ID: 404206
Sample Name: 1g1NLI6i33.exe
Cookbook: default.jbs
Time: 19:54:48
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

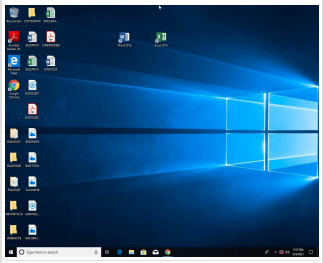
Analysis Report 1g1NLI6i33.exe

Overview

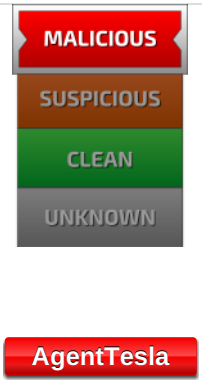
General Information

Sample Name:	1g1NLI6i33.exe
Analysis ID:	404206
MD5:	d0a8c2403c51ea..
SHA1:	825a057b9218a9..
SHA256:	0c397ebc470f594..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



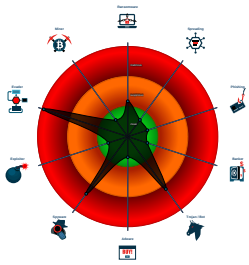
AgentTesla

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

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- .NET source code contains very larg…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Moves itself to temp directory
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- 1g1NLI6i33.exe (PID: 7020 cmdline: 'C:\Users\user\Desktop\1g1NLI6i33.exe' MD5: D0A8C2403C51EA96D820DCD443F1AAAB)
  - 1g1NLI6i33.exe (PID: 7060 cmdline: 'C:\Users\user\Desktop\1g1NLI6i33.exe' MD5: D0A8C2403C51EA96D820DCD443F1AAAB)
- vsbqyetogexvl.exe (PID: 6712 cmdline: 'C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe' MD5: D0A8C2403C51EA96D820DCD443F1AAAB)
  - vsbqyetogexvl.exe (PID: 900 cmdline: 'C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe' MD5: D0A8C2403C51EA96D820DCD443F1AAAB)
- vsbqyetogexvl.exe (PID: 6956 cmdline: 'C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe' MD5: D0A8C2403C51EA96D820DCD443F1AAAB)
  - vsbqyetogexvl.exe (PID: 6584 cmdline: 'C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe' MD5: D0A8C2403C51EA96D820DCD443F1AAAB)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "elliech@orlonimages.comchidiebere2419us2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.917550398.000000000499 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.915225171.00000000034E 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.703927470.00000000006C A000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.704176469.000000000253 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.704176469.000000000253 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 27 entries				

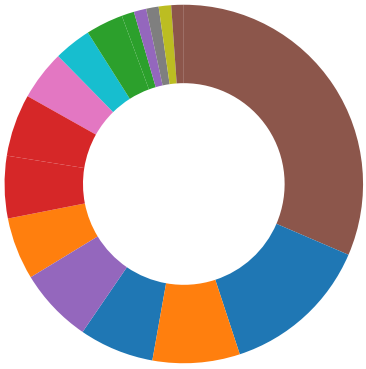
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.1g1NLI6i33.exe.23d0000.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.1g1NLI6i33.exe.24f0000.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.vsbqyetogexvl.exe.6e6240.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.vsbqyetogexvl.exe.4970000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.vsbqyetogexvl.exe.415058.0.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 46 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

Malware Analysis System Evasion:

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

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

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

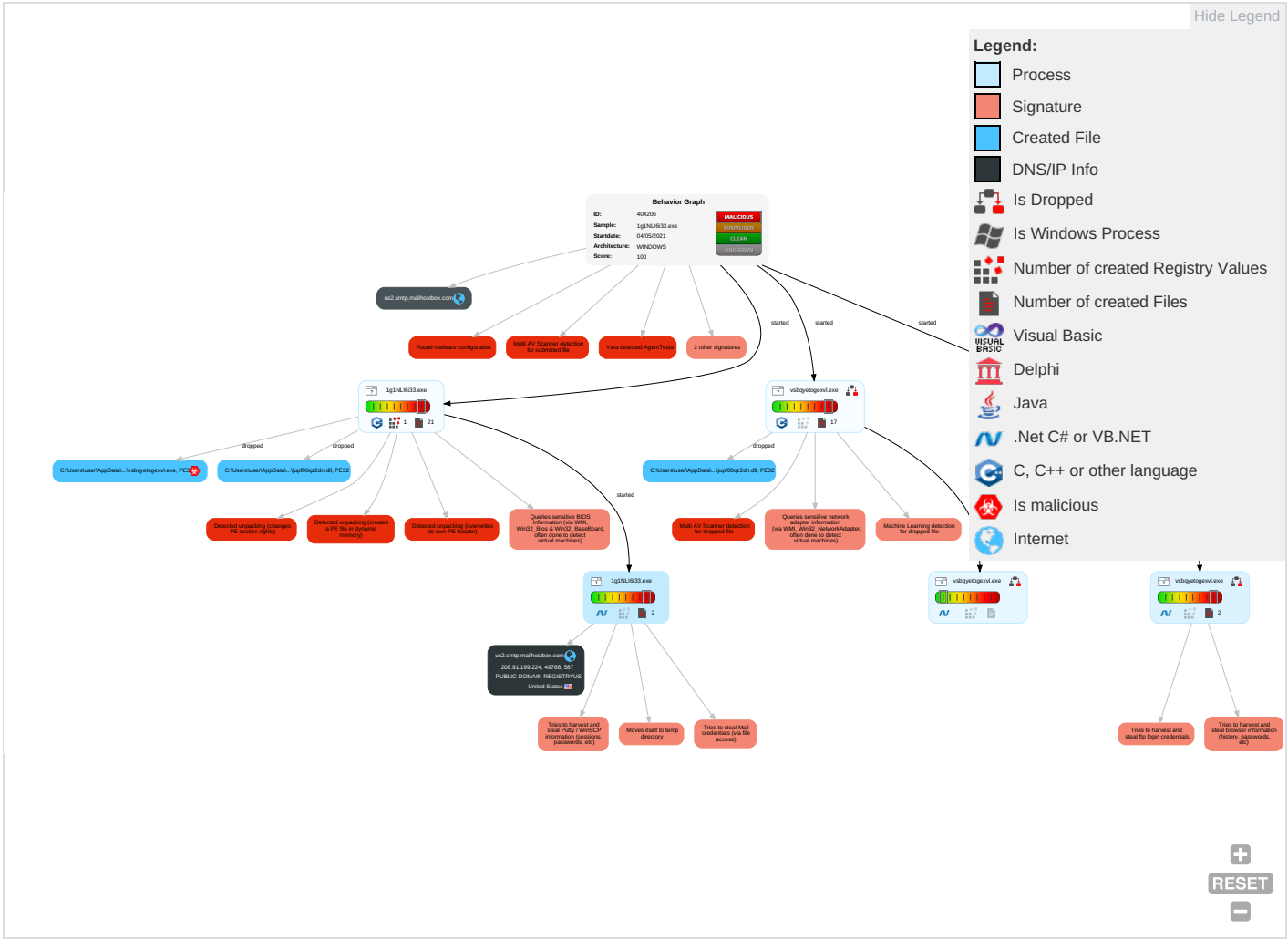
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 2 7	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 1	NTDS	Query Registry 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 1	LSA Secrets	Security Software Discovery 2 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 1 4 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 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
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 Protocol

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1g1NLI6i33.exe	29%	Virustotal		Browse
1g1NLI6i33.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe	43%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.vsbqyetogexvl.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
8.0.vsbqyetogexvl.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.1g1NLI6i33.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
7.2.vsbqyetogexvl.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.1g1NLI6i33.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
6.2.vsbqyetogexvl.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.1g1NLI6i33.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.1.vsbqyetogexvl.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.2.vsbqyetogexvl.exe.49b0000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.1g1NLI6i33.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.1g1NLI6i33.exe.4990000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.1g1NLI6i33.exe.30c0000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.vsbqyetogexvl.exe.4960000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.vsbqyetogexvl.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
9.0.vsbqyetogexvl.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
8.2.vsbqyetogexvl.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
9.1.vsbqyetogexvl.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.2.vsbqyetogexvl.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://1UVMV9Y76P8yRzwJn.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%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://kVHmOE.com	0%	Avira URL Cloud	safe	

Domains and IPs

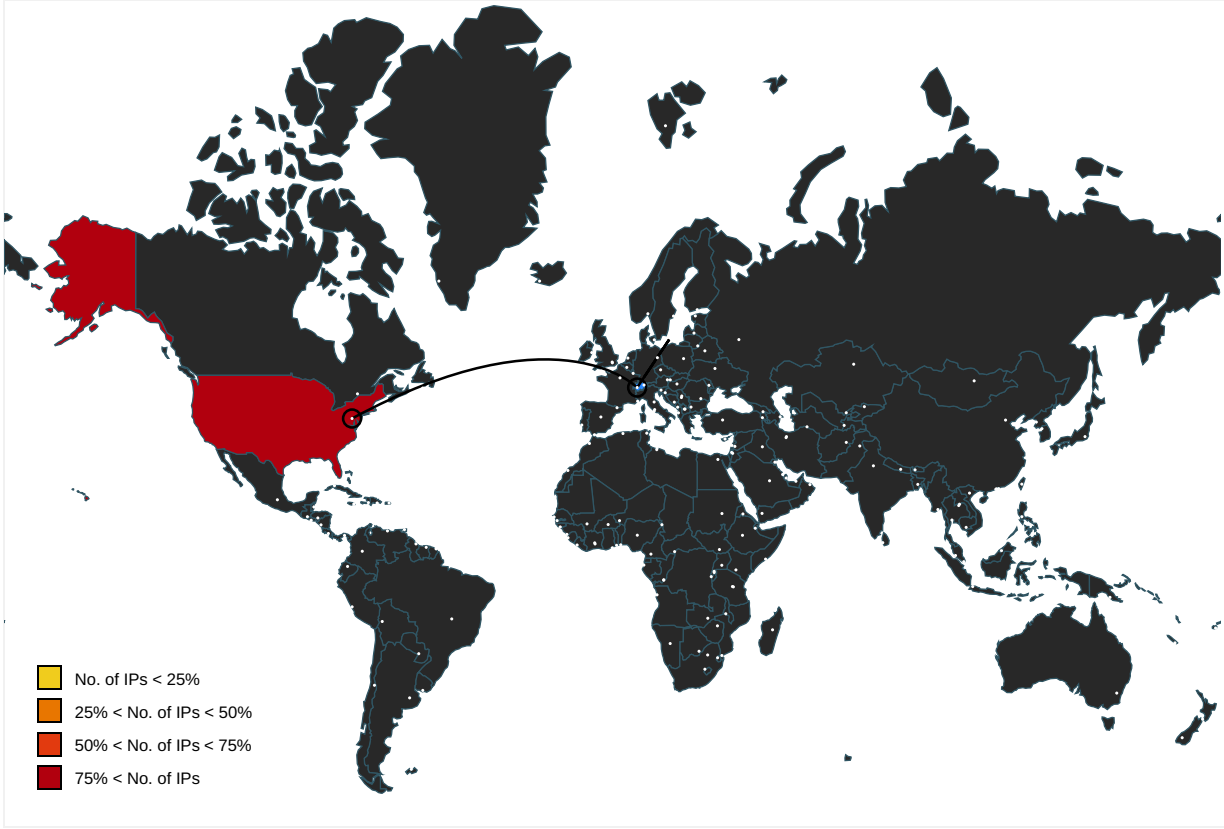
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.224	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	1g1NLI6i33.exe, 00000001.00000002.914864176.00000000028AD000.00000004.00000001.sdmp, vsbqyetogexvl.exe, 00000009.00000002.918526939.0000000005A95000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	1g1NLI6i33.exe, 00000001.00000002.914206758.0000000002551000.00000004.00000001.sdmp, vsbqyetogexvl.exe, 00000007.00000002.704176469.0000000002531000.00000004.00000001.sdmp, vsbqyetogexvl.exe, 00000009.00000002.913898804.00000000024E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ocsp.sectigo.com0A	1g1NLI6i33.exe, 00000001.00000002.914864176.00000000028AD000.00000004.00000001.sdmp, vsbqyetogexvl.exe, 00000009.00000002.918526939.0000000005A95000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://DynDns.comDynDNS	vsbqyetogexvl.exe, 00000009.00000002.913898804.00000000024E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	1g1NLI6i33.exe, 00000001.00000002.914864176.00000000028AD000.00000004.00000001.sdmp, vsbqyetogexvl.exe, 00000009.00000002.918526939.0000000005A95000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_Error	1g1NLI6i33.exe	false		high
http://1UVMV9Y76P8yRzwJn.net	vsbqyetogexvl.exe, 00000009.00000002.914620731.000000000280A000.00000004.00000001.sdmp, vsbqyetogexvl.exe, 00000009.00000002.913898804.00000000024E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	1g1NLI6i33.exe	false		high
http://us2.smtp.mailhostbox.com	1g1NLI6i33.exe, 00000001.00000002.914841865.00000000028A5000.00000004.00000001.sdmp, vsbqyetogexvl.exe, 00000009.00000002.914664635.000000000283A000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	1g1NLI6i33.exe, 00000001.00000002.914206758.0000000002551000.00000004.00000001.sdmp, vsbqyetogexvl.exe, 00000007.00000002.704176469.0000000002531000.00000004.00000001.sdmp, vsbqyetogexvl.exe, 00000009.00000002.913898804.00000000024E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	vsbqyetogexvl.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://kVHmOE.com	vsbqyetogexvl.exe, 00000009.00000002.913898804.00000000024E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404206
Start date:	04.05.2021
Start time:	19:54:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1g1NLI6i33.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:	23
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@9/13@2/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 20.6% (good quality ratio 19.1%) • Quality average: 77.8% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 92% • 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 • Excluded IPs from analysis (whitelisted): 20.82.210.154, 131.253.33.200, 13.107.22.200, 52.147.198.201, 104.43.193.48, 92.122.145.220, 13.88.21.125, 104.43.139.144, 92.122.213.247, 92.122.213.194, 52.155.217.156, 8.241.78.126, 8.241.82.254, 8.241.126.121, 8.241.88.254, 8.241.89.254, 20.54.26.129, 40.64.100.89 • Excluded domains from analysis (whitelisted): mw1eap.displaycatalog.md.mp.microsoft.com.akadns.net, displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net, consumerrp-displaycatalog-aks2eap-uswest.md.mp.microsoft.com.akadns.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, displaycatalog-uswesteap.md.mp.microsoft.com.akadns.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:55:40	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run yhtskiwswufgck C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
19:55:46	API Interceptor	697x Sleep call for process: 1g1NLI6i33.exe modified
19:55:48	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run yhtskiwswufgck C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
19:55:50	API Interceptor	569x Sleep call for process: vsbqyetogexvl.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.224	PO.xlsx	Get hash	malicious	Browse	
	Purchase Orde.pdf.exe	Get hash	malicious	Browse	
	LM Approved Invoice-03-05-2021.doc	Get hash	malicious	Browse	
	REQUEST FOR PRICE QUOTE - URGENT.exe	Get hash	malicious	Browse	
	purchace order.exe	Get hash	malicious	Browse	
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	
	Payment Advice Note from 30.04.2021 to 608760.exe	Get hash	malicious	Browse	
	Quotation-27-04-2021_PDF.exe	Get hash	malicious	Browse	
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	
	Sales order 191923.exe	Get hash	malicious	Browse	
	NEW ORDER.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.686.5407.exe	Get hash	malicious	Browse	
	Order Items.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Save.a.25790.exe	Get hash	malicious	Browse	
	hh$$$.exe	Get hash	malicious	Browse	
	RApK2RmjFR.exe	Get hash	malicious	Browse	
	PO#5300008762.exe	Get hash	malicious	Browse	
	35yLPwVr54.exe	Get hash	malicious	Browse	
	HTC-13051989.exe	Get hash	malicious	Browse	
	DHL In-TrTransit Notification, Reference Number.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Mlj6rE49Bf.exe	Get hash	malicious	Browse	• 208.91.199.223
	DHL Shipment Delivery Notification.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order Request .pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	QuoteXrequestX-DAX31312.exe	Get hash	malicious	Browse	• 208.91.199.223
	P I.exe	Get hash	malicious	Browse	• 208.91.198.143
	LM Approved Invoice-04-05-2021.doc	Get hash	malicious	Browse	• 208.91.199.223
	Purchase Orde.pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	LM Approved Invoice-03-05-2021.doc	Get hash	malicious	Browse	• 208.91.199.223
	REQUEST FOR PRICE QUOTE - URGENT.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	razi.exe	Get hash	malicious	Browse	• 208.91.199.223
	Product Sample.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	RQF_001.exe	Get hash	malicious	Browse	• 208.91.198.143
	REQUEST FOR PRICE QUOTE - URGENT.exe	Get hash	malicious	Browse	• 208.91.199.224
	Project Enquiry - KHI To LSG.exe	Get hash	malicious	Browse	• 208.91.199.223
	quotation pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	RFQ.doc	Get hash	malicious	Browse	• 208.91.199.225
	YdenPtYdbt.exe	Get hash	malicious	Browse	• 208.91.198.143
	LM Approved Invoice-02-05-2021.doc	Get hash	malicious	Browse	• 208.91.199.223
	KJ29joA7RS.exe	Get hash	malicious	Browse	• 208.91.199.223

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Mlj6rE49Bf.exe	Get hash	malicious	Browse	• 208.91.199.223
	DHL Shipment Delivery Notification.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order Request .pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	QuoteXrequestX-DAX31312.exe	Get hash	malicious	Browse	• 208.91.199.223
	items.doc	Get hash	malicious	Browse	• 162.215.24 1.145
	P I.exe	Get hash	malicious	Browse	• 208.91.198.143
	LM Approved Invoice-04-05-2021.doc	Get hash	malicious	Browse	• 208.91.198.143

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Orde.pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	LM Approved Invoice-03-05-2021.doc	Get hash	malicious	Browse	• 208.91.199.224
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 209.99.16.216
	REQUEST FOR PRICE QUOTE - URGENT.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	7A124B54.xlsm	Get hash	malicious	Browse	• 119.18.52.7
	Tree Top.html	Get hash	malicious	Browse	• 208.91.199.242
	razi.exe	Get hash	malicious	Browse	• 208.91.199.223
	af8241fb_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.215.24 1.145
	Product Sample.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	RQF_001.exe	Get hash	malicious	Browse	• 208.91.198.143
	REQUEST FOR PRICE QUOTE - URGENT.exe	Get hash	malicious	Browse	• 208.91.199.224
	Project Enquiry - KHI To LSG.exe	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\04v480yduj	
Process:	C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
File Type:	data
Category:	dropped
Size (bytes):	296960
Entropy (8bit):	**7.999373643135451**
Encrypted:	**true**
SSDEEP:	6144:XE/JlF7uLlUemo12UiBuF/3K6MCgCeSMZR/B1Rhmjs1v+9A:g97ulmq2125MHCM1Z1v+9A
MD5:	52DE7375ECF6FDC72E9B19A88433E615
SHA1:	424EC30B0A0F389DBE3A529005BC68E62F21E129
SHA-256:	A57F3187F23A8A700559ABA22514635A044B28EE740E4333D80340EDBE26EF3A
SHA-512:	41E7CF174DFCFFCABCBF599885FF0FF54B0BE83A5D48FCA477E33CFBCBF156013EFF57A0CFCC7087592BD3D2C962ADC1C4809837B4F2951D527D8E2D828E7 76
Malicious:	false
Reputation:	low
Preview:	R...|..>..V..eP..#.=.....HH..ZJd.....t.1.p....9i.!...V.?X.....h...j.%.V7..$v<.....\|..W.?}".&.B;p.....T.WH.\|".~.....oa..9.....d.x.U.....zS.v...8D.Nvu.2...X$.POGy.<..2."....A..i... ..8.5..V...6=...E...nd.....~V...h.....0;9..!...[.u,...7.&..@..;.....,k.....".[..dn-4..<.IL.F.HY.G6..y5..!.M0J.8Bwy(.5.s....M..{.;~..#...4*,..... F..s.~A.....o.bT.....v..x.....F..~.....!.bR.Iy.}P KB..NJ.....".O>...#L..T..J.T.h.p_...`....N..... .D..'.W.$C.).~U..j.YS.e.(...BL.8..%....&.+...;.t.hk.+..u.gq....x.$jj{... -.?.....#..G.....0s..-.O.W..V.0.c..c..L&.x....nB....n=.....'* b.B...s.Z.2..F..+aY.vg...B.>X.....Yd.l..?../O...J.=.^t.G.....B.....<....Q.E.0.Q...r.4..,e.6.U.Z.nZ..N.T[p{hC.G...-.....)...f@V"....n.u.[..6tHB..?..E$.9...=`..aK.#9b[O.....6..0... A..'..18.G./.3.K.&...8o...u.....mpO@]...i.t.x.....5..T..z[.s&tU_..g.\.$n...u..3..P...7...H..]..p.r[..x.0.....Ke.s.AQ."$H..."....JJ...(."HD`...L.....B..%FQkfW..^P>=;

C:\Users\user\AppData\Local\Temp\161f8ahd30a3uiifxj4	
Process:	C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
File Type:	data
Category:	dropped
Size (bytes):	9221
Entropy (8bit):	7.8407978891438175
Encrypted:	false
SSDEEP:	192:utXU91dNf7liMmG4N0TlWxxQ2VCAErhMUlMBu3XEu3XEu3XEu3P:I4LylNM0zCAglMBunnnf
MD5:	4993BD43E04A3A15F927AF54BFD67749
SHA1:	14BC0147D9957452E8FC8E2ABA2290161DE5A36E
SHA-256:	1EA6ACCD7C8BAA930BF4B127FFF9C2B8493D86789D2F4C8EAEE7A2F1849AEA89
SHA-512:	F9480747D29D4B249CC27FCA2471AE62B99670F221A9996C15798351B437F30A84DF6CE10BD3318EB50EDE467FCF4B4115F3293C130E614D41DEAB6676E25527
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\161f8ahd30a3uiifxj4	
Preview:	/.;.....t,..z..) .....9..4.90...$B..$.....&..p..p.....a..e..O...t..r.0....u....(D...t..x.>.).M..M..Q...H..J...'.A..G. J.<.`..`....=.Q..U."C.2.T..R.@...U..o.8`...dQ.h.....m0.m..u...h.. z.....q2.w.0~....;.....t..u=..P..P..IC..H...E..O.8[D..G...H..Z..SS..^+..QB.U..{`..]9..T..X..qo..p.....g..vh..j.....a".g. p.....q..u."u...tK.r.@.+.u..O.8B.0.D..H...!.M..M..C.&.Hw.Z.... ?.Q..W.0\.4.`..`.&.5.Q..U.2a.....n.....h.....G..d. .[....NZ..q..0.....Q...O...9.....i.....{oZ....m.....;.<.:...?...&6....1....@.....7.....[.$..<.....$J^c.<..4.... ....^.....h...9...y.....L.....- ...r..!....@.....F.hs....?....F...-..1.2.>.&..0..."...\..... .....&...:.....%6.<...9..@....8.0.. ...2.....9..t.....H*.....4.;...90.=.....+.....o.....6.....(.5....*..T...}.t.....w.x.O. .....#...#..!...&..:.....9..5.,....>.3.....2.7&...1^...U.p.(.....$..... .<..Yq...(...~.)@.....2

C:\Users\user\AppData\Local\Temp\nsb55F1.tmp\jupf00qz2dn.dll	
Process:	C:\Users\user\Desktop\1g1NLI6i33.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.13790327751178
Encrypted:	false
SSDEEP:	96:BHvn1ASk3NDZ+t20RKgIFln6Rul4jdkpN3:BWuuokajdkpN3
MD5:	AD0988E9810DB71DBBF62EB34162BAEB
SHA1:	78465D48ECBDCB107B6DC1937D823DBE3E789318
SHA-256:	2A344BC8389C27E68EF7BBEAAB1B98E580A9F42A1AD1EA6B2492D9635B7B5105
SHA-512:	EFC528BFB1A08A953437DF4FDB2A9365F76DF784C473A19D2749145A2D22C86035D59E09F9986B4162118F0D541044ACB6DAB2DF5197003CDA18EB8A1B9392F
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.}XX..XX..XX...0./]X....,.UX..XX..xX...1./YX...1./YX...1./YX ..RichXX.....PE..L....?.`.....!..... .....@.....p!..P...".....  .....  ..@.....  ..... .....text...1..... ..`.rdata..... .....@..@.data...T....0.....@..... ....

C:\Users\user\AppData\Local\Temp\nsg55C1.tmp	
Process:	C:\Users\user\Desktop\1g1NLI6i33.exe
File Type:	data
Category:	dropped
Size (bytes):	315042
Entropy (8bit):	7.97484316079725
Encrypted:	false
SSDEEP:	6144:c3E/JlF7uLlUemo12UiBuF/3K6MCgCeSMZR/B1Rhmjs1v+9:T97ulmq2125MHCM1Z1v+9
MD5:	8B9B248ED4ADB4BA5259317DC9C0AC28
SHA1:	9AC1E37E65A9A2BD4F32BF4F89618BEAD8F9F9FB
SHA-256:	41891B82C216709BAE67DBF48537B87829C0F91EFEB192E4F27BD3FADD51F078
SHA-512:	91B76DC90EDB37D4D94AD517E2924AE94D5E0E3CE0378868D35C5335A00564B4ABFDE32EB6A2F1AEE4A90D528B6CB885244C6FE0B7D84BF697B0EFC5F97D4A 5C
Malicious:	false
Reputation:	low
Preview:	.....,..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsgAE9F.tmp	
Process:	C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
File Type:	data
Category:	dropped
Size (bytes):	315042
Entropy (8bit):	7.97484316079725
Encrypted:	false
SSDEEP:	6144:c3E/JlF7uLlUemo12UiBuF/3K6MCgCeSMZR/B1Rhmjs1v+9:T97ulmq2125MHCM1Z1v+9
MD5:	8B9B248ED4ADB4BA5259317DC9C0AC28
SHA1:	9AC1E37E65A9A2BD4F32BF4F89618BEAD8F9F9FB
SHA-256:	41891B82C216709BAE67DBF48537B87829C0F91EFEB192E4F27BD3FADD51F078
SHA-512:	91B76DC90EDB37D4D94AD517E2924AE94D5E0E3CE0378868D35C5335A00564B4ABFDE32EB6A2F1AEE4A90D528B6CB885244C6FE0B7D84BF697B0EFC5F97D4A 5C
Malicious:	false
Reputation:	low
Preview:	.....,..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsqAEDE.tmp\jupf00qz2dn.dll	
Process:	C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.13790327751178
Encrypted:	false
SSDEEP:	96:BHvn1ASk3NDZ+t20RKgIFln6Rul4jdkpN3:BWuuokajdkpN3
MD5:	AD0988E9810DB71DBBF62EB34162BAEB
SHA1:	78465D48ECBDCB107B6DC1937D823DBE3E789318
SHA-256:	2A344BC8389C27E68EF7BBEAAB1B98E580A9F42A1AD1EA6B2492D9635B7B5105
SHA-512:	EFC528BFB1A08A953437DF4FDB2A9365F76DF784C473A19D2749145A2D22C86035D59E09F9986B4162118F0D541044ACB6DAB2DF5197003CDA18EB8A1B9392F
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.}XX..XX..XX...0./]X....,.UX..XX..xX...1./YX...1./YX...1./YX ..RichXX.....PE..L....?.`.....!..... ..... .....@.....p!..P...".....  ..... ..@..... ..... .....text...1..... ..`.rdata..... .....@..@.data...T....0.....@..... ....

C:\Users\user\AppData\Local\Temp\nsu90B8.tmp\jupf00qz2dn.dll	
Process:	C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.13790327751178
Encrypted:	false
SSDEEP:	96:BHvn1ASk3NDZ+t20RKgIFln6Rul4jdkpN3:BWuuokajdkpN3
MD5:	AD0988E9810DB71DBBF62EB34162BAEB
SHA1:	78465D48ECBDCB107B6DC1937D823DBE3E789318
SHA-256:	2A344BC8389C27E68EF7BBEAAB1B98E580A9F42A1AD1EA6B2492D9635B7B5105
SHA-512:	EFC528BFB1A08A953437DF4FDB2A9365F76DF784C473A19D2749145A2D22C86035D59E09F9986B4162118F0D541044ACB6DAB2DF5197003CDA18EB8A1B9392F
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.}XX..XX..XX...0./]X....,.UX..XX..xX...1./YX...1./YX...1./YX ..RichXX.....PE..L....?.`.....!..... ..... .....@.....p!..P...".....  ..... ..@..... ..... .....text...1..... ..`.rdata..... .....@..@.data...T....0.....@..... ....

C:\Users\user\AppData\Local\Temp\nsz9088.tmp	
Process:	C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
File Type:	data
Category:	dropped
Size (bytes):	315042
Entropy (8bit):	7.97484316079725
Encrypted:	false
SSDEEP:	6144:c3E/JlF7uLlUemo12UiBuF/3K6MCgCeSMZR/B1Rhmjs1v+9:T97ulmq2125MHCM1Z1v+9
MD5:	8B9B248ED4ADB4BA5259317DC9C0AC28
SHA1:	9AC1E37E65A9A2BD4F32BF4F89618BEAD8F9F9FB
SHA-256:	41891B82C216709BAE67DBF48537B87829C0F91EFEB192E4F27BD3FADD51F078
SHA-512:	91B76DC90EDB37D4D94AD517E2924AE94D5E0E3CE0378868D35C5335A00564B4ABFDE32EB6A2F1AEE4A90D528B6CB885244C6FE0B7D84BF697B0EFC5F97D4A 5C
Malicious:	false
Reputation:	low
Preview:	.....,..... .....J.....j..... ....

C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe	
Process:	C:\Users\user\Desktop\1g1NLI6i33.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	348416
Entropy (8bit):	7.945327965170323

C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe	
Encrypted:	false
SSDEEP:	6144:lPXZLwfTl4lCmjw3FYlbB231/KtItPfiFtDMFTDb+AqTfu8cxFdMACKtee7o:TLwl4dw36lyKtBgFMfoFdM7tGo
MD5:	D0A8C2403C51EA96D820DCD443F1AAAB
SHA1:	825A057B9218A956A632BDD563056BE37BFC0C10
SHA-256:	0C397EBC470F59440B6A317A88A2592C0B05057CEA1FF2F31B9FDDE549971AEE
SHA-512:	FB7A0307327811FE7338ECF30AB539A50E9717DB60FF6E05FB06710E536EC9CF5EC560E97EEC2FAB19D37CE81725AD514EC7C1537DB52330DE1F3BE192D5CF3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG.....PE..L.....$_.....d.....a4.....@.....@.....8.....P.....text...<b.....d..... ..`.rdata..t.....h.....@..@.data...X.....|.....@....ndata.....P.....rsrc...P.....@..@.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.945327965170323
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	1g1NLI6i33.exe
File size:	348416
MD5:	d0a8c2403c51ea96d820dcd443f1aaab
SHA1:	825a057b9218a956a632bdd563056be37bfc0c10
SHA256:	0c397ebc470f59440b6a317a88a2592c0b05057cea1ff2f31b9fdde549971aee
SHA512:	fb7a0307327811fe7338ecf30ab539a50e9717db60ff6e05fb06710e536ec9cf5ec560e97eec2fab19d37ce81725ad514ec7c1537db52330de1f3be192d5cf93
SSDEEP:	6144:lPXZLwfTl4lCmjw3FYlbB231/KtItPfiFtDMFTDb+AqTfu8cxFdMACKtee7o:TLwl4dw36lyKtBgFMfoFdM7tGo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L.....$_.....d.....a4.....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403461
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D6E4 [Sat Aug 1 02:43:48 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General

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:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042474Ch], eax
je 00007F617C7F4073h
push ebx
call 00007F617C7F71EEh
cmp eax, ebx
je 00007F617C7F4069h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F617C7F716Ah
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F617C7F404Dh
push 0000000Bh
call 00007F617C7F71C2h
push 00000009h
call 00007F617C7F71BBh
push 00000007h
mov dword ptr [00424744h], eax
call 00007F617C7F71AFh
cmp eax, ebx
je 00007F617C7F4071h
push 0000001Eh
call eax
test eax, eax
je 00007F617C7F4069h
or byte ptr [0042474Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [00424818h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax

Instruction
push ebx
push 0041FD10h
call dword ptr [0040816Ch]
push 0040A1ECh

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8438	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0xa50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x623c	0x6400	False	0.65859375	data	6.40257705324	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1274	0x1400	False	0.43359375	data	5.05749598324	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1a858	0x600	False	0.445963541667	data	4.08975001509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0xa50	0xc00	False	0.402994791667	data	4.1909607241	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d190	0x2e8	data	English	United States
RT_DIALOG	0x2d478	0x100	data	English	United States
RT_DIALOG	0x2d578	0x11c	data	English	United States
RT_DIALOG	0x2d698	0x60	data	English	United States
RT_GROUP_ICON	0x2d6f8	0x14	data	English	United States
RT_MANIFEST	0x2d710	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked

DLL	Import
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 65

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:57:23.943017960 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:24.118796110 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:24.119035959 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:24.739242077 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:24.739717007 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:24.914073944 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:24.914148092 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:24.914699078 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:25.088911057 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:25.143258095 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:25.169491053 CEST	49768	587	192.168.2.4	208.91.199.224

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:57:25.346112013 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:25.346134901 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:25.346153021 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:25.346162081 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:25.346230030 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:25.346318007 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:25.393362999 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:25.520571947 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:25.526801109 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:25.705512047 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:25.752677917 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:25.999219894 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:26.173569918 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:26.175147057 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:26.350255013 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:26.351130962 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:26.529448986 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:26.530400038 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:26.706738949 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:26.707170010 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:26.909497976 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:26.909991026 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:27.084534883 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:27.086586952 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:27.086760044 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:27.087507010 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:27.087605953 CEST	49768	587	192.168.2.4	208.91.199.224
May 4, 2021 19:57:27.260847092 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:27.261662960 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:27.359024048 CEST	587	49768	208.91.199.224	192.168.2.4
May 4, 2021 19:57:27.409185886 CEST	49768	587	192.168.2.4	208.91.199.224

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:55:26.913604021 CEST	64646	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:26.943228960 CEST	65298	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:26.963429928 CEST	53	64646	8.8.8.8	192.168.2.4
May 4, 2021 19:55:27.013655901 CEST	53	65298	8.8.8.8	192.168.2.4
May 4, 2021 19:55:27.491365910 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:27.552699089 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 19:55:28.241489887 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:28.293410063 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 19:55:29.130726099 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:29.179327011 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 19:55:29.951500893 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:30.000222921 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 19:55:30.735666990 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:30.741790056 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:30.784621000 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 19:55:30.807570934 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 19:55:31.783792973 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:31.835938931 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 19:55:32.767976046 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:32.829715014 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 19:55:33.928160906 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:33.979639053 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 19:55:34.994802952 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:35.043512106 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 19:55:36.276734114 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:36.326893091 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 19:55:37.480227947 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:37.531861067 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 19:55:38.654270887 CEST	53700	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:55:38.704623938 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 19:55:40.048588991 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:40.101906061 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 19:55:41.202709913 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:41.254343033 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 19:55:42.251008987 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:42.299649954 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 19:55:43.192339897 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:43.257647038 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 19:55:44.145685911 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:44.194401979 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 19:55:45.558096886 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:45.606745958 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 19:55:46.928947926 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:46.977621078 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 19:55:48.076014996 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 19:55:48.133192062 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 19:56:01.690052032 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:01.738876104 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 19:56:05.289829969 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:05.354681969 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 19:56:22.198290110 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:22.233735085 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:22.341166019 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 19:56:22.390881062 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 19:56:22.933301926 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:22.992398977 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 19:56:23.656773090 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:23.714102983 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 19:56:23.835767031 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:23.911418915 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 19:56:24.262164116 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:24.324031115 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 19:56:25.081983089 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:25.252849102 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 19:56:27.394263029 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:27.452574968 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 19:56:27.947618008 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:28.005918980 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 19:56:29.586570024 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:29.643693924 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 19:56:31.440572023 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:31.499273062 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 19:56:31.976922035 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:32.037569046 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 19:56:36.665498972 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:36.714122057 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 19:56:36.896244049 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:36.961635113 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 19:56:39.427544117 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 19:56:39.478876114 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 19:57:11.753685951 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 19:57:11.802438974 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 19:57:13.887898922 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 19:57:13.962274075 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 19:57:23.750916004 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 19:57:23.814285994 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 19:57:40.648552895 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 19:57:40.711267948 CEST	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 19:57:23.750916004 CEST	192.168.2.4	8.8.8.8	0x8564	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
May 4, 2021 19:57:40.648552895 CEST	192.168.2.4	8.8.8.8	0x820c	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
May 4, 2021 19:57:23.814285994 CEST	8.8.8.8	192.168.2.4	0x8564	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 4, 2021 19:57:23.814285994 CEST	8.8.8.8	192.168.2.4	0x8564	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 4, 2021 19:57:23.814285994 CEST	8.8.8.8	192.168.2.4	0x8564	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
May 4, 2021 19:57:23.814285994 CEST	8.8.8.8	192.168.2.4	0x8564	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 4, 2021 19:57:40.711267948 CEST	8.8.8.8	192.168.2.4	0x820c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 4, 2021 19:57:40.711267948 CEST	8.8.8.8	192.168.2.4	0x820c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 4, 2021 19:57:40.711267948 CEST	8.8.8.8	192.168.2.4	0x820c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 4, 2021 19:57:40.711267948 CEST	8.8.8.8	192.168.2.4	0x820c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

SMTP Packets

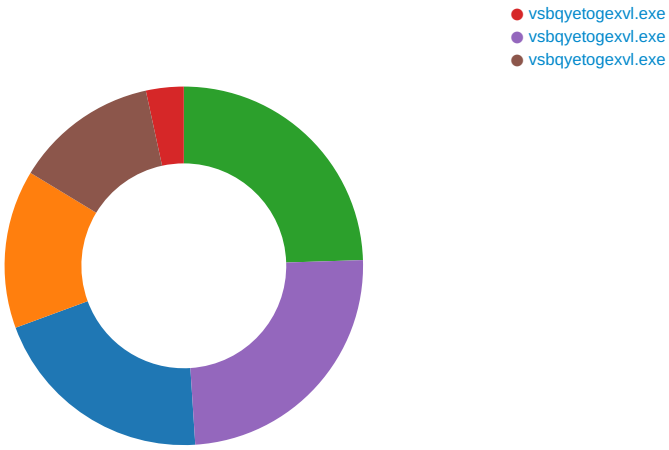
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 19:57:24.739242077 CEST	587	49768	208.91.199.224	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 4, 2021 19:57:24.739717007 CEST	49768	587	192.168.2.4	208.91.199.224	EHLO 226533
May 4, 2021 19:57:24.914148092 CEST	587	49768	208.91.199.224	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 4, 2021 19:57:24.914699078 CEST	49768	587	192.168.2.4	208.91.199.224	STARTTLS
May 4, 2021 19:57:25.088911057 CEST	587	49768	208.91.199.224	192.168.2.4	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior

- 1g1NLI6i33.exe
- 1g1NLI6i33.exe
- vsbqyetogexvl.exe



Click to jump to process

System Behavior

Analysis Process: 1g1NLI6i33.exe PID: 7020 Parent PID: 5896

General

Start time:	19:55:34
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\1g1NLI6i33.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\1g1NLI6i33.exe'
Imagebase:	0x400000
File size:	348416 bytes
MD5 hash:	D0A8C2403C51EA96D820DCD443F1AAAB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.654628131.00000000023D0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsg55C0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsg55C1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\161f8ahd30a3uiifxj4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\04v480yduj	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\nsb55F1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsb55F1.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40585E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsb55F1.tmp\jupf00qz2dn.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg55C0.tmp	success or wait	1	4036D8	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsb55F1.tmp	success or wait	1	405A1F	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg55C1.tmp	unknown	19542	8d 0c 00 00 a2 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 1c 00 00 00 d4 08 00 00 00 00 00 00 c7 0b 00 00 01 00 00 00 8d 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff 05 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 01 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........,.....................	success or wait	20	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\161f8ahd30a3uiifxj4	unknown	9221	2f ec 3b e7 e8 8c 9c e4 0d 1c 10 f9 1f 90 fb 13 1c f8 f2 dc 74 2c 06 00 7a c9 ca 29 20 fe de ad 12 f4 a8 98 c5 eb 39 96 db 34 f7 39 30 df c0 b6 24 42 d8 d7 24 0c c3 8b c3 ec ec ef f0 0e 26 f8 e4 70 b0 e9 70 9b 06 fe 88 05 85 61 a2 e3 65 9d 12 4f 99 1a 9a 74 80 e5 72 ab 30 c1 9e 13 93 75 cd cb 7f a5 28 44 97 18 98 74 f6 cd 78 bf 3e c8 ac 29 a9 4d 19 c7 4d 89 0a 51 ad 2e ae 48 11 d9 4a 87 08 f3 a2 27 a7 41 f8 cf 47 99 20 4a bb 3c bc 60 9f c1 60 ab 16 ca c0 3d bd 51 de db 55 ad 22 43 b1 32 b2 54 91 ed 52 bb 40 c5 b6 0b 8b 55 b0 e3 6f b5 38 60 8f 10 90 64 51 e5 68 8f 0e d4 84 01 81 6d 30 ef 6d 99 1a 75 85 06 86 68 fc e1 7a 97 18 e7 9a 1f 9f 71 32 e7 77 a9 30 7e 93 14 94 0e d2 80 3b a8 f5 18 98 15 74 03 ce 75 3d 8e f2 50 d0 c1 50 8b 06 49 43 c4 c8 48 0f a0 cf	/.;................t,..z..) . ...9..4.90...$B..$....... ..&..p..p......a..e..O...t..r. 0....u....(D...t..x.>..).M..M. .Q...H..J....'.A..G. J.<.`..`. ...=.Q..U."C.2.T..R.@....U.. o. 8`...dQ.h......m0.m..u...h..z. .....q2.w.0~......;.....t..u=. .P..P..IC..H...	success or wait	1	405E82	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\04v480yduj</td><td>unknown</td><td>16384</td><td>52 b9 bd 82 7c 88 15
3e be 15 56 c1 c0 65
50 e4 93 f5 23 89 3d
d4 e3 15 98 fd 48 48
b7 d8 ac 5a 4a 64 8e
b8 f3 c5 ed 74 94 31
1d 70 9c c2 bf 87 8c 39
69 10 21 ab e1 d1 56
cd 3f 58 f3 1d 9c 2e 8a
68 da 9d dc cf 9b 6a
1c 25 9a 56 37 ed b0
fe 24 76 3c 07 8b a9
c2 85 b2 fd 7c ed fe 57
f8 3f 7d 22 df 9d 26 cb
42 3b 70 96 04 ee d6
d2 db a8 54 bc 57 48
a0 7c 22 1d 7e 89 81
a6 cb eb 0a be b8 87
82 e8 b8 c5 aa 6f 61
9e d9 9d 39 15 13 e2
1a af db 04 64 80 78
0c 55 b6 d9 c0 88 fc
08 7a 53 e9 76 0d f9 df
38 44 f1 4e 76 75 bb
32 13 c8 e8 58 24 ab
50 4f 47 79 f2 9a 3c b8
e2 88 32 db 22 d7 08
08 0f 41 d2 d7 69 cf 13
0b bf 88 38 08 35 84
db 56 d8 0f d7 36 3d
cb 98 f6 ef 45 04 ff d9
6e 64 bf e5 c6 d6 fd 7e
56 ae 19 18 68 a8 9e
1f 97 10 a6 d3 30 3b
39 13 1c 21 0f c5 8f ee</td><td>R...|..>..V..eP...#.=.....HH..
.ZJd.....t.1.p.....9i.!...V.?X
.....h.....j.%.V7...$v<.......
|..W.?}"..&.B;p.......T.WH.|".
~..............oa...9.......d.
x.U......zS.v...8D.Nvu.2...X
$.POGy..
<...2."....A..i.....8.5.
.V...6=....E...nd.....~V...h..
.....0;9..!....</td><td>success or wait</td><td>19</td><td>405E82</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsb55F1.tmp\jupf00qz2dn.dll</td><td>unknown</td><td>5632</td><td>4d 5a 90 00 03 00 00
00 04 00 00 00 ff ff 00
00 b8 00 00 00 00 00
00 00 40 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 d0 00 00 00
0e 1f ba 0e 00 b4 09
cd 21 b8 01 4c cd 21
54 68 69 73 20 70 72
6f 67 72 61 6d 20 63
61 6e 6e 6f 74 20 62
65 20 72 75 6e 20 69
6e 20 44 4f 53 20 6d 6f
64 65 2e 0d 0d 0a 24
00 00 00 00 00 00 00
1c 39 89 7d 58 58 e7
2e 58 58 e7 2e 58 58
e7 2e 0a 30 e3 2f 5d
58 e7 2e 85 a7 2c 2e
55 58 e7 2e 58 58 e6
2e 78 58 e7 2e fd 31
e3 2f 59 58 e7 2e fd 31
e7 2f 59 58 e7 2e fd 31
e5 2f 59 58 e7 2e 52
69 63 68 58 58 e7 2e
00 00 00 00 00 00 00
00 50 45 00 00 4c 01
03 00 df 3f 91 60 00 00
00 00 00 00 00 00 e0
00 03 21 0b 01 0e 10
00 08 00 00 00 0c 00
00 00 00 00 00 00 00
00 00 00 10 00</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....
$........9.}XX..XX..XX...0./]X
....,.UX..XX..xX...1./YX...1./
YX...1./YX..RichXX..........P
E..L....?.`...........!........
...............</td><td>success or wait</td><td>1</td><td>405E82</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\1g1NLI6i33.exe	unknown	512	success or wait	83	405E53	ReadFile
C:\Users\user\Desktop\1g1NLI6i33.exe	unknown	16384	success or wait	20	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsg55C1.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsg55C1.tmp	unknown	3213	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nsg55C1.tmp	unknown	4	success or wait	3	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\161f8ahd30a3uiifxj4	unknown	9221	success or wait	1	1000128C	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: 1g1NLI6i33.exe PID: 7060 Parent PID: 7020

General

Start time:	19:55:35
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\1g1NLI6i33.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\1g1NLI6i33.exe'
Imagebase:	0x400000
File size:	348416 bytes
MD5 hash:	D0A8C2403C51EA96D820DCD443F1AAAB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.917550398.0000000004992000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.915437676.0000000003551000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.912048818.00000000004E9000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.914107097.00000000024F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.911491892.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.914206758.0000000002551000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1ACF06	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\1g1NLI6i33.exe	C:\Users\user\AppData\Local\Temp\tmpG607.tmp	success or wait	1	5A8C77A	MoveFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D185705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D18CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BFF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6BFF1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\6331c12b-e2b7-4266-9407-b2704ddb3ec4	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6BFF1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BFF1B4F	ReadFile

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

General

Start time:	19:55:48
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe'
Imagebase:	0x400000
File size:	348416 bytes
MD5 hash:	D0A8C2403C51EA96D820DCD443F1AAAB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.692221014.0000000003060000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 43%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsz9087.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsz9088.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsu90B8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsu90B8.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40585E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsu90B8.tmp\jupf00qz2dn.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz9087.tmp	success or wait	1	4036D8	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsu90B8.tmp	success or wait	1	405A1F	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz9088.tmp	unknown	19542	8d 0c 00 00 a2 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 1c 00 00 00 d4 08 00 00 00 00 00 00 c7 0b 00 00 01 00 00 00 8d 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff 05 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 01 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......,....................	success or wait	20	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\161f8ahd30a3uiifxj4	unknown	9221	2f ec 3b e7 e8 8c 9c e4 0d 1c 10 f9 1f 90 fb 13 1c f8 f2 dc 74 2c 06 00 7a c9 ca 29 20 fe de ad 12 f4 a8 98 c5 eb 39 96 db 34 f7 39 30 df c0 b6 24 42 d8 d7 24 0c c3 8b c3 ec ec ef f0 0e 26 f8 e4 70 b0 e9 70 9b 06 fe 88 05 85 61 a2 e3 65 9d 12 4f 99 1a 9a 74 80 e5 72 ab 30 c1 9e 13 93 75 cd cb 7f a5 28 44 97 18 98 74 f6 cd 78 bf 3e c8 ac 29 a9 4d 19 c7 4d 89 0a 51 ad 2e ae 48 11 d9 4a 87 08 f3 a2 27 a7 41 f8 cf 47 99 20 4a bb 3c bc 60 9f c1 60 ab 16 ca c0 3d bd 51 de db 55 ad 22 43 b1 32 b2 54 91 ed 52 bb 40 c5 b6 0b 8b 55 b0 e3 6f b5 38 60 8f 10 90 64 51 e5 68 8f 0e d4 84 01 81 6d 30 ef 6d 99 1a 75 85 06 86 68 fc e1 7a 97 18 e7 9a 1f 9f 71 32 e7 77 a9 30 7e 93 14 94 0e d2 80 3b a8 f5 18 98 15 74 03 ce 75 3d 8e f2 50 d0 c1 50 8b 06 49 43 c4 c8 48 0f a0 cf	/.;.................t,..z..) . ...9..4.90...$B..$....... ..&..p..p......a..e..O...t..r. 0....u....(D...t..x.>..).M..M. .Q...H..J....'.A..G. J.<.`..`. ...=.Q..U."C.2.T..R.@....U.. o. 8`...dQ.h......m0.m..u...h..z. .....q2.w.0~......;.....t..u=. .P..P..IC..H...	success or wait	1	405E82	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\04v480yduj</td><td>unknown</td><td>16384</td><td>52 b9 bd 82 7c 88 15 3e be 15 56 c1 c0 65 50 e4 93 f5 23 89 3d d4 e3 15 98 fd 48 48 b7 d8 ac 5a 4a 64 8e b8 f3 c5 ed 74 94 31 1d 70 9c c2 bf 87 8c 39 69 10 21 ab e1 d1 56 cd 3f 58 f3 1d 9c 2e 8a 68 da 9d dc cf 9b 6a 1c 25 9a 56 37 ed b0 fe 24 76 3c 07 8b a9 c2 85 b2 fd 7c ed fe 57 f8 3f 7d 22 df 9d 26 cb 42 3b 70 96 04 ee d6 d2 db a8 54 bc 57 48 a0 7c 22 1d 7e 89 81 a6 cb eb 0a be b8 87 82 e8 b8 c5 aa 6f 61 9e d9 9d 39 15 13 e2 1a af db 04 64 80 78 0c 55 b6 d9 c0 88 fc 08 7a 53 e9 76 0d f9 df 38 44 f1 4e 76 75 bb 32 13 c8 e8 58 24 ab 50 4f 47 79 f2 9a 3c b8 e2 88 32 db 22 d7 08 08 0f 41 d2 d7 69 cf 13 0b bf 88 38 08 35 84 db 56 d8 0f d7 36 3d cb 98 f6 ef 45 04 ff d9 6e 64 bf e5 c6 d6 fd 7e 56 ae 19 18 68 a8 9e 1f 97 10 a6 d3 30 3b 39 13 1c 21 0f c5 8f ee</td><td>R...|..>..V..eP...#.=.....HH.. .ZJd.....t.1.p.....9i.!...V.?X .....h.....j.%.V7...$v<....... |..W.?}"..&.B;p.......T.WH.|". ~..............oa...9.......d. x.U......zS.v...8D.Nvu.2...X $.POGy.. <...2."....A..i.....8.5. .V...6=....E...nd.....~V...h.. .....0;9..!....</td><td>success or wait</td><td>19</td><td>405E82</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsu90B8.tmp\jupf00qz2dn.dll</td><td>unknown</td><td>5632</td><td>4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1c 39 89 7d 58 58 e7 2e 58 58 e7 2e 58 58 e7 2e 0a 30 e3 2f 5d 58 e7 2e 85 a7 2c 2e 55 58 e7 2e 58 58 e6 2e 78 58 e7 2e fd 31 e3 2f 59 58 e7 2e fd 31 e7 2f 59 58 e7 2e fd 31 e5 2f 59 58 e7 2e 52 69 63 68 58 58 e7 2e 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 df 3f 91 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 10 00 08 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 10 00</td><td>MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........9.}XX..XX..XX...0./]X ....,.UX..XX..xX...1./YX...1./ YX...1./YX..RichXX..........P E..L....?.`..........!........ ....</td><td>success or wait</td><td>1</td><td>405E82</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe	unknown	512	success or wait	83	405E53	ReadFile
C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe	unknown	16384	success or wait	20	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsz9088.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsz9088.tmp	unknown	3213	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nsz9088.tmp	unknown	4	success or wait	3	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\161f8ahd30a3uiifxj4	unknown	9221	success or wait	1	1000128C	ReadFile
C:\Users\user\AppData\Local\Temp\04v480yduj	unknown	296960	success or wait	1	304177E	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3040867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3040867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3040867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3040867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3040867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3040867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3040867	ReadFile

Analysis Process: vsbqyetogexvl.exe PID: 900 Parent PID: 6712

General

Start time:	19:55:51
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe'
Imagebase:	0x400000
File size:	348416 bytes
MD5 hash:	D0A8C2403C51EA96D820DCD443F1AAAB
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: 00000007.00000002.703927470.00000000006CA000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.704176469.0000000002531000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.704176469.0000000002531000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.704217438.0000000003531000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.704708468.0000000004970000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000001.686936007.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.703482798.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.704751452.00000000049B2000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D185705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D18CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0E03DE	ReadFile

Analysis Process: vsbqyetogexvl.exe PID: 6956 Parent PID: 3424

General

Start time:	19:55:56
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe'
Imagebase:	0x400000
File size:	348416 bytes
MD5 hash:	D0A8C2403C51EA96D820DCD443F1AAAB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.703400223.0000000002430000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsgAE9E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsgAE9F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsqAEDE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsqAEDE.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40585E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsqAEDE.tmp\jupf00qz2dn.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsgAE9E.tmp	success or wait	1	4036D8	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsqAEDE.tmp	success or wait	1	405A1F	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsgAE9F.tmp	unknown	19542	8d 0c 00 00 a2 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 1c 00 00 00 d4 08 00 00 00 00 00 00 c7 0b 00 00 01 00 00 00 8d 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff 05 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 01 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......,.....................	success or wait	20	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\161f8ahd30a3uiifxj4	unknown	9221	2f ec 3b e7 e8 8c 9c e4 0d 1c 10 f9 1f 90 fb 13 1c f8 f2 dc 74 2c 06 00 7a c9 ca 29 20 fe de ad 12 f4 a8 98 c5 eb 39 96 db 34 f7 39 30 df c0 b6 24 42 d8 d7 24 0c c3 8b c3 ec ec ef f0 0e 26 f8 e4 70 b0 e9 70 9b 06 fe 88 05 85 61 a2 e3 65 9d 12 4f 99 1a 9a 74 80 e5 72 ab 30 c1 9e 13 93 75 cd cb 7f a5 28 44 97 18 98 74 f6 cd 78 bf 3e c8 ac 29 a9 4d 19 c7 4d 89 0a 51 ad 2e ae 48 11 d9 4a 87 08 f3 a2 27 a7 41 f8 cf 47 99 20 4a bb 3c bc 60 9f c1 60 ab 16 ca c0 3d bd 51 de db 55 ad 22 43 b1 32 b2 54 91 ed 52 bb 40 c5 b6 0b 8b 55 b0 e3 6f b5 38 60 8f 10 90 64 51 e5 68 8f 0e d4 84 01 81 6d 30 ef 6d 99 1a 75 85 06 86 68 fc e1 7a 97 18 e7 9a 1f 9f 71 32 e7 77 a9 30 7e 93 14 94 0e d2 80 3b a8 f5 18 98 15 74 03 ce 75 3d 8e f2 50 d0 c1 50 8b 06 49 43 c4 c8 48 0f a0 cf	/.;.....t,..z..) . ...9..4.90...$B..$..... ..&..p..p.....a..e..O...t..r. 0....u....(D...t..x.>..).M..M. .Q...H..J....'.A..G. J.<.`..`. ...=.Q..U."C.2.T..R.@....U.. o. 8`...dQ.h.....m0.m..u...h..z. .....q2.w.0~.....;.....t..u=. .P..P..IC..H...	success or wait	1	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\04v480yduj	unknown	16384	52 b9 bd 82 7c 88 15 3e be 15 56 c1 c0 65 50 e4 93 f5 23 89 3d d4 e3 15 98 fd 48 48 b7 d8 ac 5a 4a 64 8e b8 f3 c5 ed 74 94 31 1d 70 9c c2 bf 87 8c 39 69 10 21 ab e1 d1 56 cd 3f 58 f3 1d 9c 2e 8a 68 da 9d dc cf 9b 6a 1c 25 9a 56 37 ed b0 fe 24 76 3c 07 8b a9 c2 85 b2 fd 7c ed fe 57 f8 3f 7d 22 df 9d 26 cb 42 3b 70 96 04 ee d6 d2 db a8 54 bc 57 48 a0 7c 22 1d 7e 89 81 a6 cb eb 0a be b8 87 82 e8 b8 c5 aa 6f 61 9e d9 9d 39 15 13 e2 1a af db 04 64 80 78 0c 55 b6 d9 c0 88 fc 08 7a 53 e9 76 0d f9 df 38 44 f1 4e 76 75 bb 32 13 c8 e8 58 24 ab 50 4f 47 79 f2 9a 3c b8 e2 88 32 db 22 d7 08 08 0f 41 d2 d7 69 cf 13 0b bf 88 38 08 35 84 db 56 d8 0f d7 36 3d cb 98 f6 ef 45 04 ff d9 6e 64 bf e5 c6 d6 fd 7e 56 ae 19 18 68 a8 9e 1f 97 10 a6 d3 30 3b 39 13 1c 21 0f c5 8f ee	R...|..>..V..eP...#.=.....HH.. .ZJd.....t.1.p.....9i.!...V.?X .....h.....j.%.V7...$v<..... |..W.?}"..&.B;p.....T.WH.|". ~.....oa...9.....d. x.U.....zS.v...8D.Nvu.2...X $.POGy.. <...2."....A..i.....8.5. .V...6=....E...nd.....~V...h.. .....0;9..!....	success or wait	19	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsqAEDE.tmp\jupf00qz2dn.dll	unknown	5632	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1c 39 89 7d 58 58 e7 2e 58 58 e7 2e 58 58 e7 2e 0a 30 e3 2f 5d 58 e7 2e 85 a7 2c 2e 55 58 e7 2e 58 58 e6 2e 78 58 e7 2e fd 31 e3 2f 59 58 e7 2e fd 31 e7 2f 59 58 e7 2e fd 31 e5 2f 59 58 e7 2e 52 69 63 68 58 58 e7 2e 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 df 3f 91 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 10 00 08 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........9.}XX..XX..XX...0./]X ....,.UX..XX..xX...1./YX...1./ YX...1./YX..RichXX..........P E..L....?.`...........!........	success or wait	1	405E82	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe	unknown	512	success or wait	83	405E53	ReadFile
C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe	unknown	16384	success or wait	20	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsgAE9F.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsgAE9F.tmp	unknown	3213	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nsgAE9F.tmp	unknown	4	success or wait	3	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\161f8ahd30a3uiifxj4	unknown	9221	success or wait	1	1000128C	ReadFile
C:\Users\user\AppData\Local\Temp\04v480yduj	unknown	296960	success or wait	1	23D177E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D0867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D0867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D0867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D0867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D0867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D0867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D0867	ReadFile

Analysis Process: vsbqyetogexvl.exe PID: 6584 Parent PID: 6956

General

Start time:	19:55:58
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe'
Imagebase:	0x400000
File size:	348416 bytes
MD5 hash:	D0A8C2403C51EA96D820DCD443F1AAAB
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: 00000009.00000002.915225171.00000000034E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000001.699094253.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.913898804.00000000024E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.916955385.0000000004962000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.912144653.00000000005D9000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.916873369.0000000004920000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.911383328.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1ACF06	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wsvjsxxwtyqtn\vsbqyetogexvl.exe	C:\Users\user\AppData\Local\Temp\tmpG602.tmp	success or wait	1	5A8C77A	MoveFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D185705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D18CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BFF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6BFF1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\6331c12b-e2b7-4266-9407-b2704ddb3ec4	unknown	4096	success or wait	1	6BFF1B4F	ReadFile

Disassembly

Code Analysis