ID: 620525
Sample Name: 8v0aSYe34Q
Cookbook: default.jbs
Time: 21:08:13
Date: 04/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

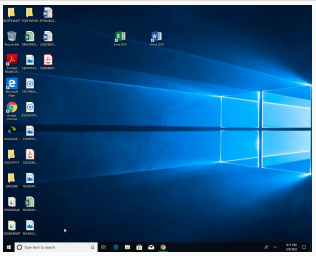
Windows Analysis Report

8v0aSYe34Q

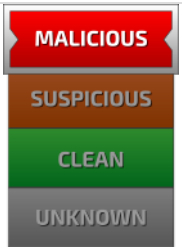
Overview

General Information

Sample Name:	8v0aSYe34Q (renamed file extension from none to exe)
Analysis ID:	620525
MD5:	859e6cf84ff73e9..
SHA1:	5bbc936fdb82ed..
SHA256:	cad1b58e38cfc1...
Tags:	32 exe trojan
Infos:	



Detection



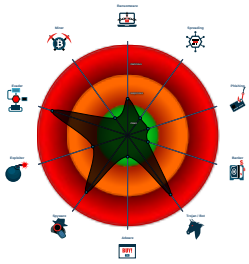
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Multi AV Scanner detection for subm...
- Detected unpacking (changes PE se...
- Snort IDS alert for network traffic
- Tries to steal Crypto Currency Walle...
- Tries to evade debugger and weak e...
- Machine Learning detection for sam...
- Queries sensitive video device infor...
- .NET source code contains method ...
- Queries sensitive disk information (v...
- Found many strings related to Crypt...

Classification



Process Tree

- **System is w10x64**
- 8v0aSYe34Q.exe (PID: 6260 cmdline: "C:\Users\user\Desktop\8v0aSYe34Q.exe" MD5: 859E6CF84FF73E9A9921FB829C3A386E)
- **cleanup**

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": "51.79.188.112:7110",
  "Bot Id": "KOL"
}
```

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.323258581.0000000003300000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: 8v0aSYe34Q.exe PID: 6260	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: 8v0aSYe34Q.exe PID: 6260	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.3 - Destination IP: 51.79.188.112

Timestamp:	05/04/22-21:09:50.022363 05/04/22-21:09:50.022363
SID:	2850286
Source Port:	49748
Destination Port:	7110
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.3 - Destination IP: 51.79.188.112

Timestamp:	05/04/22-21:09:31.442963 05/04/22-21:09:31.442963
SID:	2850286
Source Port:	49748
Destination Port:	7110
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 51.79.188.112 - Destination IP: 192.168.2.3

Timestamp:	05/04/22-21:09:31.611126 05/04/22-21:09:31.611126
SID:	2850353
Source Port:	7110
Destination Port:	49748
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.3 - Destination IP: 51.79.188.112

Timestamp:	05/04/22-21:09:28.360368 05/04/22-21:09:28.360368
SID:	2850027
Source Port:	49748
Destination Port:	7110
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.3 - Destination IP: 51.79.188.112

Timestamp:	05/04/22-21:09:40.013577 05/04/22-21:09:40.013577
SID:	2850286
Source Port:	49748
Destination Port:	7110
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Data Obfuscation

Detected unpacking (changes PE section rights)

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion

Tries to evade debugger and weak emulator (self modifying code)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Stealing of Sensitive Information

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Found many strings related to Crypto-Wallets (likely being stolen)

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

Remote Access Functionality

Yara detected RedLine Stealer

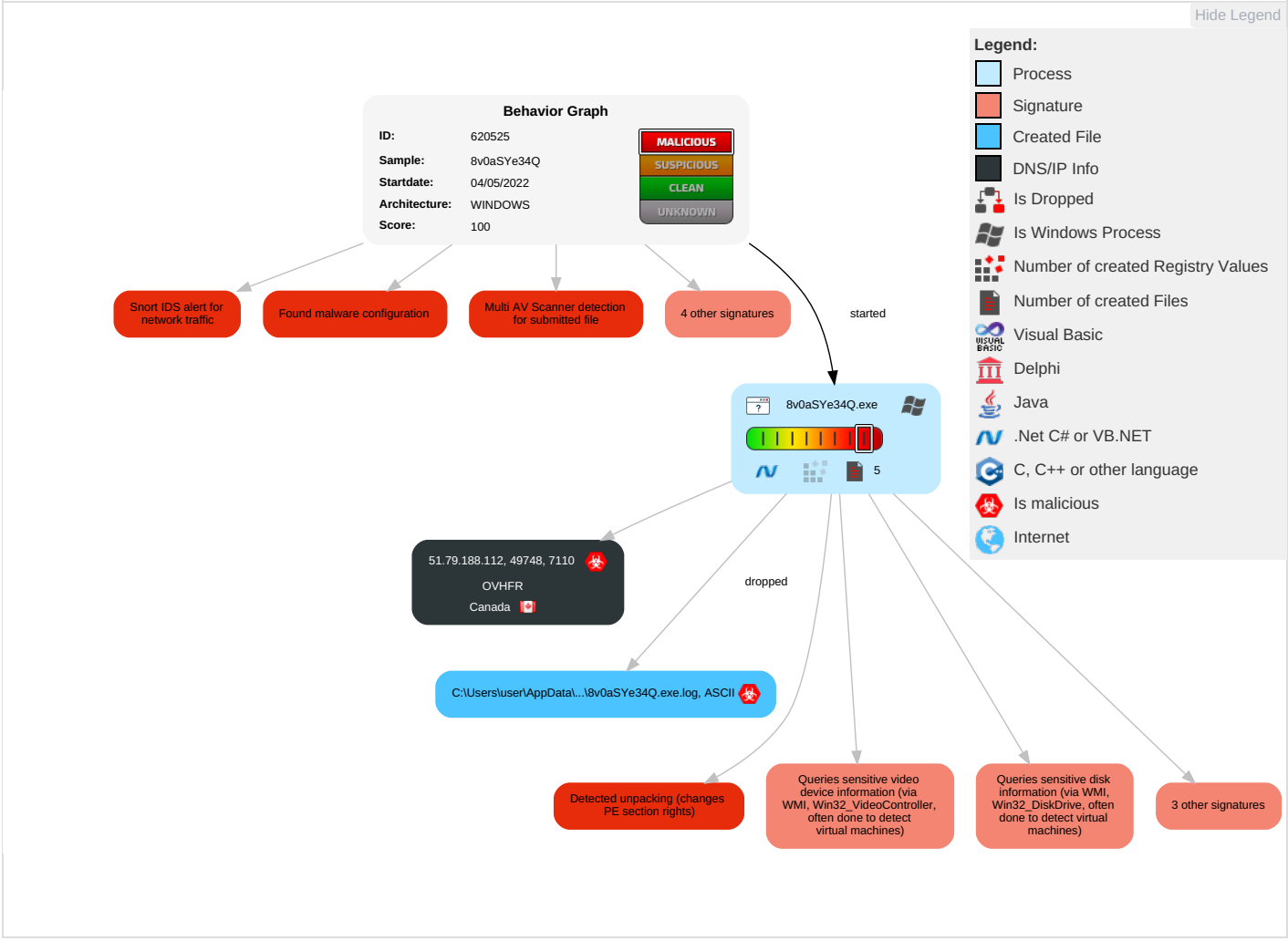
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 2 1 Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	1 OS Credential Dumping	3 3 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 1 Process Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 3 1 Virtualization/Sandbox Evasion	Security Account Manager	2 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Obfuscated Files or Information	LSA Secrets	2 3 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 3 Software Packing	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Timestomp	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

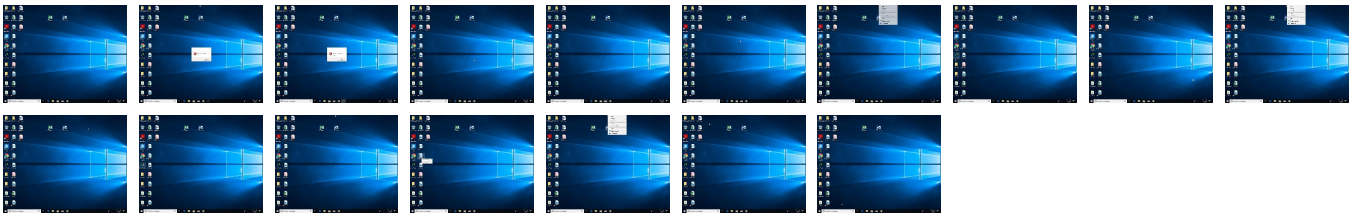
Behavior Graph



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
8v0aSYe34Q.exe	42%	Virustotal		Browse
8v0aSYe34Q.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.8v0aSYe34Q.exe.8f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.8v0aSYe34Q.exe.2a70000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2022

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	8v0aSYe34Q.exe, 00000000.00000002.326273315.00000000044CA000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.323963390.00000000034B0000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.324020976.00000000034C7000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.326129696.0000000004459000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.323759201.000000000348D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://service.r	8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	8v0aSYe34Q.exe, 00000000.00000002.326273315.00000000044CA000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.323963390.00000000034B0000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.324020976.00000000034C7000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.326129696.0000000004459000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.323759201.000000000348D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ns.adobe.c/g	8v0aSYe34Q.exe, 00000000.00000003.321186796.0000000007FE1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high

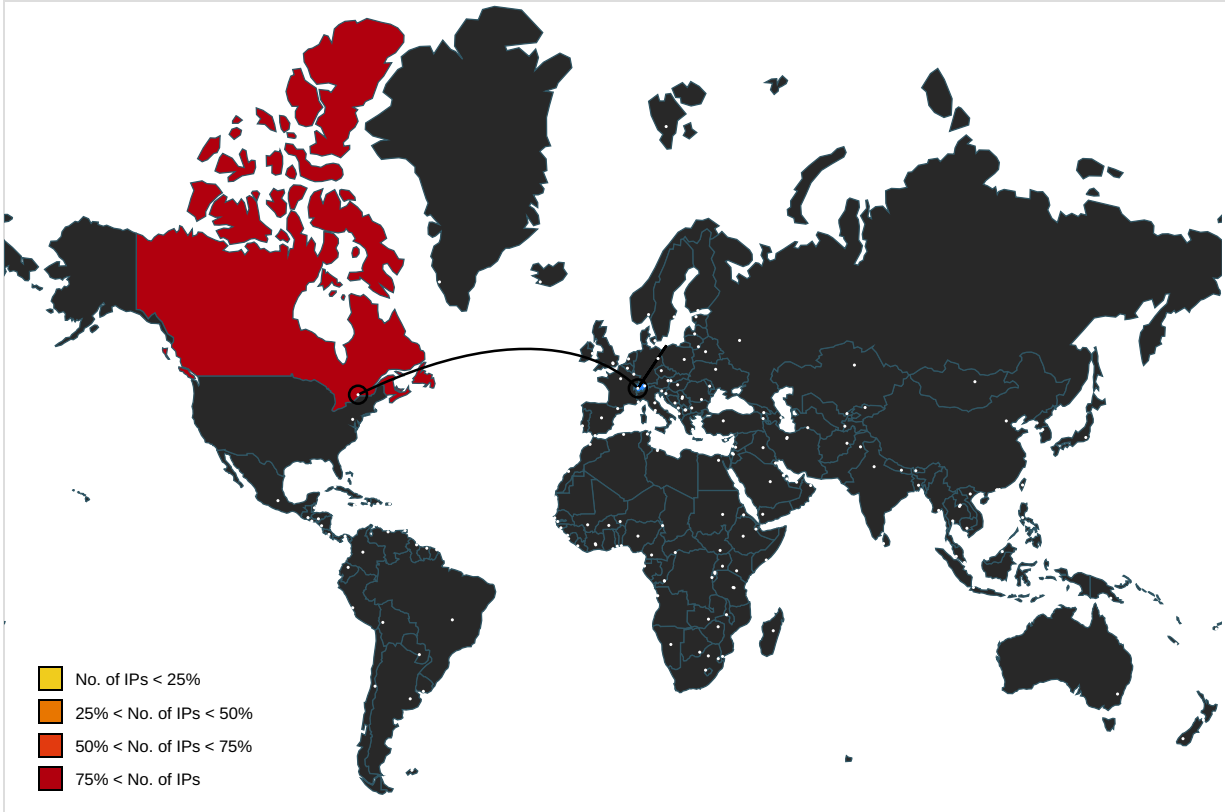
Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id4	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_real	8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_pdf	8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://forms.real.com/real/realone/download.html?type=rpsp_us	8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false		high
http://support.a	8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	8v0aSYe34Q.exe, 00000000.00000002.325424837.00000000036BD000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_quicktime	8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ns.adobe.cobj	8v0aSYe34Q.exe, 00000000.00000003.321186796.0000000007FE1000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000003.321205863.0000000007FF3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	8v0aSYe34Q.exe, 00000000.00000002.326273315.00000000044CA000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.323963390.00000000034B0000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.324020976.00000000034C7000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.326129696.0000000004459000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.323759201.000000000348D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id23	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id1Response	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_shockwave	8v0aSYe34Q.exe, 00000000.00000002.325424837.00000000036BD000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false		high
http://forms.rea	8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id5Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	8v0aSYe34Q.exe, 00000000.00000002.323045583.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.google.com/chrome/?p=plugin_wmp	8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/answer/6258784	8v0aSYe34Q.exe, 00000000.00000002.325424837.00000000036BD000.00000004.00000800.00020000.00000000.sdmp, 8v0aSYe34Q.exe, 00000000.00000002.324935951.0000000003633000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	8v0aSYe34Q.exe, 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Copyright Joe Security LLC 2022

Public IPs						
IP	**Domain**	**Country**	**Flag**	**ASN**	**ASN Name**	**Malicious**
51.79.188.112	unknown	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620525
Start date and time: 04/05/202221:08:13	2022-05-04 21:08:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8v0aSYe34Q (renamed file extension from none to 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:	25
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@1/1@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory 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
21:09:44	API Interceptor	43x Sleep call for process: 8v0aSYe34Q.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8v0aSYe34Q.exe.log

Process:	C:\Users\user\Desktop\8v0aSYe34Q.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2932
Entropy (8bit):	5.334469918014252
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIWUfHK7HKhBHKdHKB1AHKzvQTHmtHoxHImHKAHK1HQ:iqXeqm00YqhQnouOq7qLqdqUqzcGtlx1
MD5:	1A2F6CD1E6D92B812BD9E50C66E2388A
SHA1:	E510A412B93B0D48BB5AB666E1AA4DB4A8895C0B
SHA-256:	6C3E43210F51DD3BC1878E67EA7631D5B1DA1883037776EC5BC445E892F4E0B8
SHA-512:	1C24378C6635563DB5B5617DC42ED5F303DF456E0FCDD4F880B6FFA2B80AB4369549671300D5F9C2A089DCB1F485D408C50931CA9A72295FD7E57E44373D5DF
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.943516994761011
TrID:	• Win32 Executable (generic) a (10002005/4) 99.98% • DOS Executable Generic (2002/1) 0.02%
File name:	8v0aSYe34Q.exe
File size:	796304
MD5:	859e6cf84ff73e9a9921fb829c3a386e
SHA1:	5bbc936fdb82ed3e57c1ae2f4a0cbfab459883b7
SHA256:	cad1b58e38cfc1e0a0431fa9aae253a1626b4e4e3a6cbc6a8f119cd4959f6410
SHA512:	bae39f648487e4ac364152cf18061d28d834f11ea27027075ebc41508d0850fd5416b0fcfdfedbc66afc4c734bb969625046cb8f18523e437f49fb6edecc1a4c

Copyright Joe Security LLC 2022

SSDEEP:	24576:6QwJUPvfQ9Lu9lokWwq4uHopxqqYMEeq:6QwauQvWwq4wopVYME3
TLSH:	0305232635DBC53BE7906A384DADE6CADB24FD839C066B477390332CD572BA12E05781
File Content Preview:	MZ>.....M.=.A....CJR.2.c...P.....VC..#0.ph.!E....N.....Q..... .....

File Icon

Icon Hash:	30e0c4c45efc7038

Static PE Info

General

Entrypoint:	0x48e000
Entrypoint Section:	.idata
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xC25F582D [Wed May 3 09:13:17 2073 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	2d99dbf9a3c1158012345d1eb4ef7fac

Entrypoint Preview

Instruction
jmp 00007FC83CC2C246h
push 504B2040h
jmp 00007FC83CC2C243h
xor eax, ebp
sbb byte ptr [eax], al
add byte ptr [eax], al
jmp 00007FC83CC2C246h
sbb dword ptr [ecx+ebp*2-7CFE1466h], esi
xor eax, eax
jns 00007FC83CC2C245h
call far 04EBh : 6C719F46h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x37000	0x1dc	.itext
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x55a54	.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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
.didata	0x1000	0x36000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.itext	0x37000	0x1000	0x200	False	0.509765625	data	3.64540996605	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x55a54	0x55a54	False	0.801895075313	data	7.82839756911	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.idata	0x8e000	0x18000	0x175fd	False	0.999341974703	DOS executable (COM)	7.99680274273	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PKGDEF	0x38100	0x4edf	data	English	United States
PKGDEF	0x3d008	0x4f92	data	English	United States
PKGDEF	0x41fc4	0x4edf	data	English	United States
PNG	0x46ef8	0xe4a	data	English	United States
PNG	0x47d6c	0x166	data	English	United States
REGISTRY	0x47f30	0x2c	data	English	United States
REGISTRY	0x47f84	0xc5	data	English	United States
TEXTFILE	0x480c4	0x1152	data	English	United States
TYPELIB	0x4926c	0x23e4	data	English	United States
WEVT_TEMPLATE	0x4b6b0	0x129e	data	English	United States
RT_CURSOR	0x4ca68	0x134	data	English	United States
RT_CURSOR	0x4cbc4	0x134	data	English	United States
RT_CURSOR	0x4cd20	0x134	data	English	United States
RT_CURSOR	0x4ce7c	0x134	data	English	United States
RT_CURSOR	0x4cfd8	0x134	data	English	United States
RT_CURSOR	0x4d134	0x134	data	English	United States
RT_CURSOR	0x4d290	0xb4	data	English	United States
RT_CURSOR	0x4d36c	0x134	data	English	United States
RT_CURSOR	0x4d4c8	0xb4	data	English	United States
RT_CURSOR	0x4d5a4	0x134	data	English	United States
RT_CURSOR	0x4d700	0x2ec	data	English	United States
RT_CURSOR	0x4da14	0x2ec	data	English	United States
RT_CURSOR	0x4dd28	0x134	data	English	United States
RT_CURSOR	0x4de84	0x134	data	English	United States
RT_CURSOR	0x4dfe0	0x134	data	English	United States
RT_CURSOR	0x4e13c	0x134	data	English	United States
RT_CURSOR	0x4e298	0x134	data	English	United States
RT_CURSOR	0x4e3f4	0x134	data	English	United States
RT_CURSOR	0x4e550	0x134	data	English	United States
RT_CURSOR	0x4e6ac	0x134	data	English	United States
RT_CURSOR	0x4e808	0x134	data	English	United States
RT_CURSOR	0x4e964	0x134	data	English	United States
RT_CURSOR	0x4eac0	0x134	data	English	United States
RT_CURSOR	0x4ec1c	0x134	data	English	United States
RT_CURSOR	0x4ed78	0x134	data	English	United States
RT_CURSOR	0x4eed4	0x134	data	English	United States
RT_CURSOR	0x4f030	0x134	data	English	United States
RT_CURSOR	0x4f18c	0x134	data	English	United States

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x4f418	0x50	data	English	United States
RT_BITMAP	0x4f490	0x50	data	English	United States
RT_BITMAP	0x4f508	0x50	data	English	United States
RT_BITMAP	0x4f580	0x50	data	English	United States
RT_BITMAP	0x4f5f8	0x46	data	English	United States
RT_BITMAP	0x4f668	0x42	data	English	United States
RT_BITMAP	0x4f6d4	0x46	data	English	United States
RT_BITMAP	0x4f744	0x42	data	English	United States
RT_BITMAP	0x4f7b0	0xe8	data	English	United States
RT_BITMAP	0x4f8c0	0x168	data	English	United States
RT_BITMAP	0x4fa50	0xc0	data	English	United States
RT_BITMAP	0x4fb38	0xc0	data	English	United States
RT_BITMAP	0x4fc20	0x1228	data	English	United States
RT_BITMAP	0x50e70	0xc28	data	English	United States
RT_BITMAP	0x51ac0	0xc2a	data	English	United States
RT_BITMAP	0x52714	0x928	data	English	United States
RT_BITMAP	0x53064	0x32a	data	English	United States
RT_BITMAP	0x533b8	0x628	data	English	United States
RT_BITMAP	0x53a08	0xe8	data	English	United States
RT_BITMAP	0x53b18	0x32a	data	English	United States
RT_BITMAP	0x53e6c	0xe8	data	English	United States
RT_BITMAP	0x53f7c	0x32a	data	English	United States
RT_BITMAP	0x542d0	0xe8	data	English	United States
RT_BITMAP	0x543e0	0xe8	data	English	United States
RT_BITMAP	0x544f0	0x54	data	English	United States
RT_BITMAP	0x5456c	0x2c728	data	English	United States
RT_BITMAP	0x80cbc	0x228	data	English	United States
RT_BITMAP	0x80f0c	0x228	data	English	United States
RT_BITMAP	0x8115c	0x228	data	English	United States
RT_BITMAP	0x813ac	0x5c	data	English	United States
RT_BITMAP	0x81430	0x5c	data	English	United States
RT_BITMAP	0x814b4	0x328	data	English	United States
RT_BITMAP	0x81804	0x328	data	English	United States
RT_BITMAP	0x81b54	0x32a	data	English	United States
RT_BITMAP	0x81ea8	0x58	data	English	United States
RT_BITMAP	0x81f28	0xf28	data	English	United States
RT_ICON	0x82ea0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x870f0	0x4b8	data	English	United States
RT_ICON	0x875d0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_STRING	0x87ac0	0x1aa	data	English	United States
RT_STRING	0x87c94	0x214	data	English	United States
RT_STRING	0x87ed0	0x270	data	English	United States
RT_STRING	0x88168	0x216	data	English	United States
RT_STRING	0x883a8	0x282	data	English	United States
RT_STRING	0x88654	0x2b8	data	English	United States
RT_STRING	0x88934	0x236	data	English	United States
RT_STRING	0x88b94	0x296	data	English	United States
RT_STRING	0x88e54	0xa6	data	English	United States
RT_STRING	0x88f24	0x50	data	English	United States
RT_FONTDIR	0x88fc8	0x9b	data	English	United States
RT_FONT	0x890a4	0x377c	data	English	United States
RT_RCDATA	0x8c868	0x26c	data	English	United States
RT_RCDATA	0x8cafc	0x137	data		
RT_MESSAGETABLE	0x8cc74	0x24	data	English	United States
RT_GROUP_CURSOR	0x8cda0	0x14	data	English	United States
RT_GROUP_CURSOR	0x8cddc	0x14	data	English	United States
RT_GROUP_CURSOR	0x8ce18	0x14	data	English	United States
RT_GROUP_CURSOR	0x8ce54	0x14	data	English	United States

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0x8ce90	0x14	data	English	United States
RT_GROUP_CURSOR	0x8cecc	0x22	data	English	United States
RT_GROUP_CURSOR	0x8cf18	0x22	data	English	United States
RT_GROUP_CURSOR	0x8cf64	0x14	data	English	United States
RT_GROUP_CURSOR	0x8cfa0	0x14	data	English	United States
RT_GROUP_CURSOR	0x8cfdc	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d018	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d054	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d090	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d0cc	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d108	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d144	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d180	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d1bc	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d1f8	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d234	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d270	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d2ac	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d2e8	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d324	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d360	0x14	data	English	United States
RT_GROUP_CURSOR	0x8d39c	0x14	data	English	United States
RT_GROUP_ICON	0x8d400	0x14	data	English	United States
RT_GROUP_ICON	0x8d43c	0x14	data	English	United States
RT_GROUP_ICON	0x8d478	0x14	data	English	United States
RT_VERSION	0x8d4cc	0x3c8	data	English	United States
RT_MANIFEST	0x8d8d4	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
kernel32.dll	GetModuleHandleW
user32.dll	GetDlgItem
advapi32.dll	RegQueryValueA
shell32.dll	ShellAboutW
mscoree.dll	_CorExeMain
comctl32.dll	CreateStatusWindowA

Version Infos

Description	Data
LegalCopyright	Luxe USA Corporation. All rights reserved.
InternalName	LocalESPC
FileVersion	14.00.24325.1
CompanyName	Luxe USA Corp.
LegalTrademarks	Luxe is a registered trademark of USA Corporation.
ProductName	PREfast
ProductVersion	14.00.24325.1
FileDescription	PREfast LocalESPC analysis defect module
OriginalFilename	LocalESPC.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/22-21:09:50.022363 05/04/22-21:09:50.022363	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49748	7110	192.168.2.3	51.79.188.112
05/04/22-21:09:31.442963 05/04/22-21:09:31.442963	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49748	7110	192.168.2.3	51.79.188.112
05/04/22-21:09:31.611126 05/04/22-21:09:31.611126	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	7110	49748	51.79.188.112	192.168.2.3
05/04/22-21:09:28.360368 05/04/22-21:09:28.360368	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49748	7110	192.168.2.3	51.79.188.112
05/04/22-21:09:40.013577 05/04/22-21:09:40.013577	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49748	7110	192.168.2.3	51.79.188.112

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 21:09:27.983628035 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:28.151108027 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:28.151228905 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:28.360368013 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:28.529398918 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:28.654592991 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:31.442962885 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:31.611125946 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:31.654844999 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:40.013576984 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:40.183541059 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:40.183610916 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:40.183640957 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:40.183903933 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:40.287007093 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:47.554285049 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:47.722445965 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.722492933 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.722520113 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.722548008 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.722678900 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:47.722764969 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:47.722790956 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:47.890304089 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.890353918 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.890372992 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.890389919 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.890491009 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.890640974 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.890671015 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:47.890743971 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:47.890763044 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.890789986 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:47.890810013 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:47.890844107 CEST	49748	7110	192.168.2.3	51.79.188.112

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 21:09:47.891246080 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:47.894762039 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.058387995 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.058459997 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.058514118 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.058569908 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.058612108 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.058623075 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.058639050 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.058664083 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.058722019 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.058748960 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.058758020 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.058810949 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.058821917 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.058860064 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.058913946 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.059094906 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.059149027 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.059211969 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.059262037 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.059303999 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.059360027 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.059412003 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.059470892 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.059565067 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.059612989 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.059886932 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.062422037 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.062519073 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.226785898 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.226844072 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.226871014 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.227116108 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.227147102 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.227236986 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.227350950 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.227511883 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.227560043 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.227775097 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.227803946 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.227863073 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.228055954 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.228117943 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.228338957 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.228404999 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.228436947 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.228471041 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.228511095 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.228672981 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.228897095 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.228929043 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.228997946 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.229108095 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.229264975 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.229376078 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.229650974 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.229722023 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.229835033 CEST	7110	49748	51.79.188.112	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 21:09:48.230329037 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.230442047 CEST	49748	7110	192.168.2.3	51.79.188.112
May 4, 2022 21:09:48.396063089 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.396092892 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.396109104 CEST	7110	49748	51.79.188.112	192.168.2.3
May 4, 2022 21:09:48.396238089 CEST	7110	49748	51.79.188.112	192.168.2.3

Statistics

No statistics

System Behavior

Analysis Process: 8v0aSYe34Q.exe PID: 6260, Parent PID: 5572

General

Target ID:	0
Start time:	21:09:14
Start date:	04/05/2022
Path:	C:\Users\user\Desktop\8v0aSYe34Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\8v0aSYe34Q.exe"
Imagebase:	0x8f0000
File size:	796304 bytes
MD5 hash:	859E6CF84FF73E9A9921FB829C3A386E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.323167089.0000000003267000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.323258581.0000000003300000.00000004.00000800.00020000.00000000.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	6DEDCF06	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	6DEDCF06	unknown
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD2BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD2BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8v0aSYe34Q.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	987A5D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8v0aSYe34Q.exe.log	0	2932	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	9879CD	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\8v0aSYe34Q.exe	unknown	347795	success or wait	1	9887DA	ReadFile
C:\Users\user\Desktop\8v0aSYe34Q.exe	unknown	352768	success or wait	1	987A7D	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	987A1D	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	987A6D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	987A1D	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	987A0D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	987A1D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	987A1D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	9879FD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	987A0D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	987A3D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	987A2D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	987A5D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	9879FD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	987A4D	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	9879CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	987A4D	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	987A1D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	2	987A4D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	2	9879DD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	987A6D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	9879FD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Aspnet.config	unknown	4095	success or wait	1	987A1D	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Aspnet.config	unknown	8173	end of file	1	987A6D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	1	987A0D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	1	9879ED	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	987A1D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	2	9879DD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	9879FD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	1	987A4D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	1	9879DD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	987A6D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	4	987A6D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	9879CD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	2	987A1D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	987A3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	987A5D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	987A0D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	3	987A0D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	987A6D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	1	9879FD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	2	9879DD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	987A5D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	4	987A5D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	987A7D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	987A6D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	9879CD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	987A7D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	2	987A7D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	9879DD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	2	987A2D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	9879CD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	4	9879CD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	9879ED	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	2	987A3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	9879DD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	9879FD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	9879ED	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV.docx	unknown	4096	success or wait	1	987A2D	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV.docx	unknown	1022	end of file	1	987A7D	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV.docx	unknown	4096	end of file	1	987A0D	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.docx	unknown	4096	success or wait	1	987A0D	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.docx	unknown	1022	end of file	1	987A5D	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.docx	unknown	4096	end of file	1	9879ED	ReadFile
C:\Users\user\Documents\PIVFAGEAAV.docx	unknown	4096	success or wait	1	9879ED	ReadFile
C:\Users\user\Documents\PIVFAGEAAV.docx	unknown	1022	end of file	1	987A3D	ReadFile
C:\Users\user\Documents\PIVFAGEAAV.docx	unknown	4096	end of file	1	9879CD	ReadFile
C:\Users\user\Documents\SQSJKEBWDT.docx	unknown	4096	success or wait	1	9879CD	ReadFile
C:\Users\user\Documents\SQSJKEBWDT.docx	unknown	1022	end of file	1	987A1D	ReadFile

Disassembly

No disassembly