ID: 343504
Sample Name: #U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.bat
Cookbook: default.jbs
Time: 10:22:33
Date: 24/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Copyright null 2021

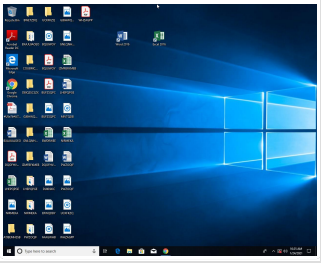
Analysis Report #U5e74#U7ec8#U63d0#U6210#U5206#U…

Overview

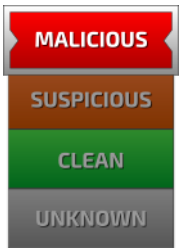
General Information

Sample Name:	#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.bat (renamed file extension from bat to exe)
Analysis ID:	343504
MD5:	6665909a2652c5..
SHA1:	84a5a2e920e816..
SHA256:	1ef7ae3509e71c3.

Most interesting Screenshot:



Detection

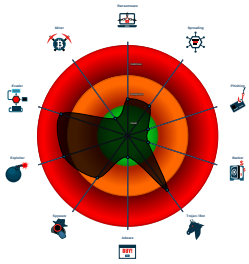


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Contains functionality to bypass UA…
- Multi AV Scanner detection for subm…
- Connects to many ports of the same…
- Tries to detect sandboxes / dynamic…
- Tries to detect sandboxes and other…
- Uses known network protocols on no…
- Abnormal high CPU Usage
- Checks for available system drives …
- Contains capabilities to detect virtua…
- Contains functionality for read data f…
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to check if a w…
- Contains functionality to communica…

Classification



Startup

- **System is w10x64**
- #U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe (PID: 4164 cmdline: 'C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe' MD5: 6665909A2652C5860FD874CB15C3991C)
  - zr.exe (PID: 6340 cmdline: 'C:\Users\user\zT6Nm@i4\zr.exe' a 'C:\Users\user\zT6Nm@i4\111.7z' 'C:\Users\user\zT6Nm@i4\TXP*' MD5: 045FCBE6C174AFA9A6A998BDD6F9FAD7)
    - conhost.exe (PID: 6356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6648 cmdline: 'C:\Windows\System32\cmd.exe' /C 'C:\Users\user\zT6Nm@i4\copy.bat' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PMRunner64.exe (PID: 7120 cmdline: 'C:\Users\user\zT6Nm@i4\PMRunner64.exe' MD5: 65DBB57517611D9DE8CE522022DCD727)
- zr.exe (PID: 6800 cmdline: 'C:\ProgramData\Microsoft\zr.exe' x C:\ProgramData\Microsoft\111.7z -y MD5: 045FCBE6C174AFA9A6A998BDD6F9FAD7)
  - conhost.exe (PID: 6656 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- PMRunner64.exe (PID: 6492 cmdline: 'C:\Users\user\zT6Nm@i4\PMRunner64.exe' MD5: 65DBB57517611D9DE8CE522022DCD727)
- PMRunner64.exe (PID: 6972 cmdline: 'C:\Users\user\zT6Nm@i4\PMRunner64.exe' MD5: 65DBB57517611D9DE8CE522022DCD727)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

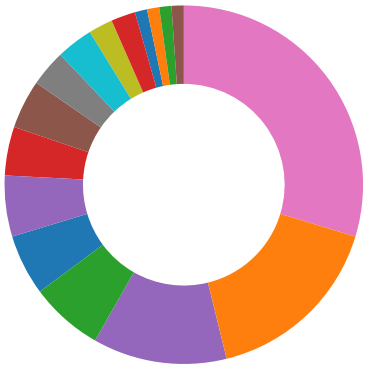
Source	Rule	Description	Author	Strings
C:\Users\user\zT6Nm@i4\ru2.url	Methodology_Suspicious_Shortcut_Local_URL	Detects local script usage for .URL persistence	@itsreallynick (Nick Carr), @QW5kcmV3 (Andrew Thompson)	• 0x13:$file: URL=file:/// • 0x0:$url_explicit: [InternetShortcut]

Copyright null 2021

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Privilege Escalation
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Privilege Escalation:

Contains functionality to bypass UAC (CMSTPLUA)

Compliance:

Binary contains paths to debug symbols

Networking:

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

Uses known network protocols on non-standard ports

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Malware Analysis System Evasion:

Tries to detect sandboxes / dynamic malware analysis system (registry check)

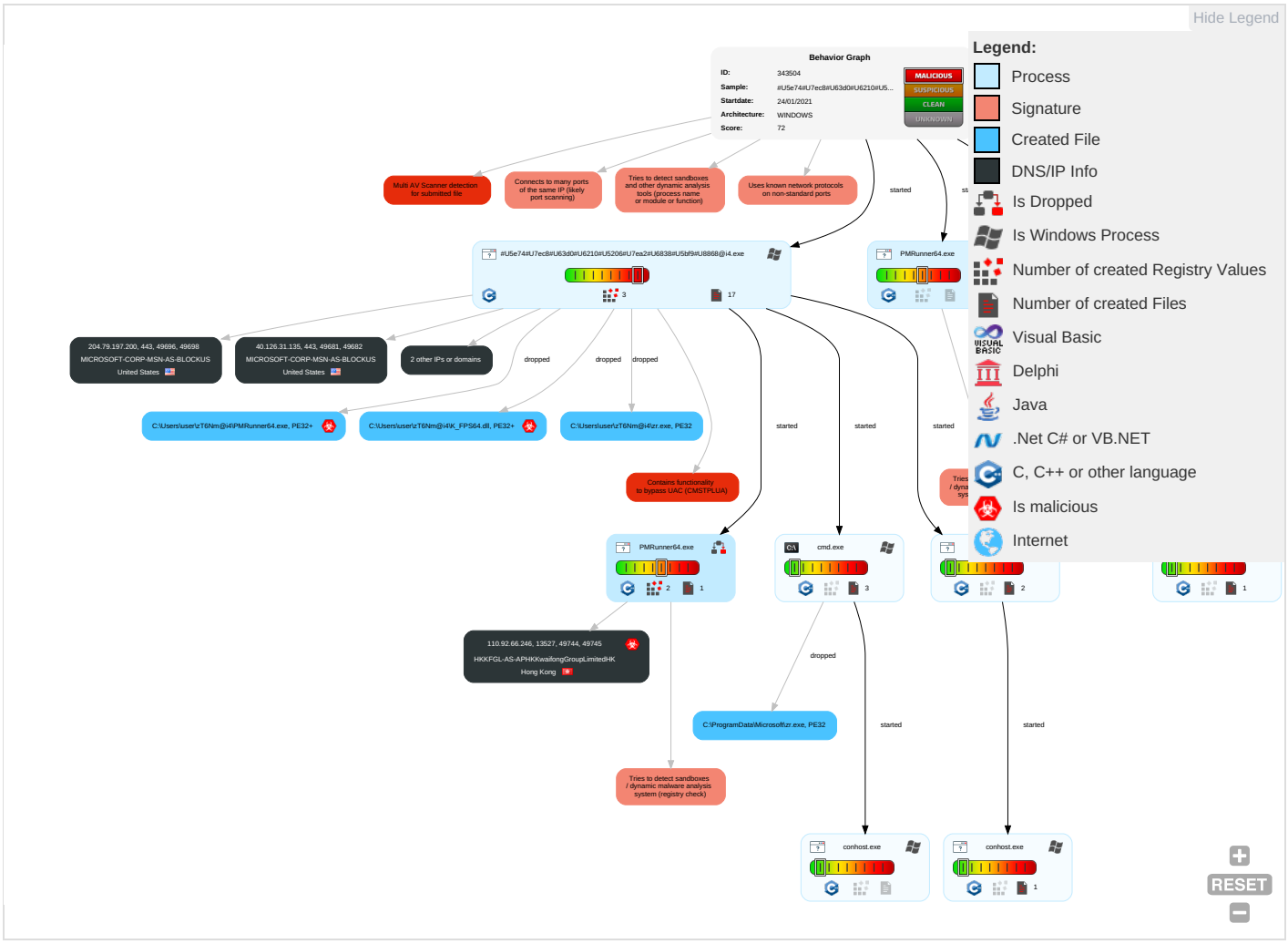
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Mitre Att&ck Matrix

Copyright null 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Replication Through Removable Media 1	Scripting 1	Startup Items 1	Startup Items 1	Deobfuscate/Decode Files or Information 1	Input Capture 3 1	System Time Discovery 2	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	Eavesdı Insecur Networ Commu
Default Accounts	Native API 2	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Scripting 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Input Capture 3 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Application Shimming 1	DLL Side-Loading 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 4	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Standard Port 1 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Registry Run Keys / Startup Folder 2 1	Application Shimming 1	DLL Side-Loading 1	NTDS	System Information Discovery 2 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Bypass User Access Control 1	Bypass User Access Control 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Access Token Manipulation 1	Masquerading 1	Cached Domain Credentials	Security Software Discovery 2 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial Service
External Remote Services	Scheduled Task	Startup Items	Process Injection 1 1	Virtualization/Sandbox Evasion 2	DCSync	Virtualization/Sandbox Evasion 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Registry Run Keys / Startup Folder 2 1	Access Token Manipulation 1	Proc Filesystem	Process Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base St

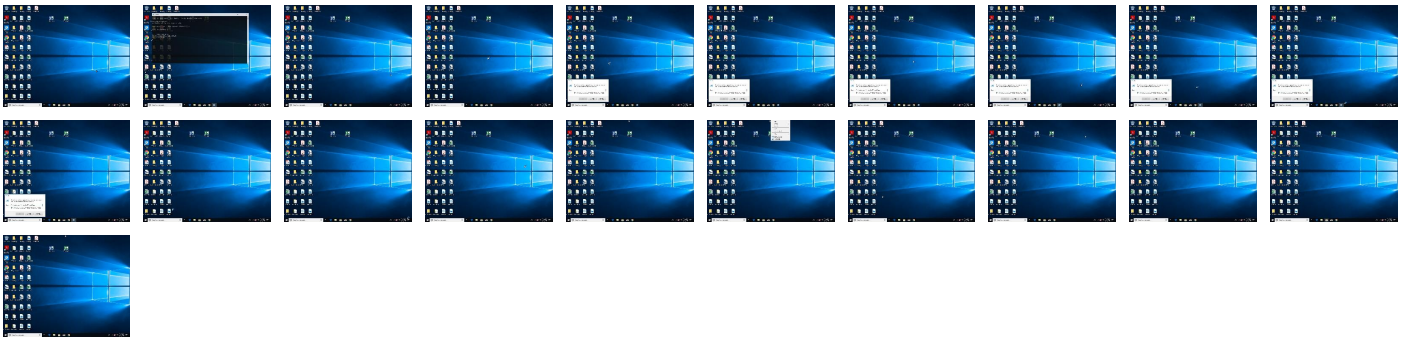
Behavior Graph



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
#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe	15%	Virustotal		Browse
#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe	22%	ReversingLabs	Win64.Trojan.CrypterX	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\Microsoft\zr.exe	0%	Virustotal		Browse
C:\ProgramData\Microsoft\zr.exe	0%	Metadefender		Browse
C:\ProgramData\Microsoft\zr.exe	0%	ReversingLabs		
C:\Users\user\zT6Nm@i4\K_FPS64.dll	6%	Virustotal		Browse
C:\Users\user\zT6Nm@i4\K_FPS64.dll	10%	ReversingLabs	Win64.Trojan.Wacatac	
C:\Users\user\zT6Nm@i4\PMRunner64.exe	0%	Virustotal		Browse
C:\Users\user\zT6Nm@i4\PMRunner64.exe	0%	Metadefender		Browse
C:\Users\user\zT6Nm@i4\PMRunner64.exe	0%	ReversingLabs		
C:\Users\user\zT6Nm@i4\zr.exe	0%	Virustotal		Browse
C:\Users\user\zT6Nm@i4\zr.exe	0%	Metadefender		Browse
C:\Users\user\zT6Nm@i4\zr.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Copyright null 2021

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.nsecsoft.com	0%	Virustotal		Browse
http://www.nsecsoft.com	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://110.92.66.246:13527/\	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.thawte.com/ThawtePremiumServerCA.crl0	#U5e74#U7ec8#U63d0#U6210#U5206 #U7ea2#U6838#U5bf9#U8868@i4.exe, 00000000.00000003.643844289 .000000000069C000.00000004.000 00001.sdmp, zr.exe.3.dr	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	#U5e74#U7ec8#U63d0#U6210#U5206 #U7ea2#U6838#U5bf9#U8868@i4.exe, 00000000.00000003.643844289 .000000000069C000.00000004.000 00001.sdmp, zr.exe.3.dr	false		high
http://https://www.thawte.com/cps0/	#U5e74#U7ec8#U63d0#U6210#U5206 #U7ea2#U6838#U5bf9#U8868@i4.exe, 00000000.00000003.643844289 .000000000069C000.00000004.000 00001.sdmp, zr.exe.3.dr	false		high
http://crl.thawte.com/ThawtePCA.crl0	#U5e74#U7ec8#U63d0#U6210#U5206 #U7ea2#U6838#U5bf9#U8868@i4.exe, 00000000.00000003.643844289 .000000000069C000.00000004.000 00001.sdmp, zr.exe.3.dr	false		high
http://www.symauth.com/cps0(	#U5e74#U7ec8#U63d0#U6210#U5206 #U7ea2#U6838#U5bf9#U8868@i4.exe, 00000000.00000003.643759945 .0000000000691000.00000004.000 00001.sdmp, PMRunner64.exe.0.dr	false		high
http://www.symauth.com/rpa00	#U5e74#U7ec8#U63d0#U6210#U5206 #U7ea2#U6838#U5bf9#U8868@i4.exe, 00000000.00000003.643759945 .0000000000691000.00000004.000 00001.sdmp, PMRunner64.exe.0.dr	false		high
http://https://www.thawte.com/cps0	#U5e74#U7ec8#U63d0#U6210#U5206 #U7ea2#U6838#U5bf9#U8868@i4.exe, 00000000.00000003.643844289 .000000000069C000.00000004.000 00001.sdmp, zr.exe.3.dr	false		high
http://www.nsecsoft.com	#U5e74#U7ec8#U63d0#U6210#U5206 #U7ea2#U6838#U5bf9#U8868@i4.exe, 00000000.00000003.643844289 .000000000069C000.00000004.000 00001.sdmp, zr.exe.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.thawte.com/repository0W	#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe, 00000000.00000003.643844289.000000000069C000.00000004.00000001.sdmp, zr.exe.3.dr	false		high
http://ocsp.thawte.com0	#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe, 00000000.00000003.643844289.000000000069C000.00000004.00000001.sdmp, zr.exe.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.126.31.135	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
204.79.197.200	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
110.92.66.246	unknown	Hong Kong		133115	HKKFGL-AS-APHKKwaifongGroupLimitedHK	true

Private

IP
192.168.2.1
192.168.2.4

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343504
Start date:	24.01.2021
Start time:	10:22:33

Copyright null 2021

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.bat (renamed file extension from bat to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.expl.evad.winEXE@13/17@0/5
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 12.2% (good quality ratio 9.2%) • Quality average: 39.6% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 59% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.139.144, 51.104.139.180, 92.122.213.194, 92.122.213.247, 8.248.141.254, 8.253.204.249, 8.241.121.126, 67.27.157.254, 8.248.113.254 • Excluded domains from analysis (whitelisted): skypedataprdcoleus15.cloudapp.net, arc.msn.com.nsatc.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, a1449.dscg2.akamai.net, arc.msn.com, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:23:40	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run C:\Users\user\zT6Nm@i4\PMRunner64.exe
10:23:48	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run C:\Users\user\zT6Nm@i4\PMRunner64.exe

Copyright null 2021

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
204.79.197.200	6.html	Get hash	malicious	Browse	• www.bing.com/favicon.ico
	6.html	Get hash	malicious	Browse	• www.bing.com/favicon.ico

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HKKFGL-AS-APHKKwaifongGroupLimitedHK	insz.exe	Get hash	malicious	Browse	• 88.218.145.49
	DOCUMENTO_MEDICO.doc	Get hash	malicious	Browse	• 154.221.28.167
	NI3651011817UL.doc	Get hash	malicious	Browse	• 103.210.237.241
	BAL_46979369.doc	Get hash	malicious	Browse	• 103.210.237.241
	427424855528075826480424.doc	Get hash	malicious	Browse	• 103.210.237.241
	FILE_81380052.doc	Get hash	malicious	Browse	• 103.210.237.241
	FILE_PO_09152020EX.doc	Get hash	malicious	Browse	• 103.210.237.241
	DOC_PO_09152020EX.doc	Get hash	malicious	Browse	• 103.210.237.241
	KH3117818420XX.doc	Get hash	malicious	Browse	• 103.210.237.241
	XCP_87353228.doc	Get hash	malicious	Browse	• 103.210.237.241
	BAL_PO_09152020EX.doc	Get hash	malicious	Browse	• 103.210.237.241
	IO3812758081JW.doc	Get hash	malicious	Browse	• 103.210.237.241
	BAL_53345761.doc	Get hash	malicious	Browse	• 103.210.237.241
	FILE_PO_09152020EX.doc	Get hash	malicious	Browse	• 103.210.237.241
	FILE_YZGLOSASM.doc	Get hash	malicious	Browse	• 103.210.237.241
	BAL_3105782760272.doc	Get hash	malicious	Browse	• 103.210.237.241
	VCG4PMFIB0AR.doc	Get hash	malicious	Browse	• 103.210.237.241
	4502009880852.doc	Get hash	malicious	Browse	• 103.210.237.241
	INV_PO_09152020EX.doc	Get hash	malicious	Browse	• 103.210.237.241
	W_RS5947693334AJ.doc	Get hash	malicious	Browse	• 103.210.237.241
MICROSOFT-CORP-MSN-AS-BLOCKUS	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 52.165.230.236
	397282_BHJ.LNK	Get hash	malicious	Browse	• 157.55.165.21
	075782_NGD.LNK	Get hash	malicious	Browse	• 157.55.165.21
	118.apk	Get hash	malicious	Browse	• 52.177.138.113
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 52.110.67.58
	ID652411022142.vbs	Get hash	malicious	Browse	• 104.41.44.79
	FileZilla_3.52.2_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 104.208.16.0
	mfpVTSmyz-Fichero.msi	Get hash	malicious	Browse	• 40.112.173.153
	Proforma Invoice.exe	Get hash	malicious	Browse	• 52.97.170.34
	ID196619484.vbs	Get hash	malicious	Browse	• 104.41.44.79

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#Ud83d#Udcde stephane.viard@colt.net @ 1200 PM 1200 PM.pff.HTM	Get hash	malicious	Browse	• 104.41.163.16
	57229937-122020-4-7676523.doc	Get hash	malicious	Browse	• 52.165.155.237
	20202237F.html	Get hash	malicious	Browse	• 52.239.172.132
	demo.js	Get hash	malicious	Browse	• 191.233.23 3.157
	demo.js	Get hash	malicious	Browse	• 191.233.23 3.157
	E-DEKONT.exe	Get hash	malicious	Browse	• 52.97.144.178
	PO-RY 001-21 Accuri.jar	Get hash	malicious	Browse	• 23.98.35.163
	ID32256523109.vbs	Get hash	malicious	Browse	• 104.41.44.79
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 20.190.63.69
	DHL Notification -AWB DHL-2021011293002.exe	Get hash	malicious	Browse	• 52.97.201.82
MICROSOFT-CORP-MSN-AS-BLOCKUS	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 52.165.230.236
	397282_BHJ.LNK	Get hash	malicious	Browse	• 157.55.165.21
	075782_NGD.LNK	Get hash	malicious	Browse	• 157.55.165.21
	118.apk	Get hash	malicious	Browse	• 52.177.138.113
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 52.110.67.58
	ID652411022142.vbs	Get hash	malicious	Browse	• 104.41.44.79
	FileZilla_3.52.2_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 104.208.16.0
	mfpVTSmyz-Fichero.msi	Get hash	malicious	Browse	• 40.112.173.153
	Proforma Invoice.exe	Get hash	malicious	Browse	• 52.97.170.34
	ID196619484.vbs	Get hash	malicious	Browse	• 104.41.44.79
	#Ud83d#Udcde stephane.viard@colt.net @ 1200 PM 1200 PM.pff.HTM	Get hash	malicious	Browse	• 104.41.163.16
	57229937-122020-4-7676523.doc	Get hash	malicious	Browse	• 52.165.155.237
	20202237F.html	Get hash	malicious	Browse	• 52.239.172.132
	demo.js	Get hash	malicious	Browse	• 191.233.23 3.157
	demo.js	Get hash	malicious	Browse	• 191.233.23 3.157
	E-DEKONT.exe	Get hash	malicious	Browse	• 52.97.144.178
	PO-RY 001-21 Accuri.jar	Get hash	malicious	Browse	• 23.98.35.163
	ID32256523109.vbs	Get hash	malicious	Browse	• 104.41.44.79
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 20.190.63.69
	DHL Notification -AWB DHL-2021011293002.exe	Get hash	malicious	Browse	• 52.97.201.82

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\111.7z	
Process:	C:\Windows\System32\cmd.exe
File Type:	7-zip archive data, version 0.4
Category:	dropped
Size (bytes):	871
Entropy (8bit):	7.6751333998200835
Encrypted:	false
SSDEEP:	24:CIOegEZhc5iZzVT78nOwNDSxEqrohfoi4:CLegEZnf8nhmtURoT
MD5:	23AEFC140636655BE400C41403524704
SHA1:	BD581B29370FD93ABF63BD2C02998A0EF2DFD2A4
SHA-256:	D37575E0B66A925ACB5432CC7B706DA8985635B80B3D60C6C90F748D1F743505
SHA-512:	2517137ABEE797FCA5E597A3826B7C02B1CB1EC045DAE4C1B493C8EE2070D6473DA9E7C584F8302D598DF11C687EE11BF2DDE9E33616243C6F94986CBD0A7AA0
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\111.7z	
Preview:	7z..'....A`.$.....#.....8.....l].&.0.!?...o..1b..V..pS.G.U.>.....Gg..1>....;...>\|*.P..D.H.ta.....0ur4..F6..f.d.2..Vzr.....#.%..a...?.6.j8KM..$...Uh..{.{._.21.!....ui8..Y*..M.. .K.L+.6zE0.....S=..c.....4.H...E}..z. D.....k...P:3...c9.....7."....V.....>..l.....R.a.i.Pk.....?*.2.c...,.L.. .VC...ui...y^..[.$..%.ea.....B...l-.....w.Ao.0.`.....Z>.....,\>.x...l..d.....B.v.#P.. ..a.8V.9`lw.f..J"r._."9j...r".C.....?.L@..=....9%...-..4...".[.....l...-...').(Dj.....`0L.Jq.;yZ.!w.i./..\2.e.....iCg...P....xr..9^...*....."..Q...V.V..... 0..M...q.).?uB...H.D..{Q.....[.4C..5....(:.{ !\.u}5....*..{..'-..X=T.....3....Ed^.$...p..@.p.u/.....#.,..o.(iAk.HY-.}1./vF...].%...W.z@.@l.....gS.....{...*.E.i.n..q.*]Y....H.=<.R.[..V%.!K-}.....v...y.M&..^....T..@....s...AZP.....t..... .....#....]......r...*...

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Realtek???????? .lnk	
Process:	C:\ProgramData\Microsoft\zr.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Icon number=0, Archive, ctime=Thu Jan 14 15:39:10 2021, mtime=Thu Jan 14 15:39:10 2021, atime=Thu Jan 14 15:39:10 2021, length=271704, window=hide
Category:	dropped
Size (bytes):	1791
Entropy (8bit):	3.466273590595946
Encrypted:	false
SSDEEP:	24:8Z3AX3ighdUAfmqpdoe7KODlWJdo7aB6m:8Z3AnisOqjl2k0B6
MD5:	5FF572CBE6B366349A9D3389D4A60CAC
SHA1:	497C442D14F4A09D00C3294784ECA1DC43A6F4A2
SHA-256:	16731A0D7B072BE60F580E93797D2E91F2DE970CF45C31EE7B9BAE52D4824B6E
SHA-512:	6DF6B097BFF0B76EC465A886ABE72EBC7DB3C850E4FA7D8CE1D60A36F57E04E3063507D3F23F059AA7024E7E7162F8F298610AA1702E16217730B1EF79D176B8
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ....K.....K.....K.....X%.....,:..DG..Yr?.D..U..k0.&...&.....-....k.2...X,~.2.....t...CFSF..1.....8R.J7.zT6Nm@i4....t.Y^...H.g.3..(.....gVA.G..k...B .....8R.J8R.J....3X.....z.T.6.N.m.@.i.4...D.j.2.X%...R. .PMRUNN~1.EXE..N.....R..R.....W.....P.M.R.u.n.n.e.r.6.4...e.x.e.....U.....-.....T..... .....w.....C:\Users\user\zT6Nm@i4\PMRunner64.exe.....\....\....\....\....\.P.M.R.u.n.n.e.r.6.4...e.x.e...C.:\.U.s.e.r.s.\.j.o.n.e.s.\.z.T.6.N.m.@.i.4.&.C.:\.U.s.e.r.s.\.j.o.n.e.s.\ .z.T.6.N.m.@.i.4.\.P.M.R.u.n.n.e.r.6.4...e.x.e.....%USERPROFILE%\zT6Nm@i4\PMRunner64.exe..... .....%.U.S.E.R.P.R.O.F.I.L.E.%.\.z.T.6.N.m.@.i.4.\.P.M.R.u.n.n.e.r.6.4...e.x.e.....

C:\ProgramData\Microsoft\zr.exe	
Process:	C:\Windows\System32\cmd.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	461088
Entropy (8bit):	6.581027593342649
Encrypted:	false
SSDEEP:	12288:tUBwDn0mdLrMkNpj6hTEXRrn9VsArg1xi:tUu7t3GTEhrn9VsA+i
MD5:	045FCBE6C174AFA9A6A998BDD6F9FAD7
SHA1:	9F477006DC176608E953EF44902FCE17DDF8FCA3
SHA-256:	08E510EF41795B4192650452D8E5482DBF71CEFAF9D67CFE02F60253D6023F96
SHA-512:	59CE53DDA80567A3B3E19FA2FBE404B655CB4203170B1295B1E6C33B9EBD0B6D2526FB568255610E64FA5C29A6F5C464766CDD746E207FFD2D48DA36811D717
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.....J.....L..G.....|.....H.....Rich..... .....PE..L.....W...../.....X.....@.....W.....x.....(..... ....text...u..... ..`.rdata.....@..@.data...\k.....@....sxdata.....p.....@....rsrc...(.....@..@..... .....

C:\Users\user\AppData\Roaming\Plugin32.dll	
Process:	C:\Users\user\zT6Nm@i4\PMRunner64.exe
File Type:	data
Category:	dropped
Size (bytes):	191488
Entropy (8bit):	**7.99619087524627**
Encrypted:	**true**
SSDEEP:	3072:SGtyjkUNHHoDhFMFI0rciHPgZwkndg0WU15pI9SmDCPAuE1L3kaF/F1Dmq:S0yjkKHHAh9t4EbHI9SmDiAQWd1Dmq
MD5:	F6773A1C5D1566F4BEBDBF81BDDDC57D
SHA1:	38CC9D3391DE6AE3773076E23B528F9534E40471
SHA-256:	5B672EE64618CCCBC94011E1BA713E5B6EFA574A8CCA18CC3653C499B2AF2202
SHA-512:	63E4BE550A66783ADFA6D064BA4912A6440986D3AF396F608F3C7B0B9F830DB8BB718216824689E1CA23D636AE67838ADB49DC0DA3263C9D64D823FB15CC964
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Plugin32.dll	
Preview:	U...u].Z....u.....D<(.8x.S....L..N..*.+^...^.r.!.....!.|u.N).Fa...L.;..{b..F.t.<.#.2=.}.r|.!l....KnR.F..4{lh..5..\.....L...Fm...4F)J..%(q..<...zE8..8...A..#.b...&*...\..Y.+^.,.....0..oi..`.g.kD .48.G....L.QNor..+2.&"..r.!.Q..".V....l7.@.)8!..h.C8.....:&=.@.1.I..~....bg.r..Z....vK..h.D\8..8....sBM..^..*5+^...~.r.!...u... .|.|..@V)8.%..+*.8.....-..B{1.)..j..=.B..._.Z.....v...(.D.(. p8.....L@.N/.*.+^.....rN!.....|..@.)8.%.(+*.8.t..s:&}.@.1....>....b%.r..Z.U<`.v.....D.8..8.g..7.L..N..*.+^r...rNv&)9.5..}..<..Q.@.+8A).+*d8.....:&.B@;....L.....r..r..Z....^i....D|(.0 8...4.....N..*U+^....r.!.....|..@v)8.%..+*.8.4..3:&=.@.1.....].b..r..Z.....v...H.D.(..8.'....L`.NO.*.+^2....rn!.1.....=....|..@.)8.%.H+*$8.....:&..@.1.9..^....bE.r..Zs..p.v+....D<(. .8....S.L..N..*.+^...^.r.!...U.....\.|u.@6)8a%.+*.8.....:&..@[1.....b..rN.Z.....v.....D.(.P8.....L .N..*u+^....r.!.....|..@.)8.%..+*.8.T..S:&].@.1.....}.b..r..Z3..0.v...h.D.(..8. GN"*8L.\.N.N.3

C:\Users\user\zT6Nm@i4\111.7z	
Process:	C:\Users\user\zT6Nm@i4\zr.exe
File Type:	7-zip archive data, version 0.4
Category:	dropped
Size (bytes):	895
Entropy (8bit):	7.58674925006426
Encrypted:	false
SSDEEP:	24:7OegEZhc5iZzVT78nOwNDSxEqrohfoiQ3T:KegEZnf8nhmtURo/3T
MD5:	8B8E701F0984126214856AEA7B49A3E1
SHA1:	BC4995ABD24C3451D3AF427F7CE03FA484055157
SHA-256:	D4714CBC4612E14FA5D62B26274411A435396094EFECAAC6D82325FA2400FD04
SHA-512:	7049B6C1ED94B5F10138C3971598A7C98D2E25F340A3C914F4E0D27074AF70A51FF53A7652CE4373140054B0E16A484D1083483CFEB105F6DF5D313C3FAF35E5
Malicious:	false
Reputation:	low
Preview:	7z..'.....l].&.0.!?...o..1b..V..pS.G.U.>.....Gg..1>....;...>|*.P..D.H.ta.....0ur4..F6..f.d.2..Vzr.....#.%..a...?.6.j8KM..$...Uh..{.{._.21.!....ui8..Y*..M...K.L+.6zE0 .....S=..c.....4.H...E}..z. D.....k...P:3...c9.....7."....V.....>..l.....R.a.i.Pk.....?*.2.c...,.L.. .VC...ui...y^..[.$..%.ea.....B...l-.....w.Ao.0.`.....Z>.....,\>.x...l..d.....B.v.#P....a.8V.9`l w.f..J"r.._."9j...r".C.....?.L@..=.....9%...-..4..."..[.....I...-...').(Dj.....`0L.Jq.;yZ.!w.i./..\2.e.....iCg...P....xr..9^...*....".Q...V.V..... 0..M...q.).?uB...H.D..{Q.....[.4C..5....(:.{!\.u}5....*.. {..'-..X=T.....3....Ed^.$...p..@.p.u/.....#.,..o.(iAk.HY-.}1./vF...].%...W.z@.@l.....gS.....{...*.E.i.n..q.*]Y....H.=<.R.[..V%.!K-}.....v...y.M&..^....T..@....s...AZP.....t.....#....].....r...*....A`.$.....#.....8.

C:\Users\user\zT6Nm@i4\KK.txt	
Process:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File Type:	data
Category:	dropped
Size (bytes):	224323
Entropy (8bit):	**7.996498851977439**
Encrypted:	**true**
SSDEEP:	6144:5SDdKtn3KwKa9xg8LIzF9yWeSBvd+tResBuYU:4Dde3xKhOIzOGBF
MD5:	7B30F5D321E85813F5E5835F92FFA0FC
SHA1:	369474EA5BFFA01DAC8C663EDE08D7D0D8967054
SHA-256:	445E5B49DA01A0D99AFD84EF3D9C5238E02D5E4FBC546D43C619005A622C9917
SHA-512:	8797E96456F2C822DA7B79486784BA49ED7A4CC85FF74F76D097339EA8C2FDC945E1EB51BEF28F7E1358EA38BD6BBB8D1C35D63A54F5000A1D75C5E90DDAB0 FD
Malicious:	false
Reputation:	low
Preview:	rc(.%c.Q.q....<cfW.&.-...SP#....|O.%'q5.XrVN\....@J..)F.YZ.....%...,...y.s.x.....C...L.y.'....V.Ck....I.4'L.b....e'.Q..QS...w.xgF...L.Q......./.....'v6=.yj..t.h.n.i.a%g..:#.\.Q.lN...r.ht... .y..I..k.ATu/.._..j._B...?%....-..N|.G....|1.V..&..^..8.L..E.y.PQ.....j|fhfm 2....e..k..\. ...Q.....'}u....<.AW".I.a6..Dv.....G.j#..f...^..6.)...ky..yI.X..vv.....v.....*.....$..4...I.....S..Zoz ..n).....%....\...TFg...`~.@V.....E.Q....L.._.PnR4OI...^ .Av.y.d.....2.t2...-.D....Y.2.T!.Pl6...@;...[..q.o..'./.3..[k.E :....i.+%....c.@.o.....eL....1.cig....?rP.O.C'....Ak...7..R....EG... ...Q.ey.._.k.r./..TOCe.y.....q..<.I:9#+5...^..&.A.....U`v.w..t...A7m.Jg..m..".mz.....#....gW.^...q.z..HbX.....2..iH.!...#H.9..>W....S..&e..k..h<2..c.....b._..0.D1.Bno.q.$bP...* .o8[.Lq.bCG.E3g.W2.^.{..''n.....N4..(.....=E..R..O....|....._L...IX.._.%.....x...`;...]Nm...Q.s7..i..QW.B...h.u.3.~..).#."&..(X.....l0.....X.....z...b'..34.

C:\Users\user\zT6Nm@i4\K_FPS64.dll	
Process:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	302592
Entropy (8bit):	5.94262128533878
Encrypted:	false
SSDEEP:	6144:YDVMbwz0W4gWqPcjwhum9o34Ec2x1tRuf+X4zNEP:YDGO0WTWq4wYb34Ec2vupEP
MD5:	B8477E4DF0F24A96BBAFD2F13C31A4A2
SHA1:	E4548C10552B1906BBE4A7EED90E97D24C958CF5
SHA-256:	5EFD269CA1CD474F68ECE50E6AC3F88F1831ACA273DE9789C17DD8A46AEA8D71
SHA-512:	6FE6FF9E3BD95CE0583AA2BBB06B8AB123363D94AFEEAB3CCE377B1FB5EABB0BA58F1107E822C39FF2D186E788783262EFFAB8270519A2A118C055013BEEC6 B3
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 6%, Browse • Antivirus: ReversingLabs, Detection: 10%
Reputation:	low

C:\Users\user\zT6Nm@i4\K_FPS64.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sl..7.@.7.@.7.@.B..6.@...-.0.@...;.,.@.7.A...@.>u...@.>u..=.@.>u..H.@.>u..+.@.>u..6.@.)_..6.@.>u..6.@.Rich7.@.....PE..d.....`....." .....4.....@.....=.....@.....@.....x....@.....h$..(.....text...h..... ..`.rdata..G.....@..@.data.....@....pdata.....@...0.....@..@.tls.....p.....@....rsrc...x.....@..@.reloc...(.....*...t.....@..B.....

C:\Users\user\zT6Nm@i4\PMRunner64.exe	
Process:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	271704
Entropy (8bit):	5.761811520401724
Encrypted:	false
SSDEEP:	3072:wWHyRIh1NDBeEOqDhPbsuB35WlP+7l1MYMb3URvwgwWwBHNFs:nrrNDBeJwhbh3mU9wgw
MD5:	65DBB57517611D9DE8CE522022DCD727
SHA1:	B33E6DB5C460E5E38DD636C4D48E9D4523E2838F
SHA-256:	0525B815E61D3CD83FD4C87032DE7C1DCBA5E8D2619539F925E43624EB6E1D77
SHA-512:	D8D34BC3642255DFF395CB47A0EA58CC07D911B3535A0A6D972CC4E501F6CCAB200A7D636FCDEE77DC6E7AD6B735918BCDF48EA6F0EA0E26804C31F2D1754 0D
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$..eJ.eJ.eJ.....eJ.....+eJ.....eJ.;I.eJ.;O.eJ.;N.eJ.d...eJ.eK.>eJ..;C.eJ..;J.eJ.+;..eJ.e..eJ..;H.eJ.Rich.eJ.....PE..d....S.^.....".....`.....l0.....@.....`.....`.....`..... ...P..... ....`..... ....X#...P.. ...`...p.....p..x.....text....^.....`..... ..`.rdata.....p.....d.....@..@.data....*...0.....@....pdata.....` .....&.....@..@.gfids.....<.....@..@.rsrc... .....>.....@..@.reloc.. ....P.....@..B.....

C:\Users\user\zT6Nm@i4\TXP\Windows\Start Menu\Programs\Startup\Realtek???????? .lnk	
Process:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Icon number=0, Archive, ctime=Thu Jan 14 15:39:10 2021, mtime=Thu Jan 14 15:39:10 2021, atime=Thu Jan 14 15:39:10 2021, length=271704, window=hide
Category:	dropped
Size (bytes):	1791
Entropy (8bit):	3.466273590595946
Encrypted:	false
SSDEEP:	24:8Z3AX3ighdUAfmqpdoe7KODlWJdo7aB6m:8Z3AnisOqjl2k0B6
MD5:	5FF572CBE6B366349A9D3389D4A60CAC
SHA1:	497C442D14F4A09D00C3294784ECA1DC43A6F4A2
SHA-256:	16731A0D7B072BE60F580E93797D2E91F2DE970CF45C31EE7B9BAE52D4824B6E
SHA-512:	6DF6B097BFF0B76EC465A886ABE72EBC7DB3C850E4FA7D8CE1D60A36F57E04E3063507D3F23F059AA7024E7E7162F8F298610AA1702E16217730B1EF79D176B8
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ....K.....K.....K.....X%.....,.:..DG..Yr?.D..U..k0.&...&.....-....k.2...X,~.2.....t...CFSF..1.....8R.J7.zT6Nm@i4....t.Y^...H.g.3..(.....gVA.G..k...B .....8R.J8R.J....3X.....z.T.6.N.m.@.i.4...D.j.2.X%...R. .PMRUNN~1.EXE..N.....R..R.....W.....P.M.R.u.n.n.e.r.6.4...e.x.e.....U.....-.....T..... .....w.....C:\Users\user\zT6Nm@i4\PMRunner64.exe.....\.....\.....\.....\.....\.P.M.R.u.n.n.e.r.6.4...e.x.e...C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.z.T.6.N.m.@.i.4.&.C.:.\.U.s.e.r.s.\.j.o.n.e.s.\ .z.T.6.N.m.@.i.4.\.P.M.R.u.n.n.e.r.6.4...e.x.e.....%USERPROFILE%\zT6Nm@i4\PMRunner64.exe..... .....%.U.S.E.R.P.R.O.F.I.L.E.%.\.z.T.6.N.m.@.i.4.\.P.M.R.u.n.n.e.r.6.4...e.x.e.....

C:\Users\user\zT6Nm@i4\copy.bat	
Process:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File Type:	ASCII text, with CR, LF line terminators
Category:	dropped
Size (bytes):	148
Entropy (8bit):	4.859584238440697
Encrypted:	false
SSDEEP:	3:55Pt+ZIgUAdkdZkRErG+ffbNQdi25Pt+ZIrUhFmRdZkRErG+fUNhn:PwZIPAra3ZQdi2wZIroakn
MD5:	7EE919ABFE2EBEFCDD420D0E0784F1C9
SHA1:	760A5A935E7453C7C3D0CFE786975F97931382BB
SHA-256:	21C285FD608237D8B329AD8266FDCC0E9C671BAEB956E9544CAEC712944EF8A9
SHA-512:	0327C9A5500BEF65DFF1501553F0471B7CF2584CAA56CBF15673AC4AF10E748C08E15C5878F0C792907F2F777C6393925A22AB36BDBB70C29963FEC9A07AFFF5
Malicious:	false
Reputation:	low
Preview:	copy "C:\Users\user\zT6Nm@i4\zr.exe" "C:\ProgramData\Microsoft\zr.exe"..copy "C:\Users\user\zT6Nm@i4\111.7z" "C:\ProgramData\Microsoft\111.7z"..

C:\Users\user\zT6Nm@i4\ru2.url	
Process:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:///C:\Users\user\zT6Nm@i4\run001.lnk>), ASCII text, with CR line terminators
Category:	dropped
Size (bytes):	65
Entropy (8bit):	4.934228490671524
Encrypted:	false
SSDEEP:	3:HRAbABGQVuOt+ZIo7g:HRYF5OwZlig
MD5:	004A6C48B0C8EE5A854123B30016589A
SHA1:	E491D660E83A6DC76EDFB00A8750B98E6F66C665
SHA-256:	2CF3CC8BCD1655AE232418CCFEBBF8D0AA5EFB062F95DF320C27B5C3A69E9A7C
SHA-512:	02CD3B044426D6CE89CECBFD16D294882AF867C33F53E6AE71104A4D4E2D57C9A551E659616B7D331CD8714E55DED39538796AD4A1F076483E619CF49E864E7
Malicious:	false
Yara Hits:	• Rule: Methodology_Suspicious_Shortcut_Local_URL, Description: Detects local script usage for .URL persistence, Source: C:\Users\user\zT6Nm@i4\ru2.url, Author: @itsreallynick (Nick Carr), @QW5kcmV3 (Andrew Thompson)
Reputation:	low
Preview:	[InternetShortcut].URL=file:///C:\Users\user\zT6Nm@i4\run001.lnk

C:\Users\user\zT6Nm@i4\run.lnk	
Process:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Wed Apr 11 22:34:14 2018, mtime=Wed Sep 30 06:35:53 2020, atime=Wed Apr 11 22:34:14 2018, length=273920, window=hide
Category:	dropped
Size (bytes):	1845
Entropy (8bit):	3.204025472281673
Encrypted:	false
SSDEEP:	24:8PHjJW6PV7Mmc7S6MAdx+/5+fUt+/g4l0Z57aB6m:8PMYdCXLiu8sIrB6
MD5:	BE3AF8B163611E11E35121A9C0DE546F
SHA1:	DFEEE23EAE5794D9C6D7B54A00CB0E42800AFAA3
SHA-256:	271541E40261A329ED49F004A2ABAAA533009C1E94B9F7CA3CED62756E59912B
SHA-512:	495C1D2427C943DFBC3739CFC3E104934449E629B39FEF81074F21151345DBA06A96DFE766B03F8CF74CDE5EB8D52CB8F00FA969186E8CECDFCF3B37346739E
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ...]......J..S....]..... .....5....P.O. .:i.....+00../C:\.....V.1....>Qz<..Windows.@.....L..8R.J.....W.i.n.d.o.w.s.....Z.1.....8R.J. .System32..B.....L..8R.J.....e...S.y.s.t.e.m.3.2.....V.2.....LH. .cmd.exe.@.....LH.>Qx<.....t.....&.c.m.d...e.x.e.....J.....-.....I.....w.....C:\Windows\System32\cmd.exe..!.....\.....\.....\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.c.m.d...e.x.e...C.:.\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.&. ./.c. .C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.z.T.6.N.m.@.i.4.\.r.u.n.0.0.1...l.n.k...C.:.\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.c.m.d...e.x.e.....%SystemRoot%\System32\cmd.exe..... .....%.S.y.s.t.e.m.R.o.o.t.%.\.S.y

C:\Users\user\zT6Nm@i4\run001.lnk	
Process:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	1457
Entropy (8bit):	1.9452446037061828
Encrypted:	false
SSDEEP:	12:8zM0i/kdvrHjHbQbfnbB5baP0yZ3ZrwPH:8AIzD7kzzk0yZ3Zk
MD5:	95A5332A3DE1AE6E16F7E139EE968E9B
SHA1:	9E7DD05E15FCAC8C1B8E91978B7EFEB923CD6A88
SHA-256:	5D0904F70763CA9D1118EFD2171BA4A0CF0D7C10B8D121836F95CE16A3E03C5A
SHA-512:	53A9CA5C5754D742BD568953B8B4A5AB58BDEA9C9CFC7E49C921484883BCF93CA9E5B6758FDFF72FF98BD0C5D1B70B97B264C89912880A7BB179CE26E8A768B0
Malicious:	false
Reputation:	low
Preview:	L.....F.@.....A....P.O. .:i.....+00../C:\.....b.1.....ProgramData.H.....P.r.o.g.r.a.m.D.a.t.a.....\.1..... ....Microsoft.D.....M.i.c.r.o.s.o.f.t.....T.2.....zr.exe..>.....z.r...e.x.e.....%.....\.....\.....\.P.r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.z.r...e.x.e...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.%. .x. .C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.1.1.1...7.z. .-.y...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.z.r...e.x.e.....%ALLUSERSPROFILE%\Microsoft\zr.exe..... .....%.A.L.L.U.S.E.R.S.P.R.O.F.I.L.E.%.\.M.i.c.r.o.s.o.f.t.\.z.r...e.x.e

C:\Users\user\zT6Nm@i4\run003.lnk	
Process:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Sun Apr 30 07:53:46 2017, mtime=Sun Apr 30 07:53:46 2017, atime=Sun Apr 30 07:53:46 2017, length=461088, window=hide
Category:	dropped
Size (bytes):	1837

C:\Users\user\zT6Nm@i4\run003.lnk	
Entropy (8bit):	3.401424786774406
Encrypted:	false
SSDEEP:	24:8hJ3AX3igX1AnxQfouopHO8jAIM7aB6m:8/3AniRyfouopHdB6
MD5:	4AC952055902E20C748E96234BF2F56C
SHA1:	9B0BADF7DE8286543D6D5C45CD19E834E76E671F
SHA-256:	0D7B6A444BFA014BEE1DC4769FB66663BB1F0FC0B3327EC41AB9F5342BF571EF
SHA-512:	80639E1E8B2C4DD3BEC66CBEF87B7E1293D9CCE7E8B34C71B9011400E536CBA39801155CAC3C691B096F2B2B55254CF53FB402B7D843E429196C8B5484DD83 A
Malicious:	false
Preview:	L.....F.@.. .....i.....i.....i.... .....:..DG..Yr?.D..U..k0.&...&.....-....k.2...X,~.2.....t...CFSF..1.....8R.J7.zT6Nm@i4....t.Y^...H.g.3..(.....gVA.G..k...B.....8 R.J8R.J....3X.....z.T.6.N.m.@.i.4...D.T.2. ....J.F .zr.exe..>.....J.F.J.F....:X.....z.r...e.x.e.....M.....-.....L.....w.....C:\Users\user\ zT6Nm@i4\zr.exe.....\.z.r...e.x.e...C.:\.U.s.e.r.s.\.j.o.n.e.s.\.z.T.6.N.m.@.i.4.B.a. .".C.:\.U.s.e.r.s.\.j.o.n.e.s.\.z.T.6.N.m.@.i.4.\.1.1.1...7.z.". .".C.:\.U.s.e.r.s.\.j.o.n.e.s.\.z.T .6.N.m.@.i.4.\.T.X.P.\.*."...C.:\.U.s.e.r.s.\.j.o.n.e.s.\.z.T.6.N.m.@.i.4.\.z.r...e.x.e.....%USERPROFILE%\zT6Nm@i4\zr.exe..... .....%.U.S.E.R.P.R.O.F.I.L.E.%.\.z.T.6.N.m

C:\Users\user\zT6Nm@i4\zr.exe	
Process:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	461088
Entropy (8bit):	6.581027593342649
Encrypted:	false
SSDEEP:	12288:tUBwDn0mdLrMkNpj6hTEXRrn9VsArg1xi:tUu7t3GTEhrn9VsA+i
MD5:	045FCBE6C174AFA9A6A998BDD6F9FAD7
SHA1:	9F477006DC176608E953EF44902FCE17DDF8FCA3
SHA-256:	08E510EF41795B4192650452D8E5482DBF71CEFAF9D67CFE02F60253D6023F96
SHA-512:	59CE53DDA80567A3B3E19FA2FBE404B655CB4203170B1295B1E6C33B9EBD0B6D2526FB568255610E64FA5C29A6F5C464766CDD746E207FFD2D48DA36811D717
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.....J.....L..G.....|.....H.....Rich..... .....PE..L.....W...../.....X.....@.....W.....x.....(..... ....text...u..... ..`.rdata.....@..@.data...\k.....@....sxdata.....p.....@....rsrc...(.....@..@..... .....

\Device\ConDrv	
Process:	C:\ProgramData\Microsoft\zr.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	484
Entropy (8bit):	4.98831110003937
Encrypted:	false
SSDEEP:	12:pltQzsBRwgaQH7pyTkaHo8ajFsQcE5+svhJAISLGN2Gy:pYzsDwXQboTjUZH+svhJAI9wv
MD5:	70C66FCD7F376B7EC9AD79053CA63030
SHA1:	E3AE64762463879E0B8C91713A291B540131E423
SHA-256:	3FD565B1794F89DB8FFA179D9EBF283A0AC7B37BD9E8AD8DE94BB1443B0416BA
SHA-512:	0B07E9206A5B8D60D93AE7AE826605FFBC2DE13B072DB3EEF2A74E0E05485B8ADDA1E5D6231CC9965FD340937396035668410986 31FBD89B8F7CC8889A2FBDA 0
Malicious:	false
Preview:	..7-Zip (r) [32] 16.04 : Igor Pavlov : Public domain : 2016-10-04....Scanning the drive for archives:.. 0M Scan C:\ProgramData\Microsoft\. .1 file, 871 bytes (1 KiB)....Extracting archive: C:\ProgramData\Microsoft\111.7z..--..Path = C:\ProgramData\Microsoft\111.7z..Type = 7z..Physical Size = 871..Headers Size = 24 3..Method = LZMA2:12..Solid = -..Blocks = 1.... 0%. .Everything is Ok....Folders: 4..Files: 1..Size: 1791..Compressed: 871..

Static File Info

General

File type:	PE32+ executable (GUI) x86-64, for MS Windows
Entropy (8bit):	6.805779435598225

General

TrID:	• Win64 Executable GUI (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
File size:	3150336
MD5:	6665909a2652c5860fd874cb15c3991c
SHA1:	84a5a2e920e8165634e510766eaa51662401a227
SHA256:	1ef7ae3509e71c3cd0904a7396831e6bd2c021f14dc5d4b2485a38ebefc3dd3d
SHA512:	c7ca90037a3e67b443fe6b8f8a8df510eb2794d53a80a416b7234de123703cf5b590f3314f1e0acf749156ce40cc176182d521679c83afceb18b60d39e07c6a5
SSDEEP:	49152:jwBFRHHY3rC5IgDAI9q8xCFEXIZ40nqSvLcUhGcwKEAX/ivWPlGbjtGysnISnvpZ:jwlHYm5IML9hGvTWlGnUysnISnBdu2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c`7...d...d...dFL.d...d.z.d...d.z.d...d.z.d...d...d...d.t.dd..d.t.d...d.t.d...d.t.d...d.t.d...dRich...d.....PE..d..

File Icon

Icon Hash:	74cac4d4d4d0c4d4

Static PE Info

General

Entrypoint:	0x1401543b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x600BDCC7 [Sat Jan 23 08:22:31 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	5894f7ecf05bebd0f6f297d29b91f916

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
call 00007F7DAC8515DCh
dec eax
add esp, 28h
jmp 00007F7DAC84AA97h
int3
int3
dec eax
mov dword ptr [esp+08h], ebx
push edi
dec eax
sub esp, 20h

Instruction
dec eax
lea eax, dword ptr [00076193h]
mov ebx, edx
dec eax
mov edi, ecx
dec eax
mov dword ptr [ecx], eax
call 00007F7DAC851667h
test bl, 00000001h
je 00007F7DAC84AC4Ah
dec eax
mov ecx, edi
call 00007F7DAC6F960Eh
dec eax
mov eax, edi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
add esp, 20h
pop edi
ret
int3
int3
int3
dec eax
sub esp, 28h
dec eax
mov eax, edx
dec eax
lea edx, dword ptr [ecx+11h]
dec eax
lea ecx, dword ptr [eax+11h]
call 00007F7DAC8516B1h
test eax, eax
sete al
dec eax
add esp, 28h
ret
int3
int3
dec eax
mov dword ptr [esp+10h], ebx
dec eax
mov dword ptr [esp+18h], ebp
dec eax
mov dword ptr [esp+20h], esi
push edi
inc ecx
push esp
inc ecx
push ebp
inc ecx
push esi
inc ecx
push edi
dec eax
sub esp, 20h
dec ecx
arpl word ptr [eax+0Ch], di
dec esp
mov edi, ecx
dec ecx
mov ecx, eax
dec ecx

Copyright null 2021

Instruction
mov ebp, ecx
dec ebp
mov ebp, eax
dec esp
mov esi, edx
call 00007F7DAC8517ADh
dec ebp
mov edx, dword ptr [edi]
dec esp
mov dword ptr [ebp+00h], edx
inc esp
mov esp, eax
test edi, edi
je 00007F7DAC84ACCAh
dec eax
lea ecx, dword ptr [edi+edi*4]
dec eax
lea esi, dword ptr [FFFFFFECh+ecx*4]
dec ecx
arpl word ptr [ebp+10h], bx
dec ecx

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1ff938	0x17c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x306000	0xb0f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x2f0000	0x13518	.pdata
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	0x17b000	0x1350	.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	0x179a48	0x179c00	False	0.519473729112	data	6.37063911403	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x17b000	0x886cc	0x88800	False	0.253088870765	data	4.38109791814	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x204000	0xeb290	0xdee00	False	0.944429595485	data	7.74292213666	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x2f0000	0x13518	0x13600	False	0.497505040323	data	6.14754754116	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
text	0x304000	0xbbd	0xc00	False	0.466796875	data	5.50929008744	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA
data	0x305000	0x760	0x800	False	0.6806640625	data	5.89712002279	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x306000	0xb0f8	0xb200	False	0.413031074438	data	5.68750375192	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x306c10	0x134	data	Chinese	China
RT_CURSOR	0x306d44	0xb4	data	Chinese	China
RT_CURSOR	0x306df8	0x134	AmigaOS bitmap font	Chinese	China
RT_CURSOR	0x306f2c	0x134	data	Chinese	China
RT_CURSOR	0x307060	0x134	data	Chinese	China
RT_CURSOR	0x307194	0x134	data	Chinese	China
RT_CURSOR	0x3072c8	0x134	data	Chinese	China
RT_CURSOR	0x3073fc	0x134	data	Chinese	China
RT_CURSOR	0x307530	0x134	data	Chinese	China
RT_CURSOR	0x307664	0x134	data	Chinese	China
RT_CURSOR	0x307798	0x134	data	Chinese	China
RT_CURSOR	0x3078cc	0x134	data	Chinese	China
RT_CURSOR	0x307a00	0x134	AmigaOS bitmap font	Chinese	China
RT_CURSOR	0x307b34	0x134	data	Chinese	China
RT_CURSOR	0x307c68	0x134	data	Chinese	China
RT_CURSOR	0x307d9c	0x134	data	Chinese	China
RT_BITMAP	0x307ed0	0xb8	data	Chinese	China
RT_BITMAP	0x307f88	0x144	data	Chinese	China
RT_ICON	0x3080cc	0xea8	data	Chinese	China
RT_ICON	0x308f74	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	Chinese	China
RT_ICON	0x30981c	0x568	GLS_BINARY_LSB_FIRST	Chinese	China
RT_ICON	0x309d84	0x25ad	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	Chinese	China
RT_ICON	0x30c334	0x25a8	data	Chinese	China
RT_ICON	0x30e8dc	0x10a8	data	Chinese	China
RT_ICON	0x30f984	0x468	GLS_BINARY_LSB_FIRST	Chinese	China
RT_DIALOG	0x30fdec	0xde	data	Chinese	China
RT_DIALOG	0x30fecc	0x210	data	Chinese	China
RT_DIALOG	0x3100dc	0xe2	data	Chinese	China
RT_DIALOG	0x3101c0	0x34	data	Chinese	China
RT_STRING	0x3101f4	0x6a	data	Chinese	China
RT_STRING	0x310260	0x4e	data	Chinese	China
RT_STRING	0x3102b0	0x2c	data	Chinese	China
RT_STRING	0x3102dc	0x84	data	Chinese	China
RT_STRING	0x310360	0x1c4	data	Chinese	China
RT_STRING	0x310524	0x14e	data	Chinese	China
RT_STRING	0x310674	0x10e	data	Chinese	China
RT_STRING	0x310784	0x50	data	Chinese	China
RT_STRING	0x3107d4	0x44	data	Chinese	China
RT_STRING	0x310818	0x68	data	Chinese	China
RT_STRING	0x310880	0x1b2	data	Chinese	China
RT_STRING	0x310a34	0xf4	data	Chinese	China
RT_STRING	0x310b28	0x24	data	Chinese	China
RT_STRING	0x310b4c	0x1a6	data	Chinese	China
RT_GROUP_CURSOR	0x310cf4	0x22	Lotus unknown worksheet or configuration, revision 0x2	Chinese	China
RT_GROUP_CURSOR	0x310d18	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310d2c	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310d40	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310d54	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310d68	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310d7c	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0x310d90	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310da4	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310db8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310dcc	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310de0	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310df4	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310e08	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x310e1c	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_ICON	0x310e30	0x68	data	Chinese	China
RT_MANIFEST	0x310e98	0x25f	ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	IsValidCodePage, GetTimeZoneInformation, LCMapStringW, GetConsoleCP, GetConsoleMode, WriteConsoleW, SetEnvironmentVariableA, RtlCaptureContext, RtlVirtualUnwind, IsDebuggerPresent, UnhandledExceptionFilter, TerminateProcess, QueryPerformanceCounter, HeapCreate, GetVersion, HeapSetInformation, FlsAlloc, FlsFree, FlsSetValue, FlsGetValue, SetHandleCount, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetStdHandle, SizeofResource, SetUnhandledExceptionFilter, GetFileType, SetStdHandle, VirtualQuery, GetSystemInfo, SetThreadStackGuarantee, HeapSize, HeapQueryInformation, RtlPcToFileHeader, GetOEMCP, CreateThread, ExitThread, HeapReAlloc, GetSystemTimeAsFileTime, DecodePointer, EncodePointer, RtlUnwindEx, RtlLookupFunctionEntry, GetStartupInfoW, GetCommandLineW, FindResourceExW, SearchPathW, Sleep, GetProfileIntW, InitializeCriticalSectionAndSpinCount, GetTickCount, GetNumberFormatW, GetWindowsDirectoryW, GetTempPathW, GetTempFileNameW, GetFileTime, GetFileSizeEx, GetFileAttributesW, FileTimeToLocalFileTime, GetFileAttributesExW, SetErrorMode, FileTimeToSystemTime, GlobalGetAtomNameW, lstrlenA, GetFullPathNameW, GetACP, GetCPInfo, RaiseException, GetStringTypeW, GetVolumeInformationW, FindFirstFileW, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, CreateFileW, lstrcmpiW, GetThreadLocale, lstrcpyW, DeleteFileW, TlsFree, DeleteCriticalSection, LocalReAlloc, TlsSetValue, GlobalHandle, GlobalReAlloc, TlsAlloc, InitializeCriticalSection, EnterCriticalSection, TlsGetValue, LeaveCriticalSection, LocalAlloc, GlobalFlags, GetCurrentDirectoryW, ReleaseActCtx, CreateActCtxW, CopyFileW, GlobalSize, FormatMessageW, LocalFree, MulDiv, GlobalFindAtomW, GetVersionExW, CompareStringW, GlobalUnlock, GlobalFree, FreeResource, GetCurrentProcessId, GlobalAddAtomW, GetPrivateProfileStringW, lstrlenW, WritePrivateProfileStringW, GetPrivateProfileIntW, CreateEventW, SuspendThread, SetEvent, WaitForSingleObject, ResumeThread, SetThreadPriority, CloseHandle, lstrcmpA, GlobalDeleteAtom, GetCurrentThread, GetCurrentThreadId, GetUserDefaultUILanguage, ConvertDefaultLocale, GetSystemDefaultUILanguage, GetModuleFileNameW, GetLocaleInfoW, ActivateActCtx, LoadLibraryW, GetLastError, DeactivateActCtx, SetLastError, WideCharToMultiByte, GlobalLock, lstrcmpW, GlobalAlloc, GetModuleHandleW, HeapAlloc, FreeLibrary, GetProcessHeap, HeapFree, IsBadReadPtr, LoadLibraryA, GetProcAddress, VirtualFree, VirtualProtect, VirtualAlloc, MultiByteToWideChar, TerminateThread, ExitProcess, FindResourceW, LoadResource, LockResource

Copyright null 2021

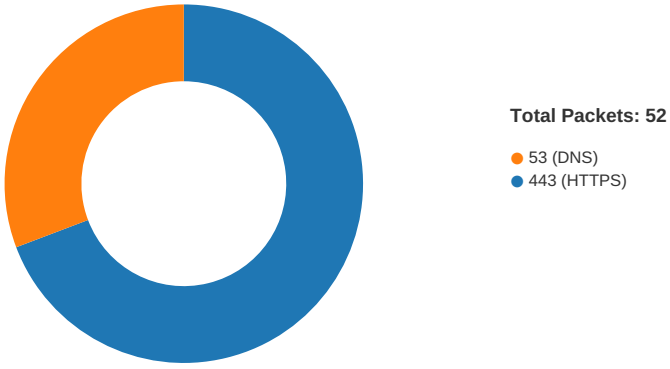
DLL	Import
USER32.dll	SetMenuDefaultItem, PostThreadMessageW, CreateMenu, IsMenu, UpdateLayeredWindow, UnionRect, MonitorFromPoint, TranslateMDISysAccel, DrawMenuBar, DefMDIChildProcW, DefFrameProcW, RegisterClipboardFormatW, CopyImage, GetIconInfo, EnableScrollBar, HideCaret, InvertRect, GetMenuDefaultItem, UnpackDDElParam, ReuseDDElParam, LoadImageW, InsertMenuItemW, TranslateAcceleratorW, LockWindowUpdate, BringWindowToTop, SetCursorPos, CreateAcceleratorTableW, LoadAcceleratorsW, GetKeyboardState, GetKeyboardLayout, ToUnicodeEx, DrawFocusRect, DrawFrameControl, DrawEdge, DrawIconEx, DrawStateW, SetClassLongPtrW, GetAsyncKeyState, NotifyWinEvent, CreatePopupMenu, DestroyAcceleratorTable, SetParent, RedrawWindow, SetWindowRgn, IsZoomed, UnregisterClassW, MessageBeep, GetNextDlgGroupItem, InvalidateRgn, SetRect, IsRectEmpty, CopyAcceleratorTableW, OffsetRect, CharNextW, IntersectRect, LoadMenuW, CharUpperW, DestroyIcon, WaitMessage, ReleaseCapture, WindowFromPoint, SetCapture, GetSysColorBrush, LoadCursorW, SetLayeredWindowAttributes, SetRectEmpty, KillTimer, SetTimer, InvalidateRect, RealChildWindowFromPoint, DeleteMenu, EndPaint, BeginPaint, GetWindowDC, ClientToScreen, GrayStringW, DrawTextExW, DrawTextW, TabbedTextOutW, FillRect, SystemParametersInfoW, DestroyMenu, IsClipboardFormatAvailable, InflateRect, GetMenuStringW, InsertMenuW, RemoveMenu, ShowWindow, SetWindowTextW, IsDialogMessageW, SetDlgItemTextW, CheckDlgButton, RegisterWindowMessageW, SendDlgItemMessageW, SendDlgItemMessageA, WinHelpW, IsChild, GetCapture, GetClassNameW, GetClassLongPtrW, SetPropW, GetPropW, RemovePropW, SetFocus, GetWindowTextLengthW, GetWindowTextW, GetForegroundWindow, BeginDeferWindowPos, EndDeferWindowPos, GetTopWindow, GetWindowLongPtrW, SetWindowLongPtrW, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, MonitorFromWindow, GetMonitorInfoW, MapWindowPoints, ScrollWindow, TrackPopupMenu, SetMenu, SetScrollRange, GetScrollRange, SetScrollPos, GetScrollPos, SetForegroundWindow, ShowScrollBar, UpdateWindow, GetSubMenu, GetMenuItemID, GetMenuItemCount, CreateWindowExW, GetClassInfoExW, GetClassInfoW, RegisterClassW, GetSysColor, AdjustWindowRectEx, GetWindowRect, ScreenToClient, EqualRect, DeferWindowPos, GetScrollInfo, SetScrollInfo, PtInRect, SetWindowPlacement, GetWindowPlacement, GetDlgCtrlID, DefWindowProcW, CallWindowProcW, GetMenu, GetWindow, SetWindowContextHelpId, FrameRect, GetUpdateRect, GetWindowRgn, DestroyCursor, SubtractRect, MapVirtualKeyExW, IsCharLowerW, GetDoubleClickTime, MapDialogRect, SetWindowPos, MapVirtualKeyW, GetKeyNameTextW, ReleaseDC, GetDC, CopyRect, GetDesktopWindow, SetActiveWindow, CreateDialogIndirectParamW, CharUpperBuffW, CopyIcon, EmptyClipboard, CloseClipboard, SetClipboardData, GetMenuItemInfoW, OpenClipboard, DestroyWindow, IsWindow, GetDlgItem, GetNextDlgTabItem, EndDialog, GetWindowThreadProcessId, GetLastActivePopup, IsWindowEnabled, MessageBoxW, ShowOwnedPopups, SetCursor, SetWindowsHookExW, CallNextHookEx, GetMessageW, TranslateMessage, DispatchMessageW, GetActiveWindow, IsWindowVisible, GetKeyState, PeekMessageW, GetCursorPos, ValidateRect, SetMenuItemBitmaps, GetMenuCheckMarkDimensions, LoadBitmapW, GetFocus, GetParent, ModifyMenuW, GetMenuState, EnableMenuItem, CheckMenuItem, PostMessageW, PostQuitMessage, GetSystemMetrics, LoadIconW, EnableWindow, GetClientRect, IsIconic, GetSystemMenu, SendMessageW, AppendMenuW, DrawIcon, MoveWindow, GetWindowLongW, SetWindowLongW, EnumDisplayMonitors
GDI32.dll	CreateSolidBrush, CreateHatchBrush, CreateDIBitmap, CreateCompatibleBitmap, GetTextMetricsW, EnumFontFamiliesW, GetTextCharsetInfo, SetRectRgn, CombineRgn, GetMapMode, DPtoLP, GetBkColor, GetTextColor, GetRgnBox, CreateDIBSection, CreateRoundRectRgn, CreatePolygonRgn, CreateEllipticRgn, Polyline, Ellipse, Polygon, CreatePalette, GetPaletteEntries, GetNearestPaletteIndex, RealizePalette, GetSystemPaletteEntries, OffsetRgn, SetDIBColorTable, CreatePen, SetPixel, Rectangle, EnumFontFamiliesExW, LPtoDP, GetWindowOrgEx, GetViewportOrgEx, PtInRegion, FillRgn, FrameRgn, GetBoundsRect, ExtFloodFill, SetPaletteEntries, GetTextFaceW, SetPixelV, RectVisible, PtVisible, GetPixel, GetObjectType, TextOutW, SelectPalette, GetStockObject, CreatePatternBrush, DeleteDC, ExtSelectClipRgn, ScaleWindowExtEx, SetWindowExtEx, OffsetWindowOrgEx, SetWindowOrgEx, ScaleViewportExtEx, SetViewportExtEx, OffsetViewportOrgEx, SetViewportOrgEx, SelectObject, StretchBlt, CreateBitmap, GetWindowExtEx, GetViewportExtEx, CreateRectRgn, SelectClipRgn, DeleteObject, SetLayout, GetLayout, SetTextAlign, MoveToEx, LineTo, IntersectClipRect, ExcludeClipRect, GetClipBox, SetMapMode, SetROP2, SetPolyFillMode, SetBkMode, RestoreDC, SaveDC, GetTextExtentPoint32W, ExtTextOutW, BitBlt, CreateCompatibleDC, CreateFontIndirectW, CreateDCW, CopyMetaFileW, GetDeviceCaps, GetObjectW, SetBkColor, SetTextColor, PatBlt, CreateRectRgnIndirect, Escape
MSIMG32.dll	AlphaBlend, TransparentBlt
COMDLG32.dll	GetFileTitleW
WINSPOOL.DRV	ClosePrinter, OpenPrinterW, DocumentPropertiesW
ADVAPI32.dll	RegEnumKeyExW, RegQueryValueExW, RegOpenKeyExW, RegCreateKeyExW, RegSetValueExW, RegDeleteValueW, RegDeleteKeyW, RegEnumKeyW, RegQueryValueW, RegCloseKey, RegEnumValueW
SHELL32.dll	SHAppBarMessage, SHGetFileInfoW, ShellExecuteW, DragFinish, DragQueryFileW, SHBrowseForFolderW, SHGetSpecialFolderLocation, SHGetPathFromIDListW, SHGetDesktopFolder
COMCTL32.dll	ImageList_GetIconSize
SHLWAPI.dll	PathFindFileNameW, PathStripToRootW, PathIsUNCW, PathFindExtensionW, PathRemoveFileSpecW
ole32.dll	OleInitialize, CoFreeUnusedLibraries, OleUninitialize, CoInitializeEx, CreateILockBytesOnHGlobal, StgCreateDocfileOnILockBytes, StgOpenStorageOnILockBytes, CoGetClassObject, CoInitialize, CoUninitialize, OleCreateMenuDescriptor, CoTaskMemAlloc, ReleaseStgMedium, CoTaskMemFree, OleDestroyMenuDescriptor, OleTranslateAccelerator, IsAccelerator, OleLockRunning, CreateStreamOnHGlobal, OleIsCurrentClipboard, OleFlushClipboard, DoDragDrop, CLSIDFromString, CLSIDFromProgID, CoCreateGuid, RevokeDragDrop, CoLockObjectExternal, RegisterDragDrop, OleGetClipboard, OleDuplicateData, CoRegisterMessageFilter, CoCreateInstance, CoRevokeClassObject
OLEAUT32.dll	SysFreeString, VarBstrFromDate, VariantCopy, SafeArrayDestroy, SystemTimeToVariantTime, VariantTimeToSystemTime, OleCreateFontIndirect, SysStringLen, VariantInit, VariantChangeType, VariantClear, SysAllocStringLen, SysAllocString
oledlg.dll	OleUIBusyW
WS2_32.dll	WSAIoctl, htons, inet_ntoa, gethostbyname, gethostname, WSASocketW, WSAStartup, ntohs, recv, bind
OLEACC.dll	LresultFromObject, AccessibleObjectFromWindow, CreateStdAccessibleObject
gdiplus.dll	GdipGetImagePixelFormat, GdipGetImageHeight, GdipGetImageWidth, GdipCloneImage, GdipDrawImageRectI, GdipSetInterpolationMode, GdipGetImagePaletteSize, GdiplusShutdown, GdiplusStartup, GdipCreateBitmapFromHBITMAP, GdipDisposeImage, GdipDeleteGraphics, GdipAlloc, GdipFree, GdipGetImagePalette, GdipCreateBitmapFromStream, GdipCreateBitmapFromScan0, GdipBitmapLockBits, GdipBitmapUnlockBits, GdipGetImageGraphicsContext, GdipCreateFromHDC, GdipDrawImageI
IMM32.dll	ImmGetOpenStatus, ImmReleaseContext, ImmGetContext
WINMM.dll	PlaySoundW

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2021 10:23:23.492737055 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:23.493050098 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:23.493232012 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:23.493341923 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:23.493448019 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:23.493484020 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:23.493712902 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:23.493824005 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:23.493865967 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:23.503756046 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.503794909 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.503830910 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.503869057 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.503894091 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.503979921 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.504018068 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.504620075 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.504646063 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.504668951 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.504837036 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.504875898 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.505203962 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.505242109 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.505482912 CET	443	49696	204.79.197.200	192.168.2.4

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2021 10:23:23.505522966 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.505681992 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.505717039 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.505799055 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.505855083 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:23.506150961 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.506251097 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.506513119 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.506541967 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.626178026 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:23.626334906 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.676939011 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.677278996 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.677455902 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.677529097 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.677571058 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.677608013 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.677635908 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.677711964 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.677747011 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.677762985 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.677767992 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.686454058 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.686647892 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.686887026 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.687319994 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.687814951 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.687844992 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.687937021 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.688262939 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.688580036 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.688678026 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.688756943 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.688922882 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.689089060 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.689160109 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.689368963 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.689434052 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.689743042 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.689924002 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.720083952 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.720293045 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:28.755439043 CET	443	49696	204.79.197.200	192.168.2.4
Jan 24, 2021 10:23:28.755672932 CET	49696	443	192.168.2.4	204.79.197.200
Jan 24, 2021 10:23:37.462538004 CET	49683	443	192.168.2.4	40.126.31.135
Jan 24, 2021 10:23:37.462593079 CET	49682	443	192.168.2.4	40.126.31.135
Jan 24, 2021 10:23:37.462704897 CET	49683	443	192.168.2.4	40.126.31.135
Jan 24, 2021 10:23:37.462745905 CET	49682	443	192.168.2.4	40.126.31.135
Jan 24, 2021 10:23:37.499459982 CET	443	49683	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.499675989 CET	443	49683	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.499989986 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.500017881 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.553977013 CET	443	49683	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.554744005 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645104885 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645154953 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645194054 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645241976 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645297050 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645302057 CET	49682	443	192.168.2.4	40.126.31.135
Jan 24, 2021 10:23:37.645345926 CET	49682	443	192.168.2.4	40.126.31.135
Jan 24, 2021 10:23:37.645354986 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645435095 CET	49682	443	192.168.2.4	40.126.31.135
Jan 24, 2021 10:23:37.645481110 CET	443	49682	40.126.31.135	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2021 10:23:37.645541906 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645591974 CET	443	49682	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645615101 CET	49682	443	192.168.2.4	40.126.31.135
Jan 24, 2021 10:23:37.645648003 CET	443	49683	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645689964 CET	443	49683	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645725965 CET	443	49683	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645764112 CET	443	49683	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645801067 CET	443	49683	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645807028 CET	49683	443	192.168.2.4	40.126.31.135
Jan 24, 2021 10:23:37.645837069 CET	443	49683	40.126.31.135	192.168.2.4
Jan 24, 2021 10:23:37.645838022 CET	49683	443	192.168.2.4	40.126.31.135
Jan 24, 2021 10:23:37.645874023 CET	443	49683	40.126.31.135	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2021 10:23:13.309921980 CET	55854	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:13.332984924 CET	53	55854	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:13.920188904 CET	64549	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:13.943337917 CET	53	64549	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:14.716948032 CET	63153	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:14.740032911 CET	53	63153	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:15.511826038 CET	52991	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:15.535604000 CET	53	52991	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:16.968394041 CET	53700	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:16.991550922 CET	53	53700	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:17.860275030 CET	51726	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:17.883440971 CET	53	51726	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:19.125066996 CET	56794	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:19.150897026 CET	53	56794	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:19.983750105 CET	56534	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:20.006917000 CET	53	56534	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:20.637813091 CET	56627	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:20.664338112 CET	53	56627	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:21.486450911 CET	56621	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:21.512278080 CET	53	56621	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:22.337990046 CET	63116	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:22.361217976 CET	53	63116	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:23.166867018 CET	64078	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:23.201261997 CET	53	64078	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:37.773974895 CET	64801	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:37.796924114 CET	53	64801	8.8.8.8	192.168.2.4
Jan 24, 2021 10:23:40.221301079 CET	61721	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:23:40.253931046 CET	53	61721	8.8.8.8	192.168.2.4
Jan 24, 2021 10:24:03.344569921 CET	51255	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:24:03.370654106 CET	53	51255	8.8.8.8	192.168.2.4
Jan 24, 2021 10:24:32.072946072 CET	61522	53	192.168.2.4	8.8.8.8
Jan 24, 2021 10:24:32.110757113 CET	53	61522	8.8.8.8	192.168.2.4

HTTP Request Dependency Graph

- 110.92.66.246:13527

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49744	110.92.66.246	13527	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 10:23:44.673149109 CET	405	OUT	GET /\ HTTP/1.1 Connection: Upgrade Sec-WebSocket-Key: FCzEFfJJGECxZCsRaGKFlJqHW Sec-WebSocket-Version: 13 Upgrade: websocket Sec-WebSocket-Extensions: permessage-deflate; client_max_window_bits Host: 110.92.66.246:13527

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	110.92.66.246	13527	192.168.2.4	49744	C:\Users\user\zT6Nm@i4\PMRunner64.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 10:23:44.892343998 CET	406	IN	HTTP/1.1 101 Switching Protocols Connection: Upgrade Upgrade: WebSocket Sec-WebSocket-Accept: J6aOSpBDe/Sy9K0gZYEbzVgYYn8= Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49745	110.92.66.246	13527	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9 #U8868@i4.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 10:23:50.193909883 CET	407	OUT	GET /\ HTTP/1.1 Connection: Upgrade Sec-WebSocket-Key: hVvGEJDDITDIJDJeQLtIKCsnC Sec-WebSocket-Version: 13 Upgrade: websocket Sec-WebSocket-Extensions: permessage-deflate; client_max_window_bits Host: 110.92.66.246:13527

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	110.92.66.246	13527	192.168.2.4	49745	C:\Users\user\zT6Nm@i4\PMRunner64.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 10:23:50.387290955 CET	407	IN	HTTP/1.1 101 Switching Protocols Connection: Upgrade Upgrade: WebSocket Sec-WebSocket-Accept: Zt5ptgVJyb+M21WHDTqV3GKtCPo= Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49746	110.92.66.246	13527	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9 #U8868@i4.exe

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 10:23:54.288530111 CET	607	OUT	GET /\ HTTP/1.1 Connection: Upgrade Sec-WebSocket-Key: IKBXBepAaaBfkIYjnCKuMRKkF Sec-WebSocket-Version: 13 Upgrade: websocket Sec-WebSocket-Extensions: permessage-deflate; client_max_window_bits Host: 110.92.66.246:13527

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	110.92.66.246	13527	192.168.2.4	49746	C:\Users\user\zT6Nm@i4\PMRunner64.exe

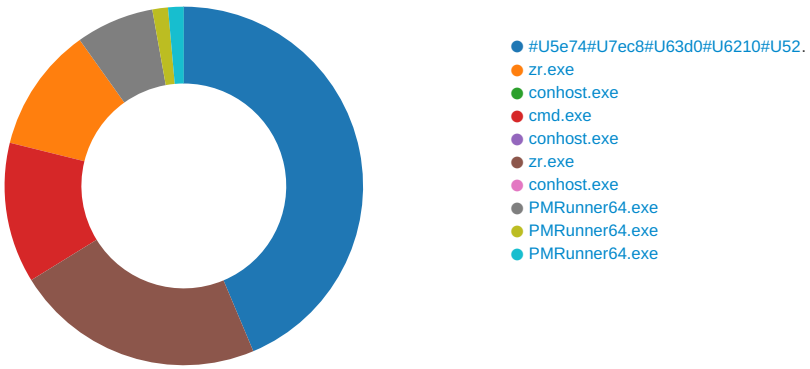
Timestamp	kBytes transferred	Direction	Data
Jan 24, 2021 10:23:54.507450104 CET	607	IN	HTTP/1.1 101 Switching Protocols Connection: Upgrade Upgrade: WebSocket Sec-WebSocket-Accept: Kj9tthj3c2jmoKNtKOHJo/S2svQ= Content-Length: 0

Copyright null 2021

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: #U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe PID: 4164 Parent PID: 5908

General

Start time:	10:23:18
Start date:	24/01/2021
Path:	C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\#U5e74#U7ec8#U63d0#U6210#U5206#U7ea2#U6838#U5bf9#U8868@i4.exe'
Imagebase:	0x140000000
File size:	3150336 bytes
MD5 hash:	6665909A2652C5860FD874CB15C3991C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1800088B2	CreateDirectoryW
C:\Users\user\zT6Nm@i4\K_FPS64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	180007B43	CreateFileW
C:\Users\user\zT6Nm@i4\KK.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	180007B43	CreateFileW
C:\Users\user\zT6Nm@i4\PMRunner64.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	180007B43	CreateFileW
C:\Users\user\zT6Nm@i4\zr.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	180007B43	CreateFileW
C:\Users\user\zT6Nm@i4\TXP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1800088B2	CreateDirectoryW
C:\Users\user\zT6Nm@i4\TXP\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1800088B2	CreateDirectoryW
C:\Users\user\zT6Nm@i4\TXP\Windows\Start Menu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1800088B2	CreateDirectoryW
C:\Users\user\zT6Nm@i4\TXP\Windows\Start Menu\Programs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1800088B2	CreateDirectoryW
C:\Users\user\zT6Nm@i4\TXP\Windows\Start Menu\Programs\Startup	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1800088B2	CreateDirectoryW
C:\Users\user\zT6Nm@i4\ru2.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	18000894E	CreateFileW
C:\Users\user\zT6Nm@i4\copy.bat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	18000894E	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\run003.lnk	success or wait	1	18000996E	DeleteFileW
C:\Users\user\zT6Nm@i4\copy.bat	success or wait	1	180009D20	DeleteFileW
C:\Users\user\zT6Nm@i4\111.7z	success or wait	1	180009D3D	DeleteFileW
C:\Users\user\zT6Nm@i4\zr.exe	success or wait	1	180009D5A	DeleteFileW
C:\Users\user\zT6Nm@i4\run.lnk	success or wait	1	180009E09	DeleteFileW
C:\Users\user\zT6Nm@i4\run001.lnk	success or wait	1	180009E26	DeleteFileW
C:\Users\user\zT6Nm@i4\ru2.url	success or wait	1	180009E43	DeleteFileW
C:\Users\user\zT6Nm@i4\TXP\Windows\Start Menu\Programs\Startup\Realtek???????? .lnk	success or wait	1	180009EC8	DeleteFileW
C:\ProgramData\Microsoft\zr.exe	success or wait	1	180009EE5	DeleteFileW
C:\ProgramData\Microsoft\111.7z	success or wait	1	180009F02	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\K_FPS64.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 73 6c 2e b1 37 0d 40 e2 37 0d 40 e2 37 0d 40 e2 8a 42 d6 e2 36 0d 40 e2 10 cb 2d e2 30 0d 40 e2 10 cb 3b e2 2c 0d 40 e2 37 0d 41 e2 07 0f 40 e2 3e 75 c3 e2 a8 0d 40 e2 3e 75 d5 e2 3d 0d 40 e2 3e 75 c4 e2 48 0d 40 e2 3e 75 ca e2 2b 0d 40 e2 3e 75 d2 e2 36 0d 40 e2 29 5f d4 e2 36 0d 40 e2 3e 75 d1 e2 36 0d 40 e2 52 69 63 68 37 0d 40 e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......sl..7.@.7.@.7.@..B.. 6.@...- .0.@...;.,.@.7.A...@.>u.. ..@.>u..=.@.>u..H.@.>u..+ .@.>u ..6.@.)_..6.@.>u..6.@.Ric h7.@................	success or wait	19	180007BC7	WriteFile
C:\Users\user\zT6Nm@i4\KK.txt	unknown	16384	72 63 28 07 25 63 e7 51 c1 71 85 92 09 1c 3c 63 66 57 ec 26 f3 2d a3 a8 18 53 50 23 d8 01 c0 cb 7c 4f eb b2 9c 25 27 71 35 b6 58 72 56 4e 5c b5 d3 87 83 d1 40 4a b3 d8 90 29 46 d5 59 5a c0 8d a3 0b d9 25 82 b2 e2 2c 80 08 a3 79 c8 73 c2 78 96 d3 b4 ad ea fc 43 cb c9 a0 e6 8d 4c a8 79 04 27 f3 cb a2 98 0d 56 f0 be 43 6b 9a f8 9d fa 49 12 34 27 4c e9 62 a0 00 05 8e 65 27 dd 51 f2 92 f0 51 53 9a 80 c7 bd 77 e4 78 67 46 e1 85 af bb e4 4c d6 51 0a f1 1c d7 e0 fe 1a 1d 2f cb 9e b4 dc 05 8d 27 76 36 3d d1 79 6a 1c 90 74 8b 68 d8 6e 94 69 b4 61 25 67 8f c7 3a 23 01 5c b5 51 b4 6c 4e 7f 8b b5 72 dc bd 68 74 f9 9f e4 ff 79 81 86 49 8c fb 6b 1b 41 54 75 2f f3 11 5f fd e0 6a d4 5f 42 9f fc bc 3f 25 89 a9 11 c8 9b 2d e9 8c 0a 4e 7c 09 47 1a b4 0c c8 7c 31 04 56 92 b0	rc(.%c.Q.q....<cfW.&.- ...SP#.. ..|O...%'q5.XrVN\.....@J...) F.YZ.....%...,...y.s.x......C... ..L.y.'.....V..Ck....I.4'L.b.. ..e'.Q...QS....w.xgF.....L.Q.. ....../......'v6=.yj..t.h.n.i. a%g..:#.\.Q.lN...r..ht....y..I ..k.ATu/.._..j._B...?%.....-.. .N|.G....|1.V..	success or wait	14	180007BC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\PMRunner64.exe	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 04 24 87 b9 65 4a d4 b9 65 4a d4 b9 65 4a d4 0d f9 bb d4 bc 65 4a d4 0d f9 b9 d4 2b 65 4a d4 0d f9 b8 d4 b4 65 4a d4 82 3b 49 d5 b1 65 4a d4 82 3b 4f d5 98 65 4a d4 82 3b 4e d5 ad 65 4a d4 64 9a 81 d4 be 65 4a d4 b9 65 4b d4 3e 65 4a d4 2e 3b 43 d5 bd 65 4a d4 2e 3b 4a d5 b8 65 4a d4 2b 3b b5 d4 b8 65 4a d4 b9 65 dd d4 b8 65 4a d4 2e 3b 48 d5 b8 65 4a d4 52 69 63 68 b9 65 4a	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........$..eJ..eJ..eJ......e J.....+eJ......eJ..;I..eJ..;O. .eJ..;N..eJ.d....eJ..eK.>eJ..; C..eJ..;J..eJ.+;...eJ..e...eJ. .;H..eJ.Rich.eJ	success or wait	17	180007BC7	WriteFile
C:\Users\user\zT6Nm@i4\zr.exe	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 80 fa b8 c7 c4 9b d6 94 c4 9b d6 94 c4 9b d6 94 bf 87 da 94 c6 9b d6 94 ab 84 dd 94 c7 9b d6 94 47 87 d8 94 cc 9b d6 94 ab 84 dc 94 cf 9b d6 94 ab 84 d2 94 c6 9b d6 94 4a 93 89 94 c5 9b d6 94 c4 9b d7 94 4c 9b d6 94 47 93 8b 94 cd 9b d6 94 f2 bd dd 94 ba 9b d6 94 df 06 7c 94 de 9b d6 94 df 06 48 94 c7 9b d6 94 03 9d d0 94 c5 9b d6 94 52 69 63 68 c4 9b d6 94 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................. ....G.................. ....J...........L...G......... ....|.......H............. Rich...........	success or wait	29	180007BC7	WriteFile
C:\Users\user\zT6Nm@i4\ru2.url	unknown	65	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 55 52 4c 3d 66 69 6c 65 3a 2f 2f 2f 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 7a 54 36 4e 6d 40 69 34 5c 72 75 6e 30 30 31 2e 6c 6e 6b	[InternetShortcut].URL=file :// /C:\Users\user\zT6Nm@i4\ run001.lnk	success or wait	1	180008A49	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\copy.bat	unknown	148	63 6f 70 79 20 20 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 7a 54 36 4e 6d 40 69 34 5c 7a 72 2e 65 78 65 22 20 22 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 5c 4d 69 63 72 6f 73 6f 66 74 5c 7a 72 2e 65 78 65 22 0a 0d 63 6f 70 79 20 20 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 7a 54 36 4e 6d 40 69 34 5c 31 31 31 2e 37 7a 22 20 22 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 5c 4d 69 63 72 6f 73 6f 66 74 5c 31 31 31 2e 37 7a 22 0a 0d	copy "C:\Users\user\zT6Nm@i4\zr.exe" "C:\ProgramData\Microsoft\zr.exe"..copy "C:\Users\user\zT6Nm@i4\111.7z" "C:\ProgramData\Microsoft\111.7z"..	success or wait	1	180008A49	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	LangID	binary	09 04	success or wait	1	180009CF8	ShellExecuteW
HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Windows\System32\cmd.exe.FriendlyAppName	unicode	Windows Command Processor	success or wait	1	180009CF8	ShellExecuteW
HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Windows\System32\cmd.exe.ApplicationCompany	unicode	Microsoft Corporation	success or wait	1	180009CF8	ShellExecuteW

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

Analysis Process: zr.exe PID: 6340 Parent PID: 4164

General

Start time:	10:23:22
Start date:	24/01/2021
Path:	C:\Users\user\zT6Nm@i4\zr.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\zT6Nm@i4\zr.exe' a 'C:\Users\user\zT6Nm@i4\111.7z' 'C:\Users\user\zT6Nm@i4\TXP*'
Imagebase:	0x400000
File size:	461088 bytes
MD5 hash:	045FCBE6C174AFA9A6A998BDD6F9FAD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\111.7z	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40664D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\111.7z	unknown	8	37 7a bc af 27 1c 00 04	7z..'...	success or wait	1	406910	WriteFile
C:\Users\user\zT6Nm@i4\111.7z	unknown	24	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	success or wait	1	406910	WriteFile
C:\Users\user\zT6Nm@i4\111.7z	unknown	627	e0 06 fe 02 6c 5d 00 26 00 30 00 21 3f c0 fb b2 6f 1e b0 31 62 eb f2 ac 56 13 ea ae 8f 70 53 d1 47 eb a0 55 a8 3e 89 d5 d1 f3 f7 ac 16 8e ee 8d 81 9f da aa d4 47 67 14 2e 31 3e b7 86 10 fa 3b c5 8a b1 08 d5 3e 7c 2a d5 b6 50 06 d6 44 a9 48 86 74 61 9f a1 de 10 f1 16 30 75 72 34 9d c6 46 36 e0 87 66 ee 64 12 32 d7 01 56 7a 72 d4 c2 0b 0d 0f 23 0b 25 e0 8f 61 00 e1 9b 1a 3f b8 36 b8 6a 38 4b 4d cf c4 24 fc 10 03 55 68 e4 a3 92 a4 7b fc 7b d2 5f da 32 31 83 21 94 11 85 ce 83 75 69 38 9c aa 59 2a 1a c8 4d e8 80 0f e5 4b 00 4c 2b e2 36 7a 45 30 07 80 c2 01 03 53 3d 97 c6 63 e4 9d bb 80 e2 89 ad a0 98 b5 34 f5 48 e0 8c dd 45 7d f5 ab 7a a1 20 44 18 f1 1a ac b9 fd 6b c6 06 1c 50 3a 33 b9 fd 95 63 39 bb 03 af 93 fa e1 c3 37 8d 22 c3 17 be ed 56 a6 a2 b5 86 d3 dd	....l].&.0.!?...o..1b...V....p S.G..U.>.....Gg..1>. ...;.....>|*..P..D.H.ta.....0 ur4..F6..f.d.2..Vzr.....#.%..a ....?.6.j8KM..$...Uh....{.{._. 21.!.....ui8..Y*..M....K.L+.6z E0.....S=..c.....4.H...E} ..z. D.....k...P:3...c9..... .7."....V.....	success or wait	3	406910	WriteFile
C:\Users\user\zT6Nm@i4\111.7z	unknown	35	17 06 82 74 01 09 80 b0 00 07 0b 01 00 01 23 03 01 01 05 5d 00 10 00 00 0c 82 72 0a 01 06 2a f3 89 00 00	...t.....#....]......r...*....	success or wait	1	406910	WriteFile
C:\Users\user\zT6Nm@i4\111.7z	unknown	24	a3 41 60 ea 24 03 00 00 00 00 00 00 23 00 00 00 00 00 00 00 e9 1e 38 e1	.A`.$.....#.....8.	success or wait	1	406910	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\TXP\Windows\Start Menu\Programs\Startup\Realtek???????? .lnk	unknown	4194304	success or wait	1	4067F7	ReadFile
C:\Users\user\zT6Nm@i4\TXP\Windows\Start Menu\Programs\Startup\Realtek???????? .lnk	unknown	4194304	end of file	1	4067F7	ReadFile

Analysis Process: conhost.exe PID: 6356 Parent PID: 6340

General

Start time:	10:23:22
Start date:	24/01/2021
Path:	C:\Windows\System32\conhost.exe

Copyright null 2021

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6648 Parent PID: 4164

General

Start time:	10:23:24
Start date:	24/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /C 'C:\Users\user\zT6Nm@i4\copy.bat'
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\zr.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FF6220758E5	CopyFileExW
C:\ProgramData\Microsoft\111.7z	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FF6220758E5	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\zr.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 80 fa b8 c7 c4 9b d6 94 c4 9b d6 94 c4 9b d6 94 bf 87 da 94 c6 9b d6 94 ab 84 dd 94 c7 9b d6 94 47 87 d8 94 cc 9b d6 94 ab 84 dc 94 cf 9b d6 94 ab 84 d2 94 c6 9b d6 94 4a 93 89 94 c5 9b d6 94 c4 9b d7 94 4c 9b d6 94 47 93 8b 94 cd 9b d6 94 f2 bd dd 94 ba 9b d6 94 df 06 7c 94 de 9b d6 94 df 06 48 94 c7 9b d6 94 03 9d d0 94 c5 9b d6 94 52 69 63 68 c4 9b d6 94 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....G.................. ....J...........L...G......... ....|.......H............ Rich...........	success or wait	4	7FF6220758E5	CopyFileExW
C:\ProgramData\Microsoft\111.7z	0	871	37 7a bc af 27 1c 00 04 a3 41 60 ea 24 03 00 00 00 00 00 00 23 00 00 00 00 00 00 00 e9 1e 38 e1 e0 06 fe 02 6c 5d 00 26 00 30 00 21 3f c0 fb b2 6f 1e b0 31 62 eb f2 ac 56 13 ea ae 8f 70 53 d1 47 eb a0 55 a8 3e 89 d5 d1 f3 f7 ac 16 8e ee 8d 81 9f da aa d4 47 67 14 2e 31 3e b7 86 10 fa 3b c5 8a b1 08 d5 3e 7c 2a d5 b6 50 06 d6 44 a9 48 86 74 61 9f a1 de 10 f1 16 30 75 72 34 9d c6 46 36 e0 87 66 ee 64 12 32 d7 01 56 7a 72 d4 c2 0b 0d 0f 23 0b 25 e0 8f 61 00 e1 9b 1a 3f b8 36 b8 6a 38 4b 4d cf c4 24 fc 10 03 55 68 e4 a3 92 a4 7b fc 7b d2 5f da 32 31 83 21 94 11 85 ce 83 75 69 38 9c aa 59 2a 1a c8 4d e8 80 0f e5 4b 00 4c 2b e2 36 7a 45 30 07 80 c2 01 03 53 3d 97 c6 63 e4 9d bb 80 e2 89 ad a0 98 b5 34 f5 48 e0 8c dd 45 7d f5 ab 7a a1 20 44 18 f1 1a ac b9 fd 6b	7z..'....A`.$.......#......... 8.....l].&.0.!?...o..1b...V... .pS.G..U.>..............Gg..1 >....;.....>\|*..P..D.H.ta..... .0ur4..F6..f.d.2..Vzr.....#.%. .a....?.6.j8KM..$...Uh....{.{. _.21.!.....ui8..Y*..M....K.L+. 6zE0.....S=..c..........4.H... E}..z. D......k	success or wait	1	7FF6220758E5	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\copy.bat	unknown	8191	success or wait	3	7FF62207F404	ReadFile
C:\Users\user\zT6Nm@i4\zr.exe	unknown	512	success or wait	1	7FF622076290	ReadFile
C:\Users\user\zT6Nm@i4\111.7z	unknown	512	success or wait	1	7FF622076290	ReadFile
C:\Users\user\zT6Nm@i4\copy.bat	unknown	8191	end of file	1	7FF62207F404	ReadFile
C:\Users\user\zT6Nm@i4\copy.bat	unknown	8191	end of file	1	7FF62207F404	ReadFile

Analysis Process: conhost.exe PID: 6700 Parent PID: 6648

General

Start time:	10:23:24
Start date:	24/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: zr.exe PID: 6800 Parent PID: 6796

General

Start time:	10:23:28
Start date:	24/01/2021
Path:	C:\ProgramData\Microsoft\zr.exe
Wow64 process (32bit):	true
Commandline:	'C:\ProgramData\Microsoft\zr.exe' x C:\ProgramData\Microsoft\111.7z -y
Imagebase:	0x400000
File size:	461088 bytes
MD5 hash:	045FCBE6C174AFA9A6A998BDD6F9FAD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	405288	CreateDirectoryW
C:\ProgramData\Microsoft\Windows\Start Menu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405288	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\Start Menu\Programs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405288	CreateDirectoryW
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405288	CreateDirectoryW
C:\ProgramData\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405288	CreateDirectoryW
C:\ProgramData\Microsoft\Windows\Start Menu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405288	CreateDirectoryW
C:\ProgramData\Microsoft\Windows\Start Menu\Programs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405288	CreateDirectoryW
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405288	CreateDirectoryW
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup \Realtek???????? .lnk	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40664D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Realtek???????? .lnk	unknown	1791	4c 00 00 00 01 14 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 db 40 00 00 20 00 00 00 00 4b 90 c8 93 ea d6 01 00 4b 90 c8 93 ea d6 01 00 4b 90 c8 93 ea d6 01 58 25 04 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2c 01 3a 00 1f 44 47 1a 03 59 72 3f a7 44 89 c5 55 95 fe 6b 30 ee 26 00 01 00 26 00 ef be 10 00 00 00 f5 85 c9 e8 13 2d d5 01 8a 19 6b 8d 32 f2 d6 01 58 2c 7e 8d 32 f2 d6 01 14 00 86 00 74 00 1e 00 43 46 53 46 18 00 31 00 00 00 00 00 38 52 ea 4a 37 00 7a 54 36 4e 6d 40 69 34 00 00 00 00 74 1a 59 5e 96 df d3 48 8d 67 17 33 bc ee 28 ba c5 cd fa df 9f 67 56 41 89 47 c5 c7 6b c0 b6 7f 42 00 09 00 04 00 ef be 38 52 ea 4a 38 52 ea 4a 2e 00 00 00 33 58 01 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 d1 9f 00 7a 00 54 00 36	L.....F.@.. ....K .....K.....K.....X%..... .....,:...DG..Yr?.D ..U..k0.&...&.....-.... k.2...X,~.2.....t...CFSF..1. ....8R.J7.zT6Nm@i4....t.Y^ ...H.g.3.. (.....gVA.G..k...B..... ..8R.J8R.J....3X..... .....z.T.6	success or wait	1	406910	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\111.7z	unknown	1024	success or wait	1	4067F7	ReadFile
C:\ProgramData\Microsoft\111.7z	unknown	153	end of file	1	4067F7	ReadFile
C:\ProgramData\Microsoft\111.7z	unknown	32	success or wait	1	4067F7	ReadFile
C:\ProgramData\Microsoft\111.7z	unknown	35	success or wait	1	4067F7	ReadFile
C:\ProgramData\Microsoft\111.7z	unknown	176	success or wait	1	4067F7	ReadFile
C:\ProgramData\Microsoft\111.7z	unknown	628	success or wait	1	4067F7	ReadFile

Analysis Process: conhost.exe PID: 6656 Parent PID: 6800

General

Start time:	10:23:28
Start date:	24/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: PMRunner64.exe PID: 7120 Parent PID: 4164

General

Start time:	10:23:37
Start date:	24/01/2021
Path:	C:\Users\user\zT6Nm@i4\PMRunner64.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\zT6Nm@i4\PMRunner64.exe'
Imagebase:	0x7ff7a5160000
File size:	271704 bytes
MD5 hash:	65DBB57517611D9DE8CE522022DCD727
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Plugin32.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1A53BEECAAC	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Plugin32.dll	unknown	71672	55 bc 0f 07 75 5d 18 5a cf 05 e4 94 01 75 f3 14 c6 cb 04 44 3c 28 02 38 78 80 53 1b f4 19 02 4c a0 0c 4e af 0e 2a c9 2b 5e 92 1c c2 5e 2e 72 9f 21 d6 91 08 10 b6 00 8a bd 10 92 21 fe 7c 75 09 4e 29 e3 46 61 d9 cf d7 4c e2 3b 84 e1 7b 62 0e ca ad 46 8d 74 af 3c a3 23 f4 32 3d 03 7d 84 72 7c 82 21 6c 92 9b 8d c8 4b 6e 52 da 46 c5 d8 34 7b 49 68 a9 b2 35 0f d3 5c 80 e7 1b f4 b3 02 4c f3 89 c4 d8 a5 46 6d af f5 ee 34 46 29 4a 8a aa 25 28 71 8c ae 3c 18 0e 9d 7a 45 38 c6 98 cd 8d 38 fc db bc c6 41 de e5 23 94 62 bc af bb 26 2a cd 9e b1 d9 90 5c a3 b5 59 e5 2b 5e ca 2c 2e f9 00 cc b2 8b 17 b2 30 de cb 6f 69 e1 98 92 f3 98 60 fe 67 ac 6b 44 1a 34 38 80 47 1b f4 13 02 4c d0 51 4e 6f 72 b0 d6 2b 32 8b 26 22 1e 2e 72 8e 21 d6 51 08 00 15 22 aa 56 12 9c 1c 1e 6c 37	U...u].Z.....u.....D<(.8x.S... .L..N..*.+^...^.r.!.....!.|u.N).Fa...L.;..{b...F.t.<.#. 2=.}.r|.!l....KnR.F..4{lh..5.. \.....L.....Fm...4F)J..%(q..< ...zE8....8....A..#.b...&*.... .\..Y.+^.,.....0..oi.....`. g.kD.48.G....L.QNor..+2.&" ..r.!.Q...".V....l7	success or wait	3	1A53BEEC923	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\KK.txt	unknown	224323	success or wait	1	7FFA99DA2E51	ReadFile
C:\Users\user\AppData\Roaming\Plugin32.dll	unknown	191488	success or wait	1	1A53BEEFAC1	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	NULL	unicode	C:\Users\user\zT6Nm@i4\PMRunner64.exe	success or wait	1	1A53BEEB0C2	RegSetValueExA

Analysis Process: PMRunner64.exe PID: 6492 Parent PID: 3424

General

Start time:	10:23:48
Start date:	24/01/2021
Path:	C:\Users\user\zT6Nm@i4\PMRunner64.exe
Wow64 process (32bit):	false

Commandline:	'C:\Users\user\zT6Nm@i4\PMRunner64.exe'
Imagebase:	0x7ff7a5160000
File size:	271704 bytes
MD5 hash:	65DBB57517611D9DE8CE522022DCD727
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\KK.txt	unknown	224323	success or wait	1	7FFA99DA2E51	ReadFile

Analysis Process: PMRunner64.exe PID: 6972 Parent PID: 3424

General

Start time:	10:23:56
Start date:	24/01/2021
Path:	C:\Users\user\zT6Nm@i4\PMRunner64.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\zT6Nm@i4\PMRunner64.exe'
Imagebase:	0x7ff7a5160000
File size:	271704 bytes
MD5 hash:	65DBB57517611D9DE8CE522022DCD727
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\zT6Nm@i4\KK.txt	unknown	224323	success or wait	1	7FFA99DA2E51	ReadFile

Disassembly

Code Analysis