ID: 528801
Sample Name:
nxHHI8WXqt.exe
Cookbook: default.jbs
Time: 19:53:23
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

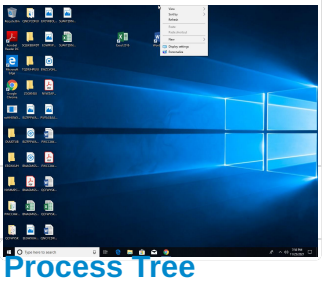
Windows Analysis Report nxHHI8WXqt.exe

Overview

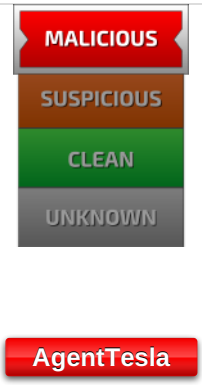
General Information

Sample Name:	nxHHI8WXqt.exe
Analysis ID:	528801
MD5:	f65b0793251364c.
SHA1:	7bc80e89bbc7c1…
SHA256:	a031918e001745..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



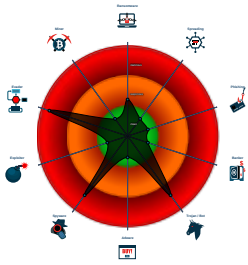
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- .NET source code contains potentia…
- Sigma detected: Powershell Defende…

Classification



Process Tree

- **System is w10x64**
- nxHHI8WXqt.exe (PID: 5860 cmdline: "C:\Users\user\Desktop\nxHHI8WXqt.exe" MD5: F65B0793251364C03D06E8E7134FC21B)
  - powershell.exe (PID: 6460 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\SzfukVRF.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6552 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\SzfukVRF" /XML "C:\Users\user\AppData\Local\Temp\tmp2EEC.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nxHHI8WXqt.exe (PID: 6728 cmdline: C:\Users\user\Desktop\nxHHI8WXqt.exe MD5: F65B0793251364C03D06E8E7134FC21B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "dubai@skycomex.com",
  "Password": "@EHbqYU1",
  "Host": "us2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000000.301853445.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000000.301853445.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000012.00000000.302484338.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000012.00000000.302484338.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.305015661.000000000311000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
18.0.nxHHI8WXqt.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.0.nxHHI8WXqt.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
18.0.nxHHI8WXqt.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.0.nxHHI8WXqt.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.2.nxHHI8WXqt.exe.4255658.2.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: 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

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

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)

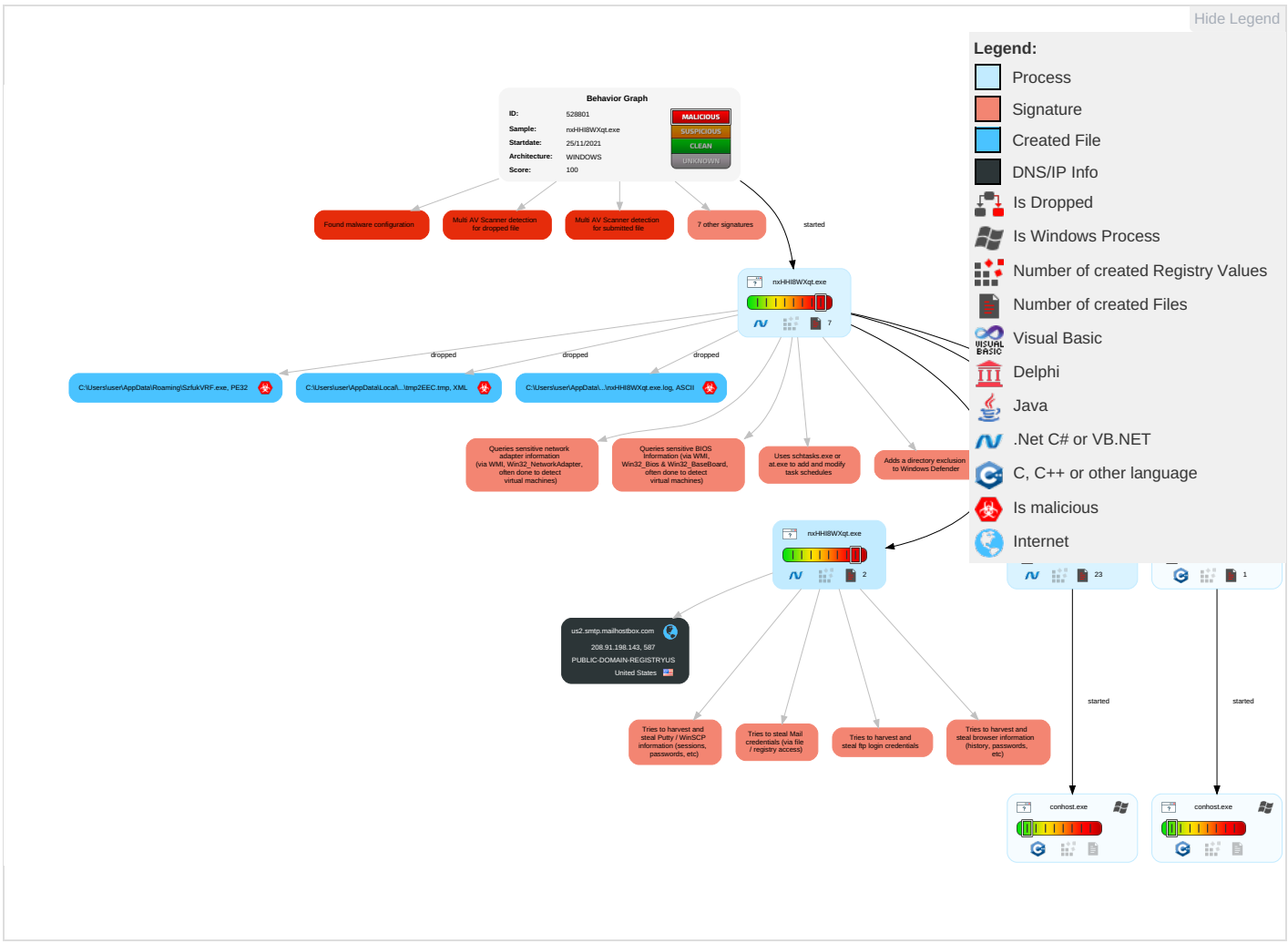
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	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	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 1 4	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 1 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	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 Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	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
nxHHI8WXqt.exe	27%	Virustotal		Browse
nxHHI8WXqt.exe	25%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\SzfukVRF.exe	25%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.nxHHI8WXqt.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.nxHHI8WXqt.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.nxHHI8WXqt.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.nxHHI8WXqt.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.nxHHI8WXqt.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.nxHHI8WXqt.exe.400000.8.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://PClGeN.com	0%	Avira URL Cloud	safe	
http://https://uvZLQjYprvsPcwavb.net4	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	
http://https://uvZLQjYprvsPcwavb.net	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.143	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.143	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528801
Start date:	25.11.2021
Start time:	19:53:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nxHHI8WXqt.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:	32
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@9/8@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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
19:54:17	API Interceptor	803x Sleep call for process: nxHHI8WXqt.exe modified
19:54:23	API Interceptor	44x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	PAGO DEL SALDO.doc	Get hash	malicious	Browse	
	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	
	Reconfirm The Details.doc	Get hash	malicious	Browse	
	Document.exe	Get hash	malicious	Browse	
	MT_101_SWIFT.doc	Get hash	malicious	Browse	
	Purchase Order PO#7701.exe	Get hash	malicious	Browse	
	TNT E-Invoice No 11073490.exe	Get hash	malicious	Browse	
	E invoice.exe	Get hash	malicious	Browse	
	UY2021 Ta-Ho Maritime Schedule.exe	Get hash	malicious	Browse	
	PNkBekAKOeQD1Jj.exe	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	
	DHL Documentos de envio originales.exe	Get hash	malicious	Browse	
	XSsBxQH419.exe	Get hash	malicious	Browse	
	devis.xlsx	Get hash	malicious	Browse	
	Quotation- 306013SQ.exe	Get hash	malicious	Browse	
	PO 4601056018.exe	Get hash	malicious	Browse	
	Purchase Order Vale-60,000MT.exe	Get hash	malicious	Browse	
	BOQ 11745692.exe	Get hash	malicious	Browse	
	dhl_doc9548255382.exe	Get hash	malicious	Browse	
	ADYP_210913_100641_PAGOS_005539.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	PAGO DEL SALDO.doc	Get hash	malicious	Browse	• 208.91.198.143
	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	• 208.91.199.224
	Reconfirm The Details.doc	Get hash	malicious	Browse	• 208.91.199.224
	Document.exe	Get hash	malicious	Browse	• 208.91.198.143
	MT_101_SWIFT.doc	Get hash	malicious	Browse	• 208.91.199.225
	ORDER INQUIRY-PVP-SP-2021-58.exe	Get hash	malicious	Browse	• 208.91.199.224
	DOC221121.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift_HSBC_0099087645 xOJ4XUjdMZ40k5Hpdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Swift_HSBC_0099087645PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	P0_636732672772_RFQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	rTyPU1zmY5PsyNl.exe	Get hash	malicious	Browse	• 208.91.199.223

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DOCUMENTS.exe	Get hash	malicious	Browse	• 208.91.199.223
	Purchase Order PO#7701.exe	Get hash	malicious	Browse	• 208.91.198.143
	STATEMENT OF ACCOUNT.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	XsFFv27rls.exe	Get hash	malicious	Browse	• 208.91.199.225
	TransactionSummary_22-11-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	TNT E-Invoice No 11073490.exe	Get hash	malicious	Browse	• 208.91.198.143
	E invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	TOP QUOTATION RFQ 2021.exe	Get hash	malicious	Browse	• 208.91.199.223
	(KOREA SHIPPING - KLCSM).exe	Get hash	malicious	Browse	• 208.91.199.224

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	PAGO DEL SALDO.doc	Get hash	malicious	Browse	• 208.91.199.224
	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	• 208.91.199.224
	Reconfirm The Details.doc	Get hash	malicious	Browse	• 208.91.199.224
	Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift Copy TT.doc	Get hash	malicious	Browse	• 207.174.212.140
	MT_101_SWIFT.doc	Get hash	malicious	Browse	• 208.91.199.224
	ORDER INQUIRY-PVP-SP-2021-58.exe	Get hash	malicious	Browse	• 208.91.199.224
	DOC221121.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift_HSBC_0099087645PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	P0_636732672772_RFQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	DOCUMENTS.exe	Get hash	malicious	Browse	• 208.91.199.223
	Activation Online Mail.htm	Get hash	malicious	Browse	• 103.50.163.110
	Purchase Order PO#7701.exe	Get hash	malicious	Browse	• 208.91.198.143
	STATEMENT OF ACCOUNT.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	XsFFv27rls.exe	Get hash	malicious	Browse	• 208.91.199.225
	TNT E-Invoice No 11073490.exe	Get hash	malicious	Browse	• 208.91.199.225
	SWIFT COPY.exe	Get hash	malicious	Browse	• 199.79.62.99
	E invoice.exe	Get hash	malicious	Browse	• 208.91.199.225
	TOP QUOTATION RFQ 2021.exe	Get hash	malicious	Browse	• 208.91.199.224
	TOwYernH3DhfPER.exe	Get hash	malicious	Browse	• 208.91.199.181

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\SzfukVRF.exe	PAGO DEL SALDO.doc	Get hash	malicious	Browse	
	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nxHHI8WXqt.exe.log

Process:	C:\Users\user\Desktop\nxHHI8WXqt.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntIxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nxHHI8WXqt.exe.log	
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):	22380
Entropy (8bit):	5.602880384397681
Encrypted:	false
SSDEEP:	384:gtCDmkG5FhnBaq8I3RYS0n0jultI277Y9gtSJ3x+T1MarZlbAV76eajtwaZBDI+a:2DhnBx8IuT0CltZftc0CSfw2eaVg
MD5:	6E5AA2B59FB30334DF2D79A38145AF66
SHA1:	40E37B125CB865884CD3E83EBB2EBE368D0BB9BB
SHA-256:	AB1905EC107D69521C6D349A4937527CADFFC599A39DED4EE5A5E117F4071D79
SHA-512:	7030BF251BF02F6FB17BE0CB45357364F1D7B650C628750E33E116E2AE50F90B07F5228C24283743D203F99B12EC0929390137FECB1117C3956770DB0B3408AA
Malicious:	false
Reputation:	low
Preview:	@...e.....h.....l.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lwqp4ijl.fo4.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:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_u4tbugmi.jyn.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:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp2EEC.tmp	
Process:	C:\Users\user\Desktop\nxHHI8WXqt.exe

C:\Users\user\AppData\Local\Temp\tmp2EEC.tmp	
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1595
Entropy (8bit):	5.151890175604769
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt5xvn:cge4MYrFdOFzOzN33ODOiDdKrsuTvv
MD5:	D286D620E2CCCEDAE1239D3C2CE20B8C
SHA1:	6B470B148C7765CFB9215E651B0E515E4F51362F
SHA-256:	AE83FF0BA1D10EE2F0FF8341DD2B11BE763D7FA938DD61715E46FF08D83D9ACA
SHA-512:	762E66A5CB6FF8958DBD9B88853693624725E0394590F0FA50173A2DF17588241CC148F99444B1FB8D0F6246B2AA97C39F22BFF43F0D64C141C477A7621D0334
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\SzfukVRF.exe	
Process:	C:\Users\user\Desktop\nxHHI8WXqt.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	504832
Entropy (8bit):	7.875034070984988
Encrypted:	false
SSDEEP:	12288:+v5E70ZixBFm0hDKr62YWLJp7WtXpcCAVS4EzOnsQ7b51:+vG70Zi1hy6O+LAVS4C
MD5:	F65B0793251364C03D06E8E7134FC21B
SHA1:	7BC80E89BBC7C10B974462E748849F9056D20D4A
SHA-256:	A031918E001745C0F07D5D0AC118A0BFEB946236033E20FA1B16E0D54EE7BCB8
SHA-512:	BAC2E15EAFEFF6708D67A224B96FBC62F062A6029D7E5DFCB773C2B07AAC4C01F910724192A6294DA3456B50E016F5A9859E9DD6EA18C2C51F02377AFBA3CB2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 25%
Joe Sandbox View:	• Filename: PAGO DEL SALDO.doc, Detection: malicious, Browse • Filename: MT_1O1_SWIFt.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.a.....0..... .....@.. ....@.....\|...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...t.....\... .....{ ...*..{!...*..{"...*..{#...*..($....} ....}!.....}".....}#...*....0..s.....u.....f..`(%....{ ....{ ...o&.. .,H('....{!....{!...o(...,0()....{"....{"...o*....,(+....{#....{#...o,...+..+..*..0..b..... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0.....r...p .....%..{ .....%q.....-.&.+.....o1....%..{!.....%q.....-.&.+.....

C:\Users\user\AppData\Roaming\SzfukVRF.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\nxHHI8WXqt.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\Documents\20211125\PowerShell_transcript.302494.M+vU4FE1.20211125195422.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):	5781
Entropy (8bit):	5.41314189541502
Encrypted:	false
SSDEEP:	96:BZuhAZNjqDo1ZtZthAZNjqDo1ZVEecjZKhAZNjqDo1ZzFMMMZj:c
MD5:	CAEADA81F2A001ED83A0883F818406CA

C:\Users\user\Documents\20211125\PowerShell_transcript.302494.M+vU4FE1.20211125195422.txt	
SHA1:	859E6592F3CE17B2BE44A982BA54E9B8FA221670
SHA-256:	42F4DF7A5DE48C0342CC19FE859D41717A4FE6B81A2DEDE517B166534FC05F6E
SHA-512:	25CC3085F3CE60ABD9AAF950F2D8A7D9A78281A8438F2B768A48351FEE115E46674B4B334EE094E3CB80064E40D04F598DB6DA31E77DDCEEF19B9A9C7EB7D374
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211125195423..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 302494 (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\SzfukVRF.exe..Process ID: 6460..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: 20211125195423..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\SzfukVRF.exe..**********..Windows PowerShell transcript start..Start time: 20211125195833..Username: computer\user..RunAs User: computer\user..C

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.875034070984988
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:	nxHHI8WXqt.exe
File size:	504832
MD5:	f65b0793251364c03d06e8e7134fc21b
SHA1:	7bc80e89bbc7c10b974462e748849f9056d20d4a
SHA256:	a031918e001745c0f07d5d0ac118a0bfeb946236033e20fa1b16e0d54ee7bcb8
SHA512:	bac2e15eafeff6708d67a224b96fbc62f062a6029d7e5dfcb773c2b07aac4c01f910724192a6294da3456b50e016f5a9859e9dd6ea18c2c51f02377afba3cb82
SSDEEP:	12288:+v5E70ZixBFm0hDKr62YWLJp7WtXpcCAVS4EzOnsQ7b51:+vG70Zi1hy6O+LAVS4C
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.a.....0..... ....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47c9ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F6AFA [Thu Nov 25 10:52:42 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

General

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	0x7a9e4	0x7aa00	False	0.898564920999	data	7.88557099769	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x5bc	0x600	False	0.429036458333	data	4.13584862194	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x80000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 19:56:05.620966911 CET	192.168.2.3	8.8.8.8	0xa0c3	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 19:56:05.667192936 CET	8.8.8.8	192.168.2.3	0xa0c3	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 19:56:05.667192936 CET	8.8.8.8	192.168.2.3	0xa0c3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 19:56:05.667192936 CET	8.8.8.8	192.168.2.3	0xa0c3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 19:56:05.667192936 CET	8.8.8.8	192.168.2.3	0xa0c3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: nxHHI8WXqt.exe PID: 5860 Parent PID: 5752

General

Start time:	19:54:15
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\nxHHI8WXqt.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\nxHHI8WXqt.exe"
Imagebase:	0xd10000
File size:	504832 bytes
MD5 hash:	F65B0793251364C03D06E8E7134FC21B
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: 00000003.00000002.305015661.0000000003121000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000003.00000002.305431251.0000000003268000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.306747115.000000000412D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.306747115.000000000412D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6460 Parent PID: 5860

General

Start time:	19:54:20
Start date:	25/11/2021
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\SzfukVRF.exe
Imagebase:	0x1350000
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: 6532 Parent PID: 6460

General

Start time:	19:54:21
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 6552 Parent PID: 5860

General

Start time:	19:54:21
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\SzfukVRF" /XML "C:\Users\user\AppData\Local\Temp\tmp2EEC.tmp
Imagebase:	0x840000
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: 6676 Parent PID: 6552

General

Start time:	19:54:22
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: nxHHI8WXqt.exe PID: 6728 Parent PID: 5860

General

Start time:	19:54:23
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\nxHHI8WXqt.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\nxHHI8WXqt.exe
Imagebase:	0xa40000
File size:	504832 bytes
MD5 hash:	F65B0793251364C03D06E8E7134FC21B
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: 00000012.00000000.301853445.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.301853445.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000000.302484338.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.302484338.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.550983065.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000002.550983065.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000000.300499752.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.300499752.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000000.301120055.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.301120055.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.558386692.0000000002F41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.558386692.0000000002F41000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis