ID: 562373
Sample Name:
Lt8Vk8wbGCb3T2o.exe
Cookbook: default.jbs
Time: 20:20:19
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Lt8Vk8wbGCb3T2o.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary 5
Jbx Signature Overview 5
AV Detection 5
System Summary 5
Data Obfuscation 6
Boot Survival 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 14
General Information 14
Warnings 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Lt8Vk8wbGCb3T2o.exe.log 15
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mnyybsss.rtc.ps1 16
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wtzka2kz.5ya.psm1 16
C:\Users\user\AppData\Local\Temp\tmpF2A5.tmp 16
C:\Users\user\AppData\Roaming\YZBvmL.exe 17
C:\Users\user\AppData\Roaming\YZBvmL.exe:Zone.Identifier 17
C:\Users\user\Documents\20220128\PowerShell_transcript.648351.Lem0wwh8.20220128202158.txt 17
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Data Directories 20
Sections 21
Resources 21
Imports 21
Version Infos 21
Network Behavior 21
Network Port Distribution 21
TCP Packets 22
Statistics 23
Behavior 23
System Behavior 23

Analysis Process: Lt8Vk8wbGCb3T2o.exePID: 2588, Parent PID: 5440 24
General 24
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 26
Analysis Process: powershell.exePID: 3976, Parent PID: 2588 26
General 26
File Activities 27
File Created 27
File Deleted 27
File Written 27
File Read 29
Analysis Process: conhost.exePID: 4560, Parent PID: 3976 33
General 33
Analysis Process: schtasks.exePID: 3020, Parent PID: 2588 33
General 33
File Activities 33
File Read 33
Analysis Process: conhost.exePID: 3232, Parent PID: 3020 33
General 33
Analysis Process: MSBuild.exePID: 4856, Parent PID: 2588 34
General 34
File Activities 34
File Created 34
File Read 35
Disassembly 35

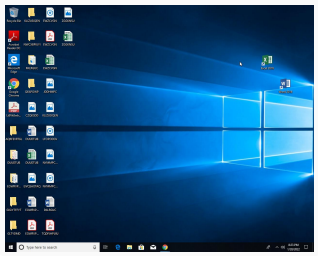
Windows Analysis Report

Lt8Vk8wbGCb3T2o.exe

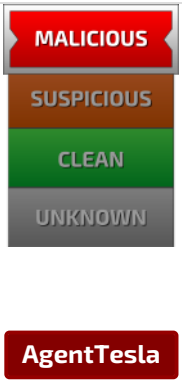
Overview

General Information

Sample Name:	Lt8Vk8wbGCb3T2o.exe
Analysis ID:	562373
MD5:	9c3893cce42e78..
SHA1:	becb237103e559..
SHA256:	b209bcfd557144..
Tags:	exe
Infos:	



Detection



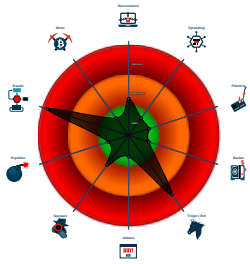
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Sigma detected: Powershell Defend…

Classification



Process Tree

- **System is w10x64**
- Lt8Vk8wbGCb3T2o.exe (PID: 2588 cmdline: "C:\Users\user\Desktop\Lt8Vk8wbGCb3T2o.exe" MD5: 9C3893CCE42E78D75B8A2A192DF70BB5)
  - powershell.exe (PID: 3976 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\YZBvmL.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 3020 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\YZBvmL" /XML "C:\Users\user\AppData\Local\Temp\tmpF2A5.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3232 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 4856 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "FTP",
  "FTP Host": "ftp://ftp.sunyimpex.com/",
  "Username": "egbon@sunyimpex.com",
  "Password": ";!zd#e{h~PQ["
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.507571498.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000002.507571498.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000010.00000000.297423015.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000010.00000000.297423015.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.301989140.0000000002DC8000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Lt8Vk8wbGCb3T2o.exe.2d5d148.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.Lt8Vk8wbGCb3T2o.exe.2d5d148.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0x8890:$v1: SbieDll.dll • 0x88aa:$v2: USER • 0x88b6:$v3: SANDBOX • 0x88c8:$v4: VIRUS • 0x8918:$v4: VIRUS • 0x88d6:$v5: MALWARE • 0x88e8:$v6: SCHMIDTI • 0x88fc:$v7: CURRENTUSER
0.2.Lt8Vk8wbGCb3T2o.exe.3e09980.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Lt8Vk8wbGCb3T2o.exe.3e09980.5.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Lt8Vk8wbGCb3T2o.exe.3e09980.5.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x2ef88:$s1: get_kbok • 0x2f8bc:$s2: get_CHoo • 0x30517:$s3: set_passwordIsSet • 0x2ed8c:$s4: get_enableLog • 0x33433:$s8: torbrowser • 0x31e0f:$s10: logins • 0x31787:$s11: credential • 0x2e176:$g1: get_Clipboard • 0x2e184:$g2: get_Keyboard • 0x2e191:$g3: get_Password • 0x2f76a:$g4: get_CtrlKeyDown • 0x2f77a:$g5: get_ShiftKeyDown • 0x2f78b:$g6: get_AltKeyDown
Click to see the 29 entries				

Sigma Overview

System Summary

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected AgentTesla

Remote Access Functionality

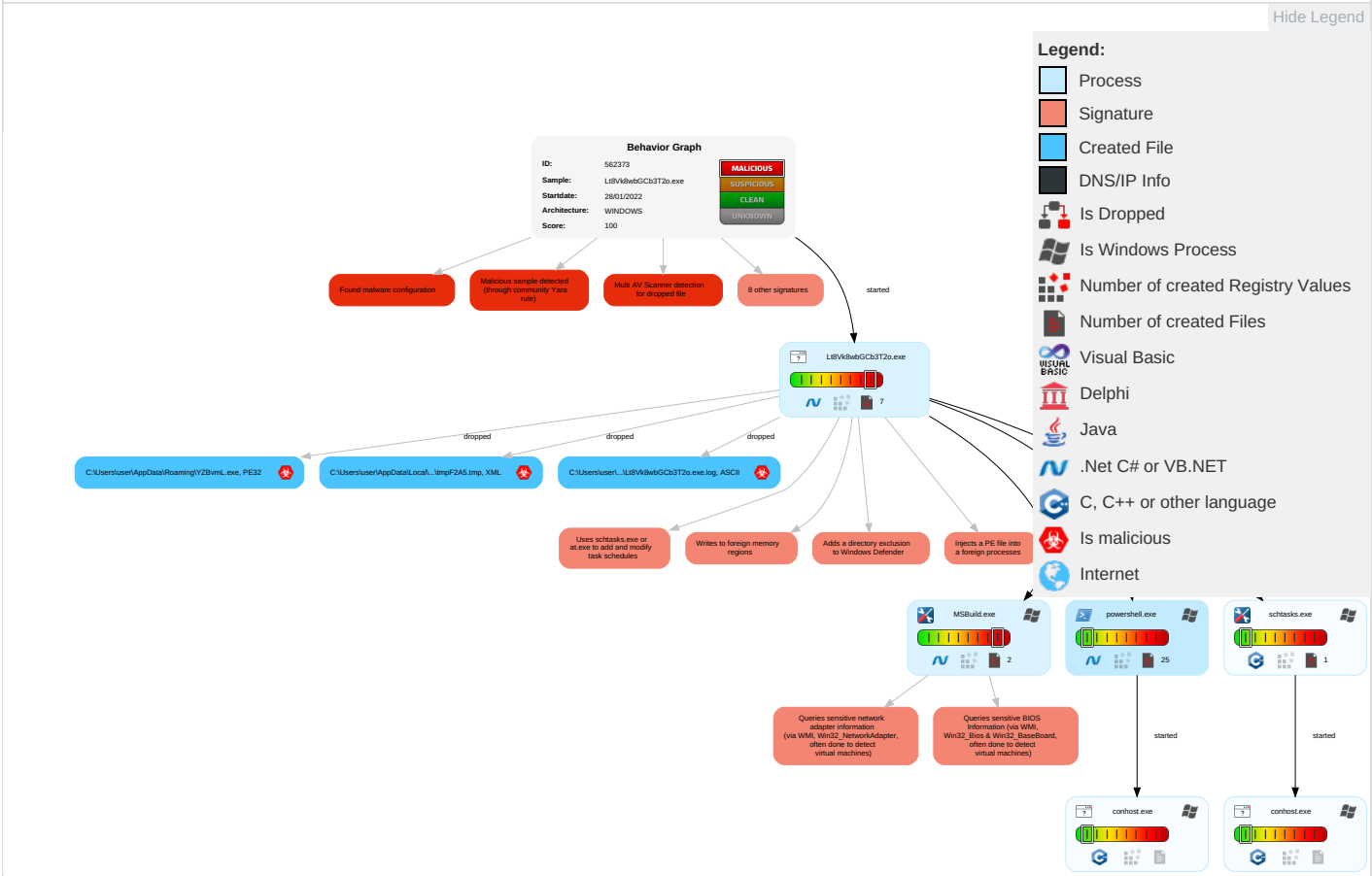
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	2 1 1 Process Injection	1 Masquerading	OS Credential Dumping	3 1 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 4 1 Virtualization/Sandbox Evasion	Security Account Manager	1 4 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	1 1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

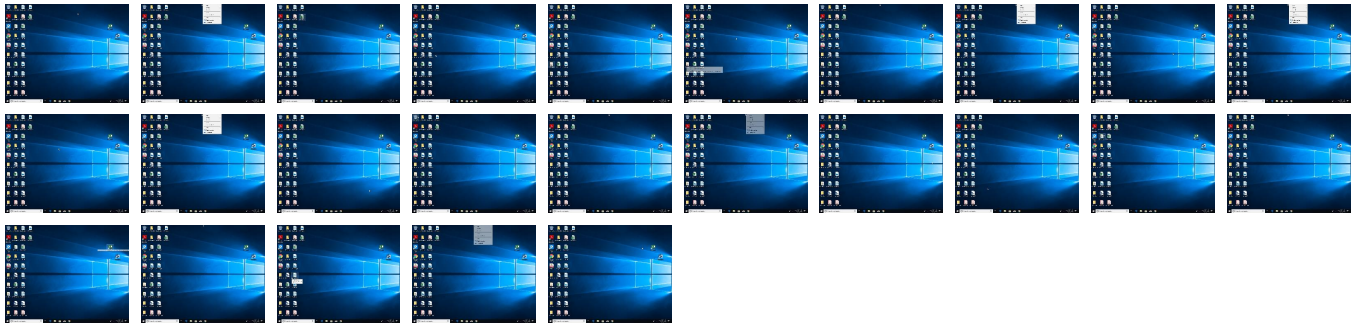
Behavior Graph



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
Lt8Vk8wbGCb3T2o.exe	28%	Virustotal		Browse
Lt8Vk8wbGCb3T2o.exe	44%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\YZBvmL.exe	44%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.0.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
16.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
16.0.MSBuild.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
16.0.MSBuild.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
16.0.MSBuild.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
16.0.MSBuild.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://blog.iandreev.com/	0%	Virustotal		Browse
http://blog.iandreev.com/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.monotype.a	0%	Avira URL Cloud	safe	
http://blog.iandreev.com/AClick	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgreta	0%	URL Reputation	safe	
http://www.sajatypeworks.comV	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://eYunMy.com	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comTF	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.tiro.comq	0%	Avira URL Cloud	safe	
http://blog.iandreev.com	0%	Avira URL Cloud	safe	
http://www.monotype.%	0%	Avira URL Cloud	safe	
http://www.carterandcone.comdd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://ftp://ftp.sunyimpex.com/egbon	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.founder.com.cn/cne-d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	MSBuild.exe, 00000010.00000002.511385017.0000000002B21000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.3 07437423.0000000006E62000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://blog.iandreev.com/	Lt8Vk8wbGCb3T2o.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.3 07437423.0000000006E62000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.3 07437423.0000000006E62000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.3 07437423.0000000006E62000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.3 07437423.0000000006E62000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.3 07437423.0000000006E62000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.monotype.a	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.2 76575828.0000000005C5B000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://blog.iandreev.com/AClick	Lt8Vk8wbGCb3T2o.exe, YZBvmL.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.3 07437423.0000000006E62000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.2 66385465.0000000005C5C000.00000004.00000 800.00020000.00000000.sdmp, Lt8Vk8wbGCb3 T2o.exe, 00000000.00000003.278852094.000 0000005C55000.00000004.00000800.00020000 .00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 000 00000.00000003.271366146.0000000005C5B00 0.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.000000 03.259244777.0000000005C56000.00000004.0 0000800.00020000.00000000.sdmp, Lt8Vk8wb GCb3T2o.exe, 00000000.00000003.282669806 .0000000005C55000.00000004.00000800.0002 0000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.260380226.0000000005C 5E000.00000004.00000800.00020000.0000000 0.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00 000003.263198052.0000000005C5B000.000000 04.00000800.00020000.00000000.sdmp, Lt8V k8wbGCb3T2o.exe, 00000000.00000003.26967 3438.0000000005C5C000.00000004.00000800. 00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.299776781.0000000005C55000. 00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003 .273099996.0000000005C56000.00000004.000 00800.00020000.00000000.sdmp, Lt8Vk8wbGC b3T2o.exe, 00000000.00000003.270110875.0 000000005C5D000.00000004.00000800.000200 00.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 0 0000000.00000003.279169050.0000000005C56 000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.28175 4098.0000000005C55000.00000004.00000800. 00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.258155802.0000000005C54000. 00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003 .259989978.0000000005C5E000.00000004.000 00800.00020000.00000000.sdmp, Lt8Vk8wbGC b3T2o.exe, 00000000.00000003.261268525.0 000000005C5E000.00000004.00000800.000200 00.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 0 0000000.00000003.266270997.0000000005C5B 000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.27185 7868.0000000005C5D000.00000004.00000800. 00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.280489374.0000000005C55000. 00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003 .260553095.0000000005C5E000.00000004.000 00800.00020000.00000000.sdmp, Lt8Vk8wbGC b3T2o.exe, 00000000.00000003.261135608.0 000000005C5E000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.248364991.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgreta	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.301719171.0000000001567000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comV	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.248364991.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	MSBuild.exe, 00000010.00000002.511385017.0000000002B21000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fonts.com	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.coma	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.248364991.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.301989140.0000000002DC8000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.301783650.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.302547654.0000000003D19000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 00000010.00000002.507571498.0000000004402000.00000040.00000400.00020000.00000000.sdmp, MSBuild.exe, 00000010.00000000.297423015.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersiv	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.280489374.0000000005C55000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNS	MSBuild.exe, 00000010.00000002.511385017.0000000002B21000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://eYunMy.com	MSBuild.exe, 00000010.00000002.511385017.0000000002B21000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comTF	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.248364991.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	MSBuild.exe, 00000010.00000002.511385017.0000000002B21000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comTC	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.266385465.0000000005C5C000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.278852094.0000000005C55000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.271366146.0000000005C5B000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.259244777.0000000005C56000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.282669806.0000000005C55000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.260380226.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.263198052.0000000005C5B000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.269673438.0000000005C5C000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.273099996.0000000005C56000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.270110875.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.279169050.0000000005C56000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.281754098.0000000005C55000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.258155802.0000000005C54000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.259989978.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.261268525.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.266270997.0000000005C5B000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.271857868.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.280489374.0000000005C55000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.260553095.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.261135608.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.260961247.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comq	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.253292090.0000000005C58000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://blog.iandreev.com	Lt8Vk8wbGCb3T2o.exe, YZBvmL.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.monotype.%	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.276575828.0000000005C5B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comdd	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.266385465.0000000005C5C000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.278852094.0000000005C55000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.271366146.0000000005C5B000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.259244777.0000000005C56000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.282669806.0000000005C55000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.260380226.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.263198052.0000000005C5B000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.269673438.0000000005C5C000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.273099996.0000000005C56000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.270110875.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.279169050.0000000005C56000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.281754098.0000000005C55000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.258155802.0000000005C54000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.259989978.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.261268525.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.266270997.0000000005C5B000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.271857868.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.280489374.0000000005C55000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.260553095.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.261135608.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.260961247.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.253103526.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.307437423.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ftp://ftp.sunyimpex.com/egbon	MSBuild.exe, 00000010.00000002.511385017.0000000002B21000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.271366146.0000000005C5B000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.271839431.0000000005C55000.00000004.00000800.00020000.00000000.sdmp, Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.276575828.0000000005C5B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cne-d	Lt8Vk8wbGCb3T2o.exe, 00000000.00000003.253103526.0000000005C58000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.3 07437423.0000000006E62000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Lt8Vk8wbGCb3T2o.exe, 00000000.00000002.3 07437423.0000000006E62000.00000004.00000 800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562373
Start date:	28.01.2022
Start time:	20:20:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Lt8Vk8wbGCb3T2o.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:	26
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:	mal100.troj.evad.winEXE@9/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 2.20.157.220, 20.82.210.154, 20.199.120.85, 20.199.120.182, 95.101.180.43, 95.101.180.35, 20.199.120.151, 40.112.88.60
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ris-prod.trafficmanager.net, asf-ris-prod-neu.northeurope.cloudapp.azure.com, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, store-images.s-microsoft.com, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:21:54	API Interceptor	2x Sleep call for process: Lt8Vk8wbGCb3T2o.exe modified
20:21:59	API Interceptor	43x Sleep call for process: powershell.exe modified
20:22:31	API Interceptor	476x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Lt8Vk8wbGCb3T2o.exe.log

Process:	C:\Users\user\Desktop\Lt8Vk8wbGCb3T2o.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22368
Entropy (8bit):	5.603517550808114
Encrypted:	false
SSDEEP:	384:ptCDy3jq0jp03QBRcS0nUjuItIiP7Y9gxSJ3xST1MaDZlbAV782mNZBDI+BzY:XjpirTUCltdrxcgCSfwIVc
MD5:	5595A4A24BFBE118A45A64C25284DEBD
SHA1:	83EC94D06AEF8E6CF7843EFDC765C74EDDFEB886
SHA-256:	B6E764A36B67E85144894D19023436404FE19E5169D51ADD12736D9BE9D60C0D
SHA-512:	6D7479E39CA52373F866B86895B13020E5A005E7541CC75902DE144F57E1B2CCF46D7AAD19790AEEFC80392F7C0A24870F79FE898CC74AD9AA4A9ECCB799EBA
Malicious:	false
Reputation:	low
Preview:	@...e.....h.....J.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mnyybsss.rtc.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wtzka2kz.5ya.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpF2A5.tmp

Process:	C:\Users\user\Desktop\Lt8Vk8wbGCb3T2o.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1597
Entropy (8bit):	5.132460105666657
Encrypted:	false

SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtMxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTMv
MD5:	154F171A9631BDF67B69E04E9568AAA4
SHA1:	BE06A46F61CCD3BEC74F40613965961A1A43C261
SHA-256:	199ADAA278AD5FEE7D49C19708F2D4D0CE3D7272902ADE12DEB57D21507C3B7B
SHA-512:	56E27626E3042F62CB273D721935DB48821FD7A91CAF83E13625958C396474C285A9F6798BFF7DED8910BC47766A2C29E205675E7DC6E4565C21CCE5C8A79B3
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Roaming\YZBvmL.exe

Process:	C:\Users\user\Desktop\Lt8Vk8wbGCb3T2o.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	897024
Entropy (8bit):	6.602318944042674
Encrypted:	false
SSDEEP:	12288:9H2lo92LsgV++yQNep3P/JHrHdmtvdwVZjS+HTD2:9QoUL9V++ySep3XJHr9mddKj3HTa
MD5:	9C3893CCE42E78D75B8A2A192DF70BB5
SHA1:	BECB237103E5595BD47320BCB01E546EBAAA507F
SHA-256:	B209BCFD557144D1195462AD7A6532247F50E8BC30E72A370EF63C2DE0F73DDE
SHA-512:	E0984179D038E05C5461C3C56925AF4E828CA15CC941C7C5656C98D0196ED8D2D36DBE90A05D378C9BC3FD1748A6C8691FCD4D7DBACD6458E2436A9B3A435E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 44%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....8.a.....0.....j.... .....@.. .....@.....O..... ....H.....text...p.... ....`.rsrc.....@..@.reloc.....@..B.....L.....H.....H..X.....X1.....^..}.....(.....(.....*.0..+.....,..{.....+....,...{....o.....(.....*...s....}.....(..... ... .s....(.....r...po.....*&.(.....*....0..9.....~.....,".r...p.....(...o!...s".....~.....+..*....0.....~.....+..*".....*.0.....(....r?..p~....o#....+..*...0.....(....rY..p~....o#....+..*...0.....(....rq..p~....o#....+..*...0.....(....r...p~....o#....+.

C:\Users\user\AppData\Roaming\YZBvmL.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Lt8Vk8wbGCb3T2o.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220128\PowerShell_transcript.648351.Lem0wwh8.20220128202158.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5783
Entropy (8bit):	5.408268485084794
Encrypted:	false
SSDEEP:	96:BZk/FN4UqDo1ZqZ5m/FN4UqDo1Z1FhrZjZJo/FN4UqDo1ZPfkJJ5hZr4:FsAAn4
MD5:	83C8FF5BD7282B12D4A3F70C39C0364F
SHA1:	592F1F6CC6B2D59FF652BA31EA10C3088C53EB0B
SHA-256:	990C2A88F26A5CBB075E76F271CAF27F144CF1D494249D5E847FCE6D8A666DB3

SHA-512:	938CCDF91463DF8A18D9BD77B64150131F321CEB13D72D906C200782FA92FFC83C88DC8EE2E686F96B7296C121C34E1122E8513E9D0E5A5DE78C61C2BF30CB3
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220128202159..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 648351 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\YZBvmL.exe..Process ID: 3976..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220128202159..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\YZBvmL.exe..**********..Windows PowerShell transcript start..Start time: 20220128202627..Username: computer\user..RunAs User: computer\user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.602318944042674
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Lt8Vk8wbGCb3T2o.exe
File size:	897024
MD5:	9c3893cce42e78d75b8a2a192df70bb5
SHA1:	becb237103e5595bd47320bcb01e546ebaaa507f
SHA256:	b209bcfd557144d1195462ad7a6532247f50e8bc30e72a370ef63c2de0f73dde
SHA512:	e0984179d038e05c5461c3c56925af4e828ca15cc941c7c5656c98d0196ed8d2d36dbe90a05d378c9bc3fd1748a6c8691fcd4d7dbacd6458e2436a9b3a435f7e
SSDEEP:	12288:9H2lo92LsgV++yQNep3P/JHrHdmtvdwVZjS+HTD2:9QoUL9V++ySep3XJHr9mddKj3HTa
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....8.a.....0.....j.... .....@.. .....@.....

File Icon

Icon Hash:	eaee8e96b2a8e0b2

Static PE Info

General

Entrypoint:	0x4cf06a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F3380C [Fri Jan 28 00:25:48 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcf018	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd0000	0xd8b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xde000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xceee0	0x1c	.text
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcd070	0xcd200	False	0.532909144576	data	6.64986881872	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd0000	0xd8b4	0xda00	False	0.0906500860092	data	3.81409951735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xde000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xd0130	0xd228	data		
RT_GROUP_ICON	0xdd358	0x14	data		
RT_VERSION	0xdd36c	0x35c	data		
RT_MANIFEST	0xdd6c8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

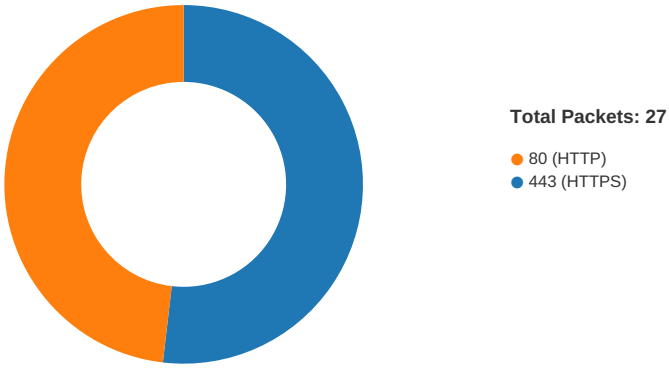
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	RemotingParameterCachedDa.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	OthelloCS
ProductVersion	1.0.0.0
FileDescription	OthelloCS
OriginalFilename	RemotingParameterCachedDa.exe

Network Behavior

Network Port Distribution



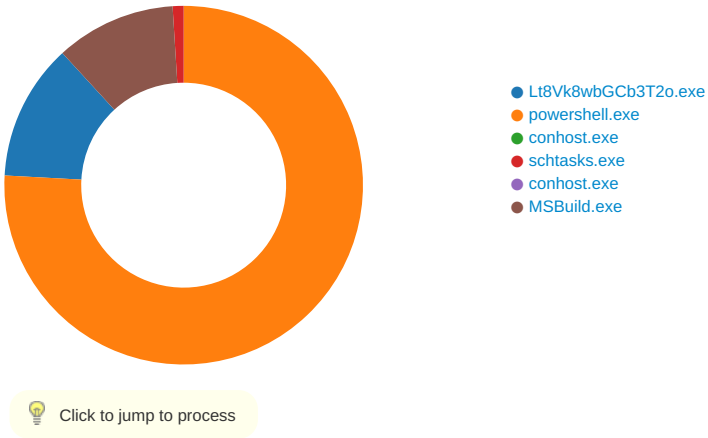
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 20:21:10.976244926 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.976367950 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.976434946 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.976475954 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.976514101 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.976540089 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.976557970 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.976579905 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.976598024 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.976617098 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.992445946 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992461920 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992470026 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992480993 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992489100 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992500067 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992511988 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992548943 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992558956 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992585897 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992598057 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992619038 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992662907 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992706060 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992717028 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992742062 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992826939 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992837906 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992872953 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992882967 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.992954969 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993000984 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993012905 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993024111 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993033886 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993046045 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993056059 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993103027 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993185997 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993196964 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993204117 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993216038 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993223906 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993271112 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993411064 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993422985 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993428946 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993442059 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993448973 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993460894 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993472099 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993513107 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993522882 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993544102 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993555069 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993555069 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:10.993624926 CET	443	49701	204.79.197.200	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 20:21:10.993637085 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993673086 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993704081 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993715048 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993726015 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993736982 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:10.993793011 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:21:11.028398037 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:21:11.028604031 CET	49701	443	192.168.2.5	204.79.197.200
Jan 28, 2022 20:22:01.028280973 CET	49676	80	192.168.2.5	104.83.132.63
Jan 28, 2022 20:22:01.051585913 CET	80	49676	104.83.132.63	192.168.2.5
Jan 28, 2022 20:22:01.051788092 CET	49676	80	192.168.2.5	104.83.132.63
Jan 28, 2022 20:22:01.637808084 CET	49680	80	192.168.2.5	92.123.101.210
Jan 28, 2022 20:22:01.664530039 CET	80	49680	92.123.101.210	192.168.2.5
Jan 28, 2022 20:22:01.664655924 CET	49680	80	192.168.2.5	92.123.101.210
Jan 28, 2022 20:22:02.892491102 CET	80	49679	93.184.220.29	192.168.2.5
Jan 28, 2022 20:22:02.892683029 CET	49679	80	192.168.2.5	93.184.220.29
Jan 28, 2022 20:22:04.141527891 CET	49690	443	192.168.2.5	104.75.89.220
Jan 28, 2022 20:22:04.141983986 CET	49691	80	192.168.2.5	93.184.220.29
Jan 28, 2022 20:22:06.804361105 CET	80	49702	93.184.220.29	192.168.2.5
Jan 28, 2022 20:22:06.804550886 CET	49702	80	192.168.2.5	93.184.220.29
Jan 28, 2022 20:22:51.188935041 CET	49678	80	192.168.2.5	92.123.101.170
Jan 28, 2022 20:22:51.189018011 CET	49679	80	192.168.2.5	93.184.220.29
Jan 28, 2022 20:22:51.210815907 CET	80	49679	93.184.220.29	192.168.2.5
Jan 28, 2022 20:22:51.211488008 CET	80	49678	92.123.101.170	192.168.2.5
Jan 28, 2022 20:22:51.211574078 CET	49678	80	192.168.2.5	92.123.101.170
Jan 28, 2022 20:22:51.211628914 CET	49679	80	192.168.2.5	93.184.220.29
Jan 28, 2022 20:23:08.240391016 CET	80	49702	93.184.220.29	192.168.2.5
Jan 28, 2022 20:23:08.240487099 CET	49702	80	192.168.2.5	93.184.220.29
Jan 28, 2022 20:23:15.926881075 CET	443	49701	204.79.197.200	192.168.2.5
Jan 28, 2022 20:23:21.947465897 CET	80	49702	93.184.220.29	192.168.2.5
Jan 28, 2022 20:23:21.947715998 CET	49702	80	192.168.2.5	93.184.220.29

Statistics

Behavior



System Behavior

Analysis Process: Lt8Vk8wbGCb3T2o.exe PID: **2588**, Parent PID: **5440**

General

Target ID:	0
Start time:	20:21:33
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\Lt8Vk8wbGCb3T2o.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Lt8Vk8wbGCb3T2o.exe"
Imagebase:	0x970000
File size:	897024 bytes
MD5 hash:	9C3893CCE42E78D75B8A2A192DF70BB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.301989140.0000000002DC8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.301783650.0000000002D11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.302547654.0000000003D19000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.302547654.0000000003D19000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EC7CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EC7CF06	unknown
C:\Users\user\AppData\Roaming\YZBvmL.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	6C7EDD66	CopyFileW
C:\Users\user\AppData\Roaming\YZBvmL.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C7EDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF2A5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C7E7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Lt8Vk8wbGCb3T2o.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EF8C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF2A5.tmp	success or wait	1	6C7E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\YZBvmL.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0c 38 fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0c 00 00 fd 00 00 00 00 00 00 6a fd 0c 00 00 20 00 00 00 00 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL8a0j @ @	success or wait	4	6C7EDD66	CopyFileW
C:\Users\user\AppData\Roaming\YZBvmL.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C7EDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF2A5.tmp	0	1597	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationInfo>	success or wait	1	6C7E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Lt8Vk8wbGCb3T2o.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6EF8C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C7E1B4F	ReadFile

Analysis Process: powershell.exe PID: **3976**, Parent PID: **2588**

General

Target ID:	11
Start time:	20:21:57
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\YZBvmL.exe
Imagebase:	0x13b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EC7CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EC7CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mnyybsss.rtc.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C7E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wtzka2kz.5ya.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C7E1E60	CreateFileW
C:\Users\user\Documents\20220128	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C7EBEFF	CreateDirectoryW
C:\Users\user\Documents\20220128\PowerShell_transcript.648351.Lem0wwh8.20220128202158.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C7E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mnyybsss.rtc.ps1	success or wait	1	6C7E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wtzka2kz.5ya.psm1	success or wait	1	6C7E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mnyybsss.rtc.ps1	0	1	31	1	success or wait	1	6C7E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wtzka2kz.5ya.psm1	0	1	31	1	success or wait	1	6C7E1B4F	WriteFile
C:\Users\user\Documents\20220128\PowerShell_transcript.648351.Lem0wwh8.20220128202158.txt	0	3	ff		success or wait	1	6C7E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220128\PowerShell_transcript.648351.Lem0wwh8.20220128202158.txt	3	676	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 38 32 30 32 31 35 39 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 36 34 38 33 35 31 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********Windows PowerShell transcript startStart time: 20220128202159Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 648351 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	44	6C7E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 14 00 00 1b 00 00 00 68 0d fd 04 fd 08 fd 08 fd 08 00 00 fd 00 fd 00 0f 00 4a 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ehJ@	success or wait	1	6EF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6EF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6EF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6EF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6EF476FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0c fd 00 54 01 40 00 fd 3e 40 01 05 0e fd 00 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 06 0e fd 00 04 0e fd 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 07 0e fd 00 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 08 0c fd 00 20 4d 40 01 08 0e fd 00 21 4d 40 01 12 6f 40 01 2a 29 40 01 1f 29 40 01 4d 64 40 01 5d 64 40 01 4e 64 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 fd 29 40 01 fd 29 40 01 38 4d 40 01 3f 4d 40 01 23 29 40 01 5c 64 40 01 5a 64 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@o@*)@)@Md@]d@Nd@;M@D@D@@M@<M@$M@)@)@8M@?M@#)@\d@Zd@	success or wait	11	6EF476FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EC5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EC55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6EC61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6EC6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EBB03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	130	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C7E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	6	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C7E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C7E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C7E1B4F	ReadFile

Analysis Process: conhost.exe PID: **4560**, Parent PID: **3976**

General

Target ID:	12
Start time:	20:21:57
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: schtasks.exe PID: **3020**, Parent PID: **2588**

General

Target ID:	13
Start time:	20:21:57
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\YZBvmL" /XML "C:\Users\user\AppData\Local\Temp\tmpF2A5.tmp
Imagebase:	0x120000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF2A5.tmp	unknown	2	success or wait	1	12AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF2A5.tmp	unknown	1598	success or wait	1	12ABD9	ReadFile

Analysis Process: conhost.exe PID: **3232**, Parent PID: **3020**

General

Target ID:	14
Start time:	20:21:58
Start date:	28/01/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: MSBuild.exe PID: **4856**, Parent PID: **2588**

General

Target ID:	16
Start time:	20:22:00
Start date:	28/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0x5d0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.507571498.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.507571498.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.297423015.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.297423015.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.297696265.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.297696265.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.298339143.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.298339143.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.298034248.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.298034248.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.511385017.0000000002B21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.511385017.0000000002B21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000010.00000002.511385017.0000000002B21000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EC7CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EC7CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6EC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6EC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	success or wait	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	end of file	1	6C7E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6EC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6EC55705	unknown

Disassembly

No disassembly