 6A 1A 6A 6A 1A 6A 6A 6A 6A 6A 6A 1A 6A 6A 6A 7A 35 6A 6A 2B 6A 6A 6A F2 0A 6A 6A F6 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 2A 6A 6A CA 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 0A 6A 6A 2A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 38 E6 F1 E2 E6 6A 6A 6A DF 14 6A 6A 6A 1A 6A 6A 6A 16 6A 6A 6A 16 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 0A 6A 6A CA 38 E4 F6 F5 E6 F5 6A 6A 3B 14 6A 6A 6A 0A 6A 6A 6A 16 6A 6A 6A 12 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 2A 6A 6A 2A 38 F6 F5 E6 F5 6A 6A 6A D2 14 6A 6A 6A 3A 6A 6A 6A 14 6A 6A 6A 1E 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 2A 6A 6A AA 38 E4 F1 FE FB F7 6A 6A 84 6A 6A 6A 6A 2A 6A 6A 6A 14 6A 6A 6A 18 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 2A 6A 6A D4 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 9F D6 36 12 91 AA E1 18 2D 11 1A 3A 6A 1A E8 38 6B 19 1A 3A 6A 1A 9F 19 3A 0A 6A 1A 97 62 15 9F 1D 9D 19 22 24 6A 1A E1 2B F2 EA 6A 6A 6A 6B 01 3E 0A 6A 1A 91 AA CD B7 2A 24 6A 1A E1 16 27 AA 7F F0 97 0A 6A B5 2A 24 6A 1A F2 16 3A 6A 1A F2 6A 3A 6A 1A B7 2E 24 6A 1A 72 7C 6A 6A 6A 6B 11 1A 3A 6A 1A CD CD 7F 29 91 AA E1 2D B5 2A 24 6A 1A 91 AA E6 3A 9F 19 2E 24 6A 1A C0 99 E5 6E 2F 7A E4 04 9F 18 91 5D E6 13 6B 45 B5 2A 24 6A 1A 97 78 16 7F 7C DA 6B 01 36 0A 6A 1A 97 31 2A 24 6A 1A 6A CD C8 FC 15 C2 54 1E 6A C1 9F 7E C7 9F C9 12 C0 9F E1 1E C3 9F E9 1A 91 60 E1 1D 97 29 1A 3A 6A 1A 6A 7F 30 97 68 15 E6 11 97 68 14 E1 34 B5 D6 24 6A 1A 91 AA E6 1D C3 C0 C7 6B 5A 91 AA E6 1E C3 C0 C7 72 01 6B 6B 91 AA E1 16 27 AA 7F D8 C3 C0 C7 72 39 15 6A 6A 97 68 15 9D D1 1E E1 1E 91 AA E1 23 C3 DA C7 72 65 68 6B 6B 91 60 E6 11 97 68 17 E1 30 C3 C0 C7 72 4A 68 6B 6B 91 AA E1 17 35 D1 1E 97 E9 1E 6A E6 05 B5 D6 24 6A 1A 91 AA E6 12 C3				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			C0 C7 6B 5A 9D D1 1E 9F D1 1E CB C8 CF C9 54 1E 6A 6B 31 32 0A 6A 1A C1 9F 7E C5 C7 C0 C3 99 D1 6E DA F2 CE 0A 6A 1A F2 15 6A 6A EA 6B 01 6A 0A 6A 1A F2 16 15 6A 6A AB 3A 3A 6A 1A C3 6B 21 0A 3A 6A 1A 6B 01 12 0A 6A 1A 27 AA F0 B7 20 3A 6A 1A 27 4F 1B A3 92 2A 0A 6A 1A F0 9D 92 3A 3A 6A 1A 97 AA 14 F0 2F 5F E1 7C FC 15 C7 C7 C3 C7 C7 6B 01 22 0A 6A 1A 27 AA F0 B7 20 3A 6A 1A 1B A3 92 D6 0A 6A 1A F0 9D 92 3A 3A 6A 1A 97 AA 14 F0 2F 5F E1 7C FC 2A A8 6A 1A 6A 6A C0 C0 C7 6B 01 1A 0A 6A 1A C7 F2 EA 6A 6A 6A FC 17 C7 FC 15 F2 6A 6A 6A EA C3 B7 02 3A 6A 1A 6B 01 1E 0A 6A 1A B7 0E 3A 6A 1A C7 97 62 6B E1 10 6B 01 0E 0A 6A 1A F2 36 3A 6A 1A C0 6B 21 02 3A 6A 1A DA 6B 01 06 0A 6A 1A 6B 01 02 3A 6A 1A CB C8 CF 5D 54 1A 6A C1 9F 7E 9F D1 1E D2 E1 07 9F D1 12 F2 EE 14 6A 6A B7 0A 3A 6A 1A 6B 01 02 0A 6A 1A 27 AA 2A C9 54 1E 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A FA 35 6A 6A 6A 6A 6A 6A 38 35 6A 6A D6 35 6A 6A C4 35 6A 6A 34 35 6A 6A 0C 35 6A 6A 1E 35 6A 6A 6A 6A 6A 6A B2 35 6A 6A BA 35 6A 6A AE 35 6A 6A 50 35 6A 6A 6A 6A 6A 6A 9E 35 6A 6A 6A 6A 6A 6A 8A 6A 6A 6A F6 6A F1 6A E7 6A FF 6A E6 6A FB 6A FA 6A 38 6A FD 6A F8 6A FD 6A 6A 6A DA E4 FD F8 E6 F1 E4 E7 6A 6A 6A 6A 46 0A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A F4 35 6A 6A 12 0A 6A 6A 5E 0A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A E8 35 6A 6A 6A 0A 6A 6A 16 35 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 8E 35 6A 6A 22 0A 6A 6A 7A 0A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 40 35 6A 6A 36 0A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A FA 35 6A 6A 6A 6A 6A 6A 38 35 6A 6A D6 35 6A 6A C4 35 6A 6A 34 35 6A 6A 0C 35 6A 6A 1E 35 6A 6A 6A 6A 6A 6A B2 35 6A 6A BA 35 6A 6A AE 35 6A 6A 50 35 6A 6A 6A 6A 6A 6A 9E 35 6A 6A 6A 6A 6A 6A 0D 15 D1 E2 FD E6 DA E4 FB F7 F1 E7 E7 6A A4 16 C7 FE				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			E1 F1 FA 6A AA 17 C4 F1 F5 F6 D0 FD FE F1 6A 6A 06 14 D3 F1 E6 D9 FB F6 E1 FE F1 D0 FD FE F1 D8 F5 F9 F1 C3 6A 6A 9B 6A D7 E4 F1 F5 E6 F1 D0 FD FE F1 C3 6A 7D 16 C0 FD E4 E6 E1 F5 FE D5 FE FE FB F7 6A 6A DF D1 C4 D8 D1 DE 27 24 38 F6 FE FE 6A 6A CB 14 C4 F1 F3 DB FA F1 F8 DF F1 ED D5 6A D5 D6 C0 D5 DA DD 27 24 38 F6 FE FE 6A 6A 34 15 C7 F2 F1 FE FE D1 E2 F1 F7 E1 E6 F1 C3 6A C7 D2 D1 DE DE 27 24 38 F6 FE FE 6A C8 14 F0 E4 F1 F1 6A 6A 1B 15 CB FD F8 FD E6 E6 F1 E4 F9 6A 85 14 F9 F5 FE FE FB F7 6A 6A 89 6A CB F5 F6 FC E1 E7 E6 CB F0 F6 FD E0 6A 6A D9 C7 C0 D7 C4 C6 38 F6 FE FE 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 99 F6 D7 C5 6A 6A 6A 6A 34 34 6A 6A 15 6A 6A 6A 15 6A 6A 6A 15 6A 6A 6A 02 34 6A 6A 0E 34 6A 6A 0A 34 6A 6A D8 05 6A 6A 3C 34 6A 6A 6A 6A FB F9 F3 38 F6 FE FE 6A F7 E4 ED E7 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 1A 6A 6A CA 6A 6A 6A 1C 3A 04 3A 02 3A 37 3A 3A 3A 22 3A D0 3A DF 3A DA 3A C1 3A CA 3A F9 3A E3 3A 9E 3A 82 3A 88 3A AA 3A 44 3A 38 25 DC 25 CC 25 F1 25 FB 25 E0 25 EE 25 96 25 99 25 86 25 BD 25 A5 25 A2 25 AB 25 43 25 79 25 67 25 62 25 16 24 1D 24 1A 24 03 24 09 24 2C 24 2A 24 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A				

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

Disassembly

No disassembly