ID: 625006
Sample Name:
vsQkhWCXxv.exe
Cookbook: default.jbs
Time: 10:29:44
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report vsQkhWCXxv.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
AV Detection 6
E-Banking Fraud 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 7
Networking 7
E-Banking Fraud 7
System Summary 7
Data Obfuscation 7
Boot Survival 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 13
Public IPs 13
Private 13
General Information 14
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
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\vsQkhWCXxv.exe.log 15
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jpzyxe0b.155.psm1 16
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qftbfgou.aym.ps1 16
C:\Users\user\AppData\Local\Temp\tmp5508.tmp 16
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 16
C:\Users\user\AppData\Roaming\vyJCJmhRnRK.exe 17
C:\Users\user\AppData\Roaming\vyJCJmhRnRK.exe:Zone.Identifier 17
C:\Users\user\Documents\20220512\PowerShell_transcript.878411.S4i67LBI.20220512103126.txt 17
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18

Copyright Joe Security LLC 2022

Data Directories 20
Sections 21
Resources 21
Imports 21
Version Infos 21
Network Behavior 21
Network Port Distribution 21
TCP Packets 21
UDP Packets 22
DNS Queries 23
DNS Answers 23
Statistics 23
Behavior 23
System Behavior 24
Analysis Process: vsQkhWCXxv.exePID: 3472, Parent PID: 6092 24
General 24
File Activities 24
File Created 24
File Deleted 25
File Written 25
File Read 26
Analysis Process: powershell.exePID: 1300, Parent PID: 3472 27
General 27
File Activities 27
File Created 27
File Deleted 28
File Written 28
File Read 29
Analysis Process: conhost.exePID: 1308, Parent PID: 1300 32
General 32
Analysis Process: schtasks.exePID: 6280, Parent PID: 3472 32
General 32
File Activities 33
File Read 33
Analysis Process: conhost.exePID: 6288, Parent PID: 6280 33
General 33
Analysis Process: vsQkhWCXxv.exePID: 6340, Parent PID: 3472 33
General 33
File Activities 34
File Created 34
File Deleted 35
File Written 35
File Read 35
Disassembly 35

Copyright Joe Security LLC 2022

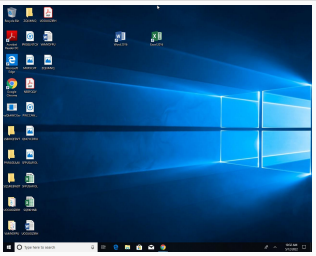
Windows Analysis Report

vsQkhWCXxv.exe

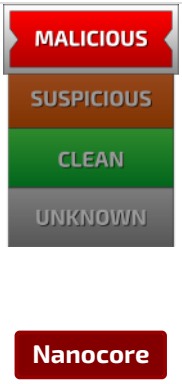
Overview

General Information

Sample Name:	vsQkhWCXxv.exe
Analysis ID:	625006
MD5:	ff76da561669973.
SHA1:	9b0c1bf91bfd6e8..
SHA256:	ec04ec5840bcab..
Tags:	exe NanoCore RAT
Infos:	



Detection



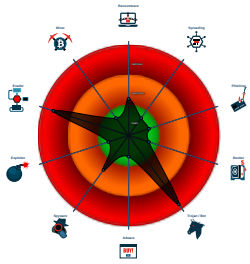
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT

Classification



Process Tree

- **System is w10x64**
- vsQkhWCXxv.exe (PID: 3472 cmdline: "C:\Users\user\Desktop\vsQkhWCXxv.exe" MD5: FF76DA5616699735C9F7C70BA9E66909)
  - powershell.exe (PID: 1300 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\vyJCJmhRnRK.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6280 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\vyJCJmhRnRK" /XML "C:\Users\user\AppData\Local\Temp\tmp5508.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vsQkhWCXxv.exe (PID: 6340 cmdline: C:\Users\user\Desktop\vsQkhWCXxv.exe MD5: FF76DA5616699735C9F7C70BA9E66909)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "ac8dc510-d280-4bfd-8a77-cea13b6d",
  "Group": "2ND MARCH",
  "Domain1": "ella666.duckdns.org",
  "Domain2": "mikeljack321.ddns.net",
  "Port": 31788,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "ella666.duckdns.org"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.346722851.0000000005340000.00000004.08000000.00040000.00000000.sdmp	INDICATOR_EXE_Packed_DotNetReactor	Detects executables packed with unregistered version of .NET Reactor	ditekSHen	• 0xd071:$s2: is protected by an unregistered version of .NET Reactor!");</script>
00000011.00000002.517843994.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000011.00000002.517843994.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000011.00000002.517843994.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000011.00000000.334851227.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 35 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.vsQkhWCXxv.exe.5460000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
17.2.vsQkhWCXxv.exe.5460000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
17.2.vsQkhWCXxv.exe.5460000.6.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
17.0.vsQkhWCXxv.exe.400000.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
17.0.vsQkhWCXxv.exe.400000.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
Click to see the 74 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Yara detected Nanocore RAT

Networking

- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud

- Yara detected Nanocore RAT

System Summary

- Malicious sample detected (through community Yara rule)

Data Obfuscation

- .NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

- Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

- Yara detected Nanocore RAT

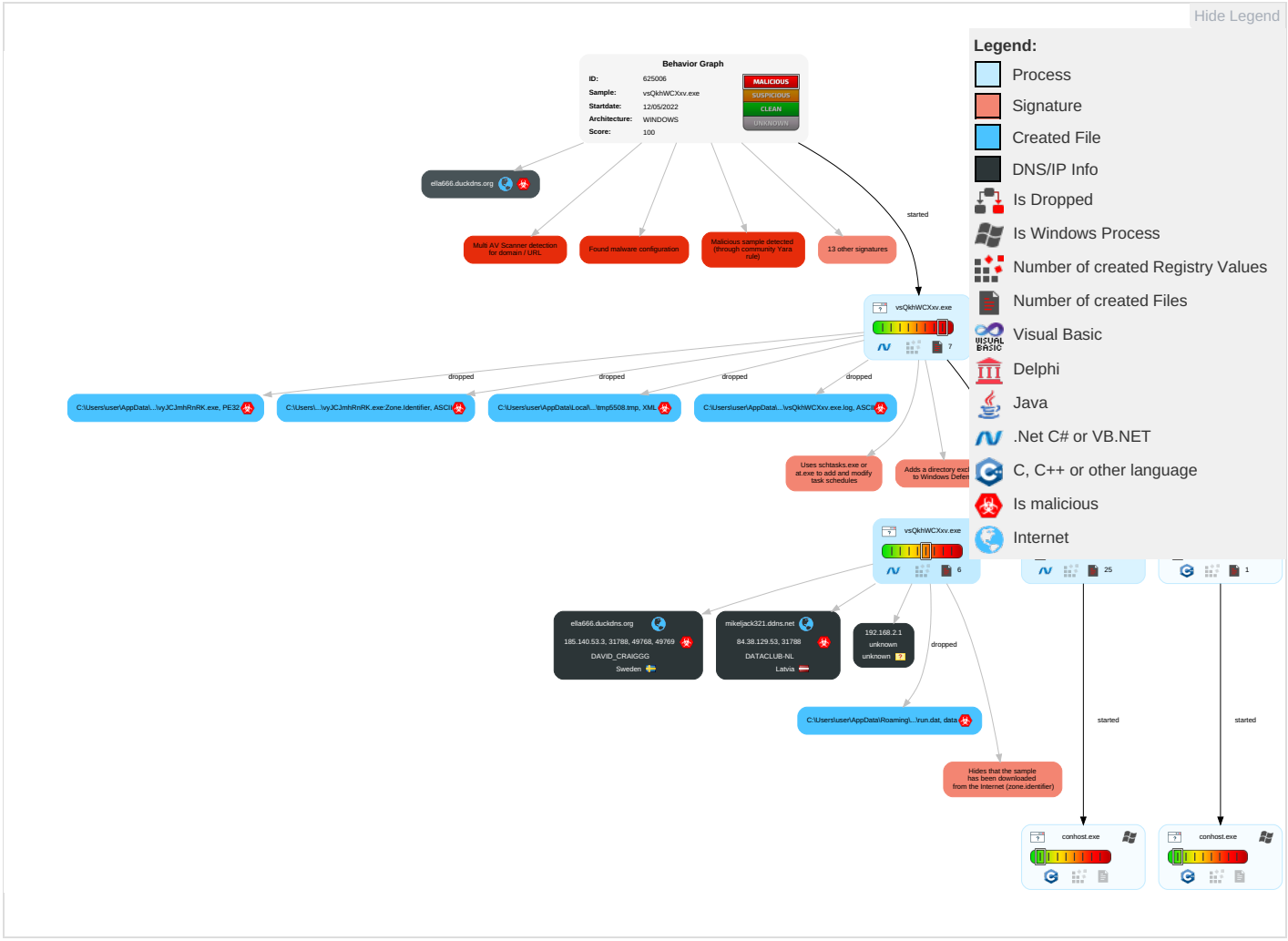
Remote Access Functionality

- Detected Nanocore Rat
- Yara detected Nanocore RAT

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	1 Scheduled Task/Job	1 Scheduled Task/Job	1 2 Process Injection	1 Masquerading	2 1 Input Capture	1 Query Registry	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
vsQkhWCXxv.exe	51%	Virustotal		Browse
vsQkhWCXxv.exe	31%	Metadefender		Browse
vsQkhWCXxv.exe	61%	ReversingLabs	ByteCode-MSIL.Trojan.AgenteslaPacker	
vsQkhWCXxv.exe	100%	Avira	TR/AD.BDSNanoCoreClient.wibth	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\vyJCJmhRnRK.exe	100%	Avira	TR/AD.BDSNanoCoreClient.wibth	
C:\Users\user\AppData\Roaming\vyJCJmhRnRK.exe	31%	Metadefender		Browse
C:\Users\user\AppData\Roaming\vyJCJmhRnRK.exe	61%	ReversingLabs	ByteCode-MSIL.Trojan.AgenteslaPacker	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
17.0.vsQkhWCXxv.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.2.vsQkhWCXxv.exe.790000.1.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
17.0.vsQkhWCXxv.exe.790000.0.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
17.0.vsQkhWCXxv.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.vsQkhWCXxv.exe.790000.9.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
17.0.vsQkhWCXxv.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.vsQkhWCXxv.exe.790000.1.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
17.0.vsQkhWCXxv.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.2.vsQkhWCXxv.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.vsQkhWCXxv.exe.790000.5.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
17.0.vsQkhWCXxv.exe.790000.3.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
0.0.vsQkhWCXxv.exe.6f0000.0.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
0.2.vsQkhWCXxv.exe.6f0000.0.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
17.0.vsQkhWCXxv.exe.790000.7.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
17.0.vsQkhWCXxv.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.vsQkhWCXxv.exe.790000.11.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
17.0.vsQkhWCXxv.exe.790000.2.unpack	100%	Avira	HEUR/AGEN.1247014		Download File
17.2.vsQkhWCXxv.exe.5e00000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
17.0.vsQkhWCXxv.exe.790000.13.unpack	100%	Avira	HEUR/AGEN.1247014		Download File

Domains

Source	Detection	Scanner	Label	Link
mikeljack321.ddns.net	7%	Virustotal		Browse
ella666.duckdns.org	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
ella666.duckdns.org	100%	Avira URL Cloud	malware	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
mikeljack321.ddns.net	0%	Avira URL Cloud	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	

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mikeljack321.ddns.net	84.38.129.53	true	true	• 7%, Virustotal, Browse	unknown
ella666.duckdns.org	185.140.53.3	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

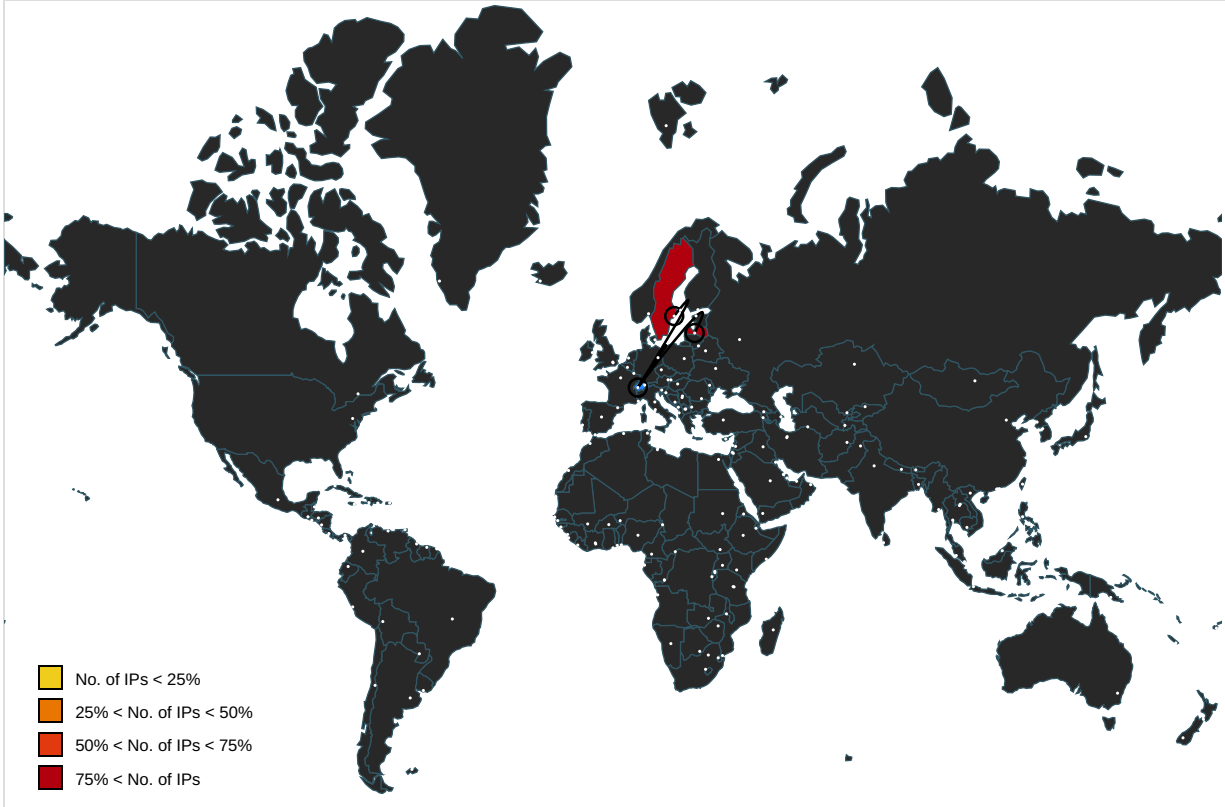
Name	Malicious	Antivirus Detection	Reputation
ella666.duckdns.org	true	• Avira URL Cloud: malware	unknown
mikeljack321.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vsQkhWCXxv.exe, 00000000.00000002.340724952.0000000002BE8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	vsQkhWCXxv.exe, 00000000.00000002.347282671.0000000006C62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.38.129.53	mikeljack321.ddns.net	Latvia		203557	DATACLUB-NL	true
185.140.53.3	ella666.duckdns.org	Sweden		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

Copyright Joe Security LLC 2022

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	625006
Start date and time: 12/05/202210:29:44	2022-05-12 10:29:44 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vsQkhWCXxv.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:	30
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@9/9@9/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 2.4% (good quality ratio 2.2%) • Quality average: 65.2% • Quality standard deviation: 26.4%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.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
10:31:02	API Interceptor	675x Sleep call for process: vsQkhWCXxv.exe modified
10:31:30	API Interceptor	42x Sleep call for process: powershell.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\vsQkhWCXxv.exe.log

Process:	C:\Users\user\Desktop\vsQkhWCXxv.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):	22252
Entropy (8bit):	5.599636441543448
Encrypted:	false
SSDEEP:	384:ptCDrq0Rvr96K0JvKSPMnAjultIQ47nvPg3hInEML+efmAV7eWMAeVZQvnI++KE:avR6Kz6MAClL866PKCpat+4
MD5:	8A1BB05627515BF89BD00839D5041BA6
SHA1:	0FA91C60610811EFD9023FB580AF5682DB5D63BB
SHA-256:	46091A6623122EDA14D3EF45C186E3A6AA382F97B004457CF9341DEB91A98FFC
SHA-512:	6340102BB75E72A4FF3A81290914900B5B6D976FE2A93706D9BBBDC0373B5089D8E9DE2FD66191C8C98BE6E0AE21526982113E2D5C46DF1A9F189A515B05DA7D
Malicious:	false
Reputation:	low

Preview:	@...e.....s.....K.....c...,.....@.....H.....<@.^.L."My...:X..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.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.....Sy stem.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_jpzyxe0b.155.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qftbfgou.aym.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp5508.tmp

Process:	C:\Users\user\Desktop\vsQkhWCXxv.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.145443390101725
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtazNLxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTgv
MD5:	12B9B2BAAC3F00A5E887C9C33ABC0C1E
SHA1:	0F510DF35E91D3D9461DDB4E86D5B07471E07A4F
SHA-256:	670F799B23BDAAA40E6DEC6DED42E675CEFF4826A1F27CBFE4D2CCD9731D4451
SHA-512:	D35AD7B94A732ACB816F0461313D83EE02D656F368234E4F88ADD1CF640CA62024D6560969D3E38035EA2E8F324053B79A7F00600431C13C1697CB6CD288A896
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>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\vsQkhWCXxv.exe
File Type:	data

Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:yYN:yYN
MD5:	DFC7C11287DD654FD4E905F8490E6813
SHA1:	3B869E06DC55A327E4773BCB3BAF25B9AA142B7B
SHA-256:	277234ED4E56E5D347A0E3549D8DE8BFE0F98DCC58D9F213891EE60ED3BD3668
SHA-512:	B6134B050D683DA8B773ACEA54391EC6E36D5BCF965F85BD918D029529F3A164EFD45D83EDFA1D08F6E1F23E0346E304B1485B9AB97C648A48312592E275371
Malicious:	**true**
Preview:	..z..3.H

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

Process:	C:\Users\user\Desktop\vsQkhWCXxv.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1093632
Entropy (8bit):	7.665758507270367
Encrypted:	false
SSDEEP:	24576:SDR/oGw6CEzu7ycumCcFTJScFcWVMoy+x:SDR9w6CfycuMJ0cA
MD5:	FF76DA5616699735C9F7C70BA9E66909
SHA1:	9B0C1BF91BFD6E8E0A1D68F5D0DA2F8ADDAD231D
SHA-256:	EC04EC5840BCAB1B86EC8E2A9D5D8FCBBC687A6235DF0BC416E3CB6B149FAF97
SHA-512:	A78D80C4129769F7A0F70C60FEC6A791D88C2F3C7C89D1C970171B588C6EABE323A44B5D1FE53C4482B7C32F56710F71F45B6718104C68CED05CF54387CC9C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 61%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....6.... .....@.. ....@.....O..... ....H.....text...<.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....0w.....2.. .....^..}.....(.....(.....*.0..+.....,..{.....+....,...{....o.....(.....*...(.....".."...@"..PAs....(.....(..... .r...p(.....(.....*..0.....(.....(....s.....o.....*&.(!.....*...0..9.....~.....,".r...p.....("...o#...s$.....~.....+..*....0.....~.....+..*".....*.0..!.....(....rW..p~....o%.....t.....+..*....0.. .....~.....+..*".(&....*Vs....('...t.....*...0.....

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

Process:	C:\Users\user\Desktop\vsQkhWCXxv.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220512\PowerShell_transcript.878411.S4i67LBI.20220512103126.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):	5793
Entropy (8bit):	5.406527687074698
Encrypted:	false
SSDEEP:	96:BZAjLNeDqDo1ZHwZTjLNeDqDo1ZrUK8jZ7jLNeDqDo1ZSZMMkZT:RdzP/
MD5:	703E7E0F3E2622C3EDC9F502016ED9E1
SHA1:	04D252F060DC57DECD2E4E900A3E75B2824B5C88
SHA-256:	C5D97B30E7D27E802121350F8417EA5790BAFECBD8517B661B81A51039B8CA83

SHA-512:	0D8B3E0E6F95A64D2FE54F6459D15A7BEE871F55E4F5034016990DD4985DD0D31FA08DA4B163C2C4AD08F2C4E7628A63FF03AC94B8FD4E4568B02D47E4F08E5A
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220512103130..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878411 (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\vyJCJmhRnRK.exe..Process ID: 1300..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: 20220512103130..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\vyJCJmhRnRK.exe..**********..Windows PowerShell transcript start..Start time: 20220512103601..Username: computer\user..RunAs User: computer\jo

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.665758507270367
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	vsQkhWCXxv.exe
File size:	1093632
MD5:	ff76da5616699735c9f7c70ba9e66909
SHA1:	9b0c1bf91bfd6e8e0a1d68f5d0da2f8addad231d
SHA256:	ec04ec5840bcab1b86ec8e2a9d5d8fcbbc687a6235df0bc416e3cb6b149faf97
SHA512:	a78d80c4129769f7a0f70c60fec6a791d88c2f3c7c89d1c970171b588c6eabe323a44b5d1fe53c4482b7c32f56710f71f45b6718104c68ced05cf54387cc9c08
SSDEEP:	24576:SDR/oGw6CEzu7ycumCcFTJScFcWVMoy+x:SDR9w6CfycuMJ0cA
TLSH:	51358DE0AB08567FDEB1237AC1B855313EB61D4AA495FF28578E32C84973F8E09D241D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....6.... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x50c336
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:	0x622E9991 [Mon Mar 14 01:25:37 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]
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

Copyright Joe Security LLC 2022

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10c2e4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10e000	0x614	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x110000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Copyright Joe Security LLC 2022

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x10a33c	0x10a400	False	0.783547901995	data	7.670144875	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10e000	0x614	0x800	False	0.33349609375	data	3.48672712067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x110000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x10e090	0x384	data		
RT_MANIFEST	0x10e424	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

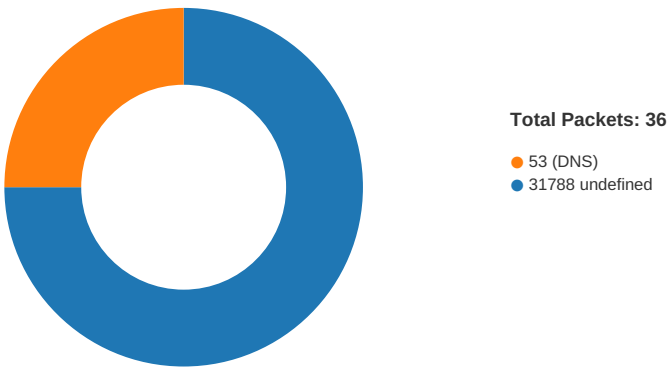
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	RSAPKCS1SHA256SignatureDescript.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	Auto Jack
ProductVersion	1.0.0.0
FileDescription	Auto Jack
OriginalFilename	RSAPKCS1SHA256SignatureDescript.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 10:31:41.443510056 CEST	49768	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:31:41.647921085 CEST	31788	49768	185.140.53.3	192.168.2.4
May 12, 2022 10:31:42.158616066 CEST	49768	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:31:42.353931904 CEST	31788	49768	185.140.53.3	192.168.2.4
May 12, 2022 10:31:42.861835003 CEST	49768	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:31:43.080113888 CEST	31788	49768	185.140.53.3	192.168.2.4
May 12, 2022 10:31:47.861615896 CEST	49769	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:31:48.078548908 CEST	31788	49769	185.140.53.3	192.168.2.4
May 12, 2022 10:31:48.706176043 CEST	49769	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:31:48.919456005 CEST	31788	49769	185.140.53.3	192.168.2.4
May 12, 2022 10:31:49.612406969 CEST	49769	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:31:49.817852020 CEST	31788	49769	185.140.53.3	192.168.2.4
May 12, 2022 10:31:54.555962086 CEST	49770	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:31:54.756643057 CEST	31788	49770	185.140.53.3	192.168.2.4
May 12, 2022 10:31:55.362884998 CEST	49770	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:31:55.566855907 CEST	31788	49770	185.140.53.3	192.168.2.4
May 12, 2022 10:31:56.175672054 CEST	49770	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:31:56.397176981 CEST	31788	49770	185.140.53.3	192.168.2.4
May 12, 2022 10:32:00.578315020 CEST	49773	31788	192.168.2.4	84.38.129.53
May 12, 2022 10:32:03.676088095 CEST	49773	31788	192.168.2.4	84.38.129.53
May 12, 2022 10:32:09.676594973 CEST	49773	31788	192.168.2.4	84.38.129.53
May 12, 2022 10:32:19.841871977 CEST	49779	31788	192.168.2.4	84.38.129.53
May 12, 2022 10:32:22.865271091 CEST	49779	31788	192.168.2.4	84.38.129.53
May 12, 2022 10:32:28.865794897 CEST	49779	31788	192.168.2.4	84.38.129.53
May 12, 2022 10:32:39.639579058 CEST	49781	31788	192.168.2.4	84.38.129.53
May 12, 2022 10:32:42.773185015 CEST	49781	31788	192.168.2.4	84.38.129.53
May 12, 2022 10:32:48.773736954 CEST	49781	31788	192.168.2.4	84.38.129.53
May 12, 2022 10:32:57.213046074 CEST	49795	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:32:57.434855938 CEST	31788	49795	185.140.53.3	192.168.2.4
May 12, 2022 10:32:57.961960077 CEST	49795	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:32:58.164561033 CEST	31788	49795	185.140.53.3	192.168.2.4
May 12, 2022 10:32:58.665092945 CEST	49795	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:32:58.866548061 CEST	31788	49795	185.140.53.3	192.168.2.4
May 12, 2022 10:33:02.986813068 CEST	49817	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:33:03.188015938 CEST	31788	49817	185.140.53.3	192.168.2.4
May 12, 2022 10:33:03.696804047 CEST	49817	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:33:03.914177895 CEST	31788	49817	185.140.53.3	192.168.2.4
May 12, 2022 10:33:04.415616989 CEST	49817	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:33:04.644908905 CEST	31788	49817	185.140.53.3	192.168.2.4
May 12, 2022 10:33:08.671421051 CEST	49818	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:33:08.871973038 CEST	31788	49818	185.140.53.3	192.168.2.4
May 12, 2022 10:33:09.541074038 CEST	49818	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:33:09.746056080 CEST	31788	49818	185.140.53.3	192.168.2.4
May 12, 2022 10:33:10.338000059 CEST	49818	31788	192.168.2.4	185.140.53.3
May 12, 2022 10:33:10.547224998 CEST	31788	49818	185.140.53.3	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 10:31:41.317061901 CEST	60758	53	192.168.2.4	8.8.8.8
May 12, 2022 10:31:41.425947905 CEST	53	60758	8.8.8.8	192.168.2.4
May 12, 2022 10:31:47.738454103 CEST	60647	53	192.168.2.4	8.8.8.8
May 12, 2022 10:31:47.848288059 CEST	53	60647	8.8.8.8	192.168.2.4
May 12, 2022 10:31:54.446476936 CEST	64909	53	192.168.2.4	8.8.8.8
May 12, 2022 10:31:54.553020000 CEST	53	64909	8.8.8.8	192.168.2.4
May 12, 2022 10:32:00.555375099 CEST	56509	53	192.168.2.4	8.8.8.8
May 12, 2022 10:32:00.574847937 CEST	53	56509	8.8.8.8	192.168.2.4
May 12, 2022 10:32:19.817687035 CEST	57747	53	192.168.2.4	8.8.8.8
May 12, 2022 10:32:19.838841915 CEST	53	57747	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 10:32:39.620493889 CEST	58171	53	192.168.2.4	8.8.8.8
May 12, 2022 10:32:39.637758017 CEST	53	58171	8.8.8.8	192.168.2.4
May 12, 2022 10:32:57.095071077 CEST	51679	53	192.168.2.4	8.8.8.8
May 12, 2022 10:32:57.204433918 CEST	53	51679	8.8.8.8	192.168.2.4
May 12, 2022 10:33:02.872683048 CEST	58816	53	192.168.2.4	8.8.8.8
May 12, 2022 10:33:02.982228041 CEST	53	58816	8.8.8.8	192.168.2.4
May 12, 2022 10:33:08.651254892 CEST	56437	53	192.168.2.4	8.8.8.8
May 12, 2022 10:33:08.670778036 CEST	53	56437	8.8.8.8	192.168.2.4

DNS Queries

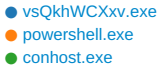
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2022 10:31:41.317061901 CEST	192.168.2.4	8.8.8.8	0xc1ba	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 12, 2022 10:31:47.738454103 CEST	192.168.2.4	8.8.8.8	0x9415	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 12, 2022 10:31:54.446476936 CEST	192.168.2.4	8.8.8.8	0x895c	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 12, 2022 10:32:00.555375099 CEST	192.168.2.4	8.8.8.8	0xfcda	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 10:32:19.817687035 CEST	192.168.2.4	8.8.8.8	0x48e2	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 10:32:39.620493889 CEST	192.168.2.4	8.8.8.8	0xae23	Standard query (0)	mikeljack321.ddns.net	A (IP address)	IN (0x0001)
May 12, 2022 10:32:57.095071077 CEST	192.168.2.4	8.8.8.8	0x6306	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 12, 2022 10:33:02.872683048 CEST	192.168.2.4	8.8.8.8	0xf208	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 12, 2022 10:33:08.651254892 CEST	192.168.2.4	8.8.8.8	0x99b9	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)

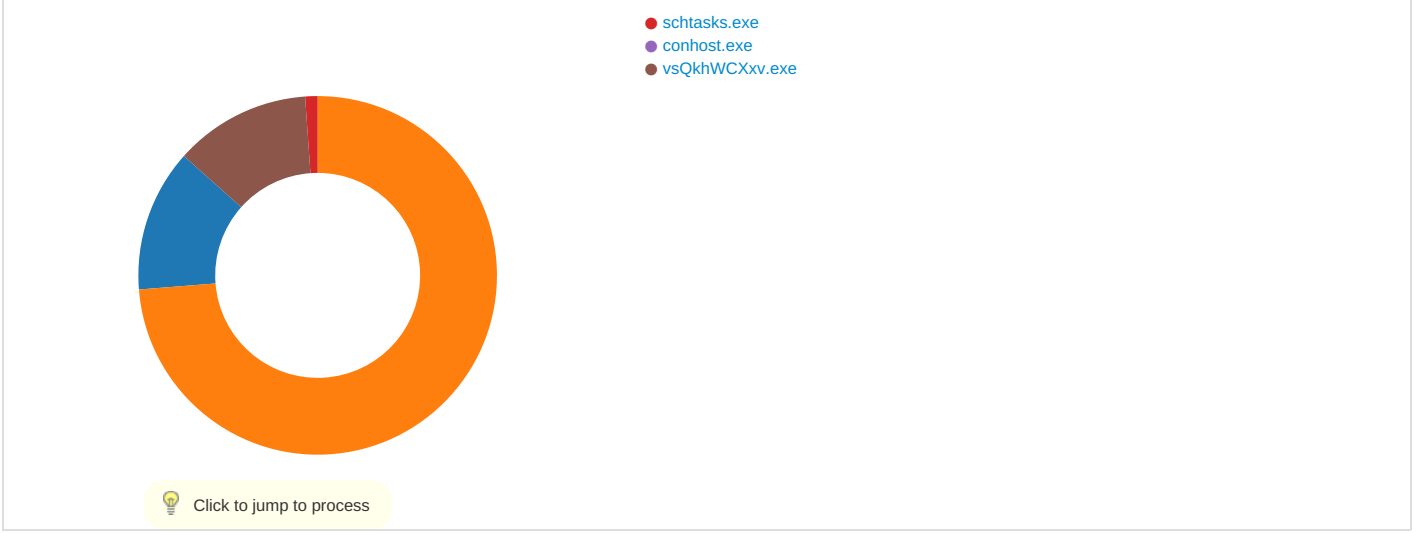
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2022 10:31:41.425947905 CEST	8.8.8.8	192.168.2.4	0xc1ba	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 12, 2022 10:31:47.848288059 CEST	8.8.8.8	192.168.2.4	0x9415	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 12, 2022 10:31:54.553020000 CEST	8.8.8.8	192.168.2.4	0x895c	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 12, 2022 10:32:00.574847937 CEST	8.8.8.8	192.168.2.4	0xfcda	No error (0)	mikeljack321.ddns.net		84.38.129.53	A (IP address)	IN (0x0001)
May 12, 2022 10:32:19.838841915 CEST	8.8.8.8	192.168.2.4	0x48e2	No error (0)	mikeljack321.ddns.net		84.38.129.53	A (IP address)	IN (0x0001)
May 12, 2022 10:32:39.637758017 CEST	8.8.8.8	192.168.2.4	0xae23	No error (0)	mikeljack321.ddns.net		84.38.129.53	A (IP address)	IN (0x0001)
May 12, 2022 10:32:57.204433918 CEST	8.8.8.8	192.168.2.4	0x6306	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 12, 2022 10:33:02.982228041 CEST	8.8.8.8	192.168.2.4	0xf208	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 12, 2022 10:33:08.670778036 CEST	8.8.8.8	192.168.2.4	0x99b9	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)

Statistics

Behavior





System Behavior

Analysis Process: vsQkhWCXxv.exe PID: **3472**, Parent PID: **6092**

General

Target ID:	0
Start time:	10:30:54
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\vsQkhWCXxv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\vsQkhWCXxv.exe"
Imagebase:	0x6f0000
File size:	1093632 bytes
MD5 hash:	FF76DA5616699735C9F7C70BA9E66909
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: INDICATOR_EXE_Packed_DotNetReactor, Description: Detects executables packed with unregistered version of .NET Reactor, Source: 00000000.00000002.346722851.0000000005340000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.340724952.0000000002BE8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.342641640.0000000003BB9000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.342641640.0000000003BB9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.342641640.0000000003BB9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.343578588.0000000003DAA000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.343578588.0000000003DAA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.343578588.0000000003DAA000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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	6DA4CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DA4CF06	unknown
C:\Users\user\AppData\Roaming\vyJCJmhRnRK.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	6C89DD66	CopyFileW
C:\Users\user\AppData\Roaming\vyJCJmhRnRK.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C89DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp5508.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C897038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vsQkhWCXxv.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD5C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5508.tmp	success or wait	1	6C896A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\vyJCJmhRnRK.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 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 fd fd 2e 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 10 00 00 0a 00 00 00 00 00 00 36 fd 10 00 00 20 00 00 00 fd 10 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 20 11 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.$PEL.b06 @ @	success or wait	5	6C89DD66	CopyFileW
C:\Users\user\AppData\Roaming\vyJCJmhRnRK.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	6C89DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5508.tmp	0	1598	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 6a 6f 6e 65 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 20	<?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	6C891B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vsQkhWCXxv.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	6DD5C907	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	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA25705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C891B4F	ReadFile

Analysis Process: powershell.exe PID: **1300**, Parent PID: **3472**

General

Target ID:	12
Start time:	10:31:24
Start date:	12/05/2022
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\vyJCJmhRnRK.exe
Imagebase:	0xa90000
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	6DA4CF06	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	6DA4CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C7F5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C7F5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qftbfgou.aym.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C891E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jpzyxe0b.155.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C891E60	CreateFileW
C:\Users\user\Documents\20220512	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C89BEFF	CreateDirectoryW
C:\Users\user\Documents\20220512\PowerShell_transcript.878411.S4i67LBI.20220512103126.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C891E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qftbfgou.aym.ps1	success or wait	1	6C896A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jpzyxe0b.155.psm1	success or wait	1	6C896A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qftbfgou.aym.ps1	0	1	31	1	success or wait	1	6C891B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jpzyxe0b.155.psm1	0	1	31	1	success or wait	1	6C891B4F	WriteFile
C:\Users\user\Documents\20220512\PowerShell_transcript.878411.S4i67LBI.20220512103126.txt	0	3	ff		success or wait	1	6C891B4F	WriteFile
C:\Users\user\Documents\20220512\PowerShell_transcript.878411.S4i67LBI.20220512103126.txt	3	678	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 35 31 32 31 30 33 31 33 30 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 6a 6f 6e 65 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 6a 6f 6e 65 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 38 37 38 34 31 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 57 69	**********Windows PowerShell transcript startStart time: 20220512103130Username: computer\userRunAsUser: computer\userConfiguration Name: Machine: 878411 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6C891B4F	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 73 14 00 00 19 00 00 00 4b 0c fd 04 fd 07 fd 07 fd 07 00 00 fd 01 63 00 09 00 2c 0c 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@esKc,@	success or wait	1	6DD176FC	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 58 00 00 00 0e 00 20 00	H<@^L"My:X	success or wait	17	6DD176FC	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	6DD176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DD176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DD176FC	WriteFile

Copyright Joe Security LLC 2022

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 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 01 40 00 55 00 40 00 47 00 40 00 fd 29 40 01 fd 3f 40 01 fd 6f 40 01 fd 6f 40 01 fd 6f 40 01 fd 3f 40 01 56 00 40 00 fd 01 40 00 fd 00 40 00 fd 00 40 00 56 01 40 00 fd 67 40 01 48 01 40 00 58 01 40 00 fd 01 40 00 fd 00 40 00 5b 01 40 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 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40	T@>@@U@G@)@? @o@o@o@? @V@@@@V@g@ 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@;M@D@D@@M @<M@	success or wait	11	6DD176FC	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	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA2CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA2CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA25705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DA31F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23124	success or wait	1	6DA3203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9803DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C891B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C891B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C891B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	70	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C891B4F	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C891B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C891B4F	ReadFile

Analysis Process: conhost.exe PID: **1308**, Parent PID: **1300**

General

Target ID:	13
Start time:	10:31:24
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: **6280**, Parent PID: **3472**

General

Target ID:	15
Start time:	10:31:31
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\vyJCJmhRnRK" /XML "C:\Users\user\AppData\Local\Temp\tmp5508.tmp
Imagebase:	0x9e0000
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\tmp5508.tmp	unknown	2	success or wait	1	9EAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5508.tmp	unknown	1599	success or wait	1	9EABD9	ReadFile

Analysis Process: conhost.exe PID: **6288**, Parent PID: **6280**

General

Target ID:	16
Start time:	10:31:32
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: vsQkhWCXxv.exe PID: **6340**, Parent PID: **3472**

General

Target ID:	17
Start time:	10:31:33
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\vsQkhWCXxv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\vsQkhWCXxv.exe
Imagebase:	0x790000
File size:	1093632 bytes
MD5 hash:	FF76DA5616699735C9F7C70BA9E66909
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.517843994.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.517843994.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.517843994.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.334851227.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.334851227.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.334851227.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.526264633.0000000005E00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000011.00000002.526264633.0000000005E00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.526264633.0000000005E00000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000011.00000002.526264633.0000000005E00000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.336072667.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.336072667.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.336072667.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.335466598.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.335466598.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.335466598.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.525905019.0000000005460000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000011.00000002.525905019.0000000005460000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000011.00000002.525905019.0000000005460000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.523753940.0000000002BD1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.337380622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.337380622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.337380622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.524933429.0000000003BD9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.524933429.0000000003BD9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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	6DA4CF06	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	6DA4CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C89BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C891E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C89BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C89BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\vsQkhWCXxv.exe:Zone.Identifier	success or wait	1	6C812935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	04 fd 7a fd fd 33 fd 48	z3H	success or wait	1	6C891B4F	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	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C891B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C891B4F	ReadFile
C:\Users\user\Desktop\vsQkhWCXxv.exe	unknown	4096	success or wait	1	6DA0D72F	unknown
C:\Users\user\Desktop\vsQkhWCXxv.exe	unknown	512	success or wait	1	6DA0D72F	unknown

Disassembly

No disassembly