ID: 652391
Sample Name:
AHj20WexRe.exe
Cookbook: default.jbs
Time: 09:43:23
Date: 26/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report AHj20WexRe.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: RedLine 4
Yara Signatures 4
PCAP (Network Traffic) 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
System Summary 6
Malware Analysis System Evasion 6
Anti Debugging 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 18
Public IPs 18
General Information 18
Warnings 19
Simulations 19
Behavior and APIs 19
Joe Sandbox View / Context 19
IPs 19
Domains 19
ASNs 20
JA3 Fingerprints 20
Dropped Files 20
Created / dropped Files 20
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log 20
Static File Info 20
General 20
File Icon 21
Static PE Info 21
General 21
Entrypoint Preview 21
Data Directories 23
Sections 23
Imports 23
Network Behavior 23
Snort IDS Alerts 23
TCP Packets 24
Statistics 25
Behavior 26
System Behavior 26
Analysis Process: AHj20WexRe.exePID: 5964, Parent PID: 5116 26
General 26
File Activities 26
Analysis Process: conhost.exePID: 4220, Parent PID: 5964 26
General 26
Analysis Process: AppLaunch.exePID: 5308, Parent PID: 5964 27
General 27

File Activities 27
File Created 27
File Written 27
File Read 28
Disassembly 29

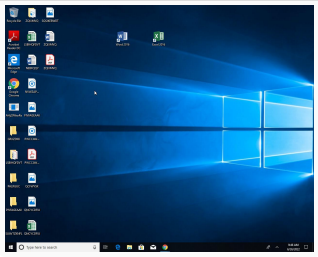
Windows Analysis Report

AHj20WexRe.exe

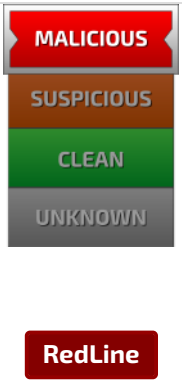
Overview

General Information

Sample Name:	AHj20WexRe.exe
Analysis ID:	652391
MD5:	feed21ebd82979..
SHA1:	b05191bad788b3.
SHA256:	7220cc97230b21..
Tags:	exe RedLineStealer
Infos:	



Detection



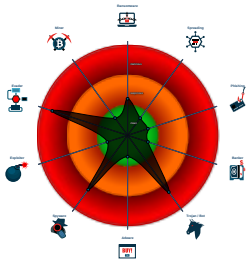
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Malicious sample detected (through…
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Tries to steal Crypto Currency Walle…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader
- Queries sensitive video device infor…
- Contains functionality to inject code…
- Queries sensitive disk information (v…

Classification



Process Tree

- **System is w10x64**
- AHj20WexRe.exe (PID: 5964 cmdline: "C:\Users\user\Desktop\AHj20WexRe.exe" MD5: FEED21EBD82979E5638211CA7B5F9F02)
  - conhost.exe (PID: 4220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AppLaunch.exe (PID: 5308 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "193.233.193.55:48403"
  ],
  "Bot Id": "166",
  "Authorization Header": "cb0f6806eb50e7a87e4ac51ebd57f0da"
}
```


Yara Signatures

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.265307308.0000000000EB2000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.342959659.0000000000402000.00000020.00000400.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.266075212.00000000010EC000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000000.265590293.0000000000402000.00000020.00000400.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000000.265268925.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.AppLaunch.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
2.0.AppLaunch.exe.400000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
2.0.AppLaunch.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x19c50:$pat14: , CommandLine: • 0x12cc1:$v2_1: ListOfProcesses • 0x12a81:$v4_3: base64str • 0x136c5:$v4_4: stringKey • 0x11233:$v4_5: BytesToStringConverted • 0x1032e:$v4_6: FromBase64 • 0x117a6:$v4_8: procName • 0x11abc:$v5_1: DownloadAndExecuteUpdate • 0x12958:$v5_2: ITaskProcessor • 0x11aaa:$v5_3: CommandLineUpdate • 0x11a9b:$v5_4: DownloadUpdate • 0x11e9f:$v5_5: FileScanning • 0x11454:$v5_7: RecordHeaderField • 0x110bc:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.3.AHj20WexRe.exe.eb0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.AHj20WexRe.exe.eb0000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
Click to see the 9 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 193.233.193.55 - Destination IP: 192.168.2.4

Timestamp:	193.233.193.55192.168.2.448403497582850353 06/26/22-09:44:57.292264
SID:	2850353
Source Port:	48403
Destination Port:	49758
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.4 - Destination IP: 193.233.193.55

Timestamp:	192.168.2.4193.233.193.5549758484032850286 06/26/22-09:45:16.984458
SID:	2850286
Source Port:	49758
Destination Port:	48403
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.4 - Destination IP: 193.233.193.55	
Timestamp:	192.168.2.4193.233.193.5549758484032850027 06/26/22-09:44:55.578726
SID:	2850027
Source Port:	49758
Destination Port:	48403
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

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)

Anti Debugging

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Stealing of Sensitive Information

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

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

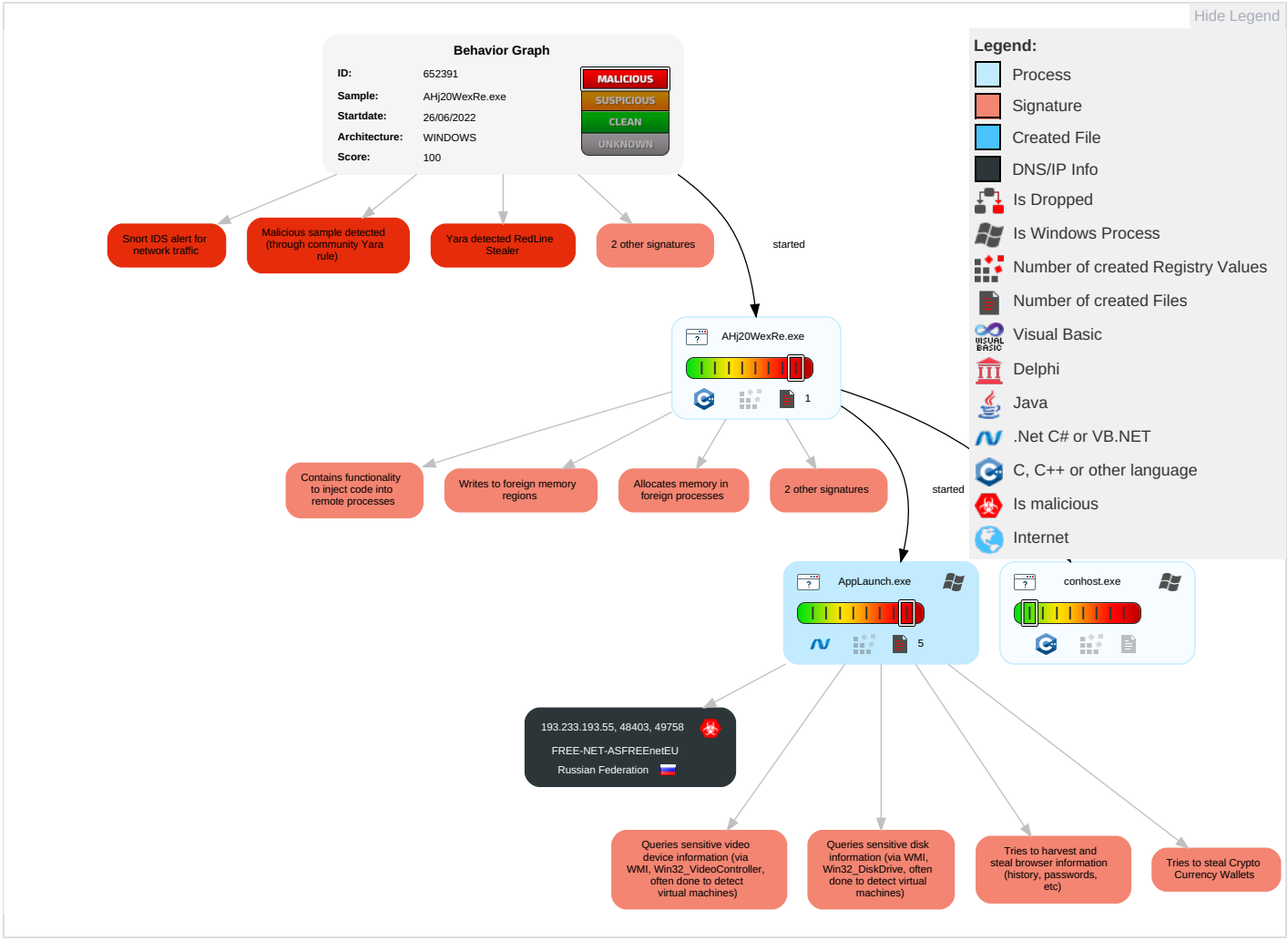
Remote Access Functionality

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	4 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	3 4 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	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	1 1 Process Discovery	SMB/Windows Admin Shares	2 Data from Local System	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)	4 1 1 Process Injection	NTDS	2 3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window 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 1 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory 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	Compile After Delivery	DCSync	1 3 5 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

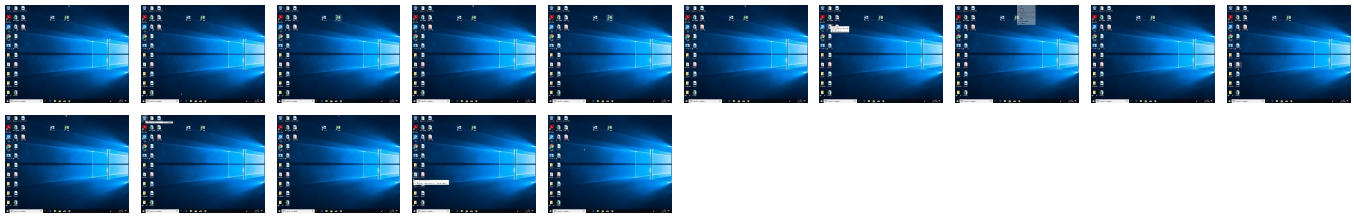
Behavior Graph



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
AHj20WexRe.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1234971		Download File
2.0.AppLaunch.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1234971		Download File
2.0.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1234971		Download File
0.3.AHj20WexRe.exe.eb0000.0.unpack	100%	Avira	HEUR/AGEN.1234971		Download File

Domains

No Antivirus matches

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://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://ns.ado/Ident	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://iptc.tc4xmp	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	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	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	AppLaunch.exe, 00000002.00000002.3448259 89.00000000072BF000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.347684515.00000000076E000 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.000 00000073BE000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000003.341095518.0000000008748000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.347991345 .00000000077A0000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.346163068.0000000007483000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.34865 7429.0000000008273000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000002.346963057.0000000007544 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.348898606.0 000000008329000.00000004.00000800.000200 00.00000000.sdmp, AppLaunch.exe, 0000000 2.00000002.345511061.000000000073A8000.00 000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.3460395 44.000000000746C000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.346852241.000000000752E00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.341005290.000 00000086D7000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.347919190.0000000007789000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.349554568 .0000000008665000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.348407129.0000000008202000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://service.r	AppLaunch.exe, 00000002.00000002.3448259 89.00000000072BF000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.347684515.00000000076E000 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.000 00000073BE000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.346163068.0000000007483000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.347453951 .0000000007623000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.347200620.00000000075AD000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/ac/?q=	AppLaunch.exe, 00000002.00000002.3448259 89.00000000072BF000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.347684515.00000000076E000 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.000 00000073BE000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000003.341095518.0000000008748000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.347991345 .00000000077A0000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.346163068.0000000007483000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.34865 7429.0000000008273000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000002.346963057.0000000007544 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.348898606.0 000000008329000.00000004.00000800.000200 00.00000000.sdmp, AppLaunch.exe, 0000000 2.00000002.345511061.00000000073A8000.00 000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.3460395 44.000000000746C000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.346852241.000000000752E00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.341005290.000 00000086D7000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.347919190.0000000007789000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.349554568 .0000000008665000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.348407129.0000000008202000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultL	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id5	AppLaunch.exe, 00000002.00000002.344385468.0000000007171000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4	AppLaunch.exe, 00000002.00000002.344385468.0000000007171000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	AppLaunch.exe, 00000002.00000002.344385468.0000000007171000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	AppLaunch.exe, 00000002.00000002.344385468.0000000007171000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_real	AppLaunch.exe, 00000002.00000002.344825989.00000000072BF000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347684515.00000000076E0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.00000000073BE000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346163068.0000000007483000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347453951.0000000007623000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347200620.00000000075AD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	AppLaunch.exe, 00000002.00000002.344385468.0000000007171000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	AppLaunch.exe, 00000002.00000002.344825989.00000000072BF000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347684515.00000000076E0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.00000000073BE000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346163068.0000000007483000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347453951.0000000007623000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347200620.00000000075AD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	AppLaunch.exe, 00000002.00000002.344385468.0000000007171000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ns.ado/Ident	AppLaunch.exe, 00000002.00000002.344360939.00000000058CC000.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.342734183.00000000058CC000.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.342701692.00000000058CB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome/?p=plugin_pdf	AppLaunch.exe, 00000002.00000002.344825989.00000000072BF000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347684515.00000000076E0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.00000000073BE000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346163068.0000000007483000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347453951.0000000007623000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	AppLaunch.exe, 00000002.00000002.344385468.0000000007171000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://forms.real.com/real/realone/download.html?type=rpsp_us	AppLaunch.exe, 00000002.00000002.344825989.00000000072BF000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347684515.00000000076E0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.00000000073BE000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346163068.0000000007483000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347453951.0000000007623000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347200620.00000000075AD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://support.a	AppLaunch.exe, 00000002.00000002.344825989.00000000072BF000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347684515.00000000076E0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.00000000073BE000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346163068.0000000007483000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347453951.0000000007623000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://iptc.tc4xmp	AppLaunch.exe, 00000002.00000002.344360939.00000000058CC000.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.342734183.00000000058CC000.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.342701692.00000000058CB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6Response	AppLaunch.exe, 00000002.00000002.344385468.0000000007171000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high

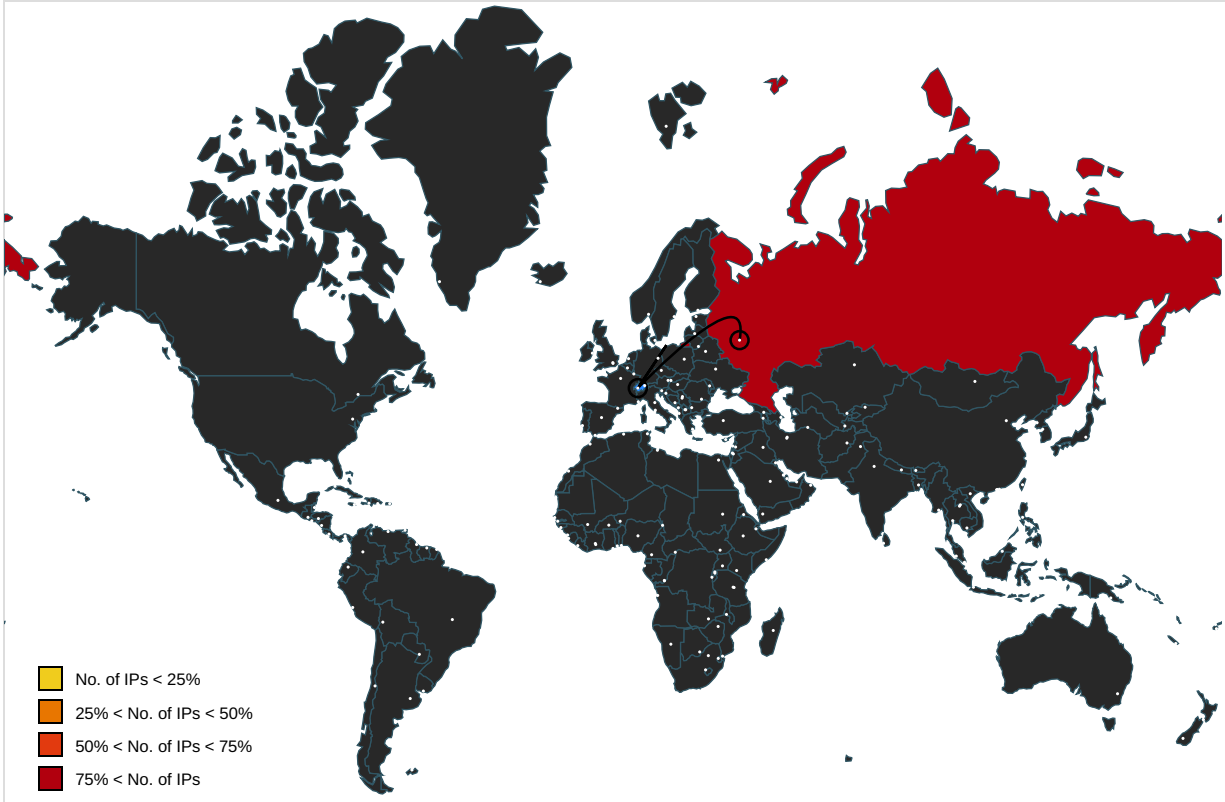
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ip.sb/ip	AHj20WexRe.exe, 00000000.00000002.266075212.00000000010EC000.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.342959659.0000000000402000.00000020.00000400.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000000.265268925.0000000000402000.00000040.00000400.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	AppLaunch.exe, 00000002.00000002.347453951.0000000007623000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_quicktime	AppLaunch.exe, 00000002.00000002.344825989.00000000072BF000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347684515.00000000076E000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.00000000073BE000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346163068.0000000007483000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347453951.0000000007623000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/sc	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	AppLaunch.exe, 00000002.00000002.344385468.0000000007171000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	AppLaunch.exe, 00000002.00000002.344825989.00000000072BF000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347684515.00000000076E000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.00000000073BE000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.341095518.0000000008748000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347991345.00000000077A0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346163068.0000000007483000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.348657429.0000000008273000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346963057.0000000007544000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.348898606.0000000008329000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345511061.00000000073A8000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346039544.000000000746C000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346852241.000000000752E000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.341005290.00000000086D7000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347919190.0000000007789000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.349554568.0000000008665000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.348407129.0000000008202000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	AppLaunch.exe, 00000002.00000002.344385468.0000000007171000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id21	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id23	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24Response	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id1Response	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_shockwave	AppLaunch.exe, 00000002.00000002.3474539 51.0000000007623000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://forms.rea	AppLaunch.exe, 00000002.00000002.3448259 89.00000000072BF000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.347684515.00000000076E000 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.000 00000073BE000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.346163068.0000000007483000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.347453951 .0000000007623000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.347200620.00000000075AD000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	AppLaunch.exe, 00000002.00000002.3445525 48.0000000007201000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	AppLaunch.exe, 00000002.00000002.3443854 68.0000000007171000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.344552548.000000000720100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome/?p=plugin_wmp	AppLaunch.exe, 00000002.00000002.344825989.00000000072BF000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347684515.00000000076E0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.345620761.00000000073BE000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.346163068.0000000007483000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347453951.0000000007623000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.347200620.00000000075AD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/answer/6258784	AppLaunch.exe, 00000002.00000002.347453951.0000000007623000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	AppLaunch.exe, 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.233.193.55	unknown	Russian Federation		2895	FREE-NET-ASFREEnetEU	true

General Information

Joe Sandbox Version:	35.0.0 Citrine

Analysis ID:	652391
Start date and time: 26/06/202209:43:23	2022-06-26 09:43:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AHj20WexRe.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:	27
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@4/1@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 97.4% (good quality ratio 90%) • Quality average: 76.9% • Quality standard deviation: 30.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • 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): www.bing.com, ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target AppLaunch.exe, PID 5308 because it is empty
- 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 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
09:45:15	API Interceptor	11x Sleep call for process: AppLaunch.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\AppLaunch.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2932
Entropy (8bit):	5.334469918014252
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIWUfHK7HKhBHKdHKB1AHKzvQTHmtHoxHImHK1HxLHW:iqXeqm00YqhQnouOq7qLqdqUqzcGtlxf
MD5:	92A61FC50E2FFFA916EF86C2F42C7557
SHA1:	145AD3EAEB578E9BBEE8F36DF312024BDA733602
SHA-256:	12D868AA2721F27C9353109BC11B79E28880B388AE22A0681EB337540DD1D798
SHA-512:	35A0CC24FD5D081CDD4065F118A6FA2EBA688D756EAC708AC5F85D21C2358D6DF815BC23399096507F5562AF882303AA361EB92EA0F98ECA6AE9356C34BC43B
Malicious:	false
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 (console) Intel 80386, for MS Windows
Entropy (8bit):	6.810014353516838
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:	AHj20WexRe.exe
File size:	237568
MD5:	feed21ebd82979e5638211ca7b5f9f02
SHA1:	b05191bad788b3cef9fd56c2da96846531b25856
SHA256:	7220cc97230b21abdcf6d7d01db4be1d85679828173f537349b87ed4a914f979
SHA512:	b8ee60c264335458c64d73cb77df3b8199159adc7734069fd02d61d6a2720da7b1ad6a2fe851e4ff96d60758adc11dfa402adcee0187665b3d36f33d6e64a119
SSDEEP:	6144:rIQe6Nq6jNux2lqlWdmXxdNi+ThB1bl7ELdY+bC9JIT:rs6Nq6j5lqGmXIul74too
TLSH:	2834AE6137DC98F1C775BA791C23B7A444BDF8704E11BAAB238B67BD0F660C28916817
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q...5..Z5..Z5..Z!..[?..Z!..[...Z!..['..ZW..[$..ZW..[#..Z!..[0..Z5..Z...ZW..[...Z...Z7..Z...[4..Z...[4..ZRich5..Z.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x406a9c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x62B7F96D [Sun Jun 26 06:15:09 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	01c7deffe7567fdea4e6658ade466fd3

Entrypoint Preview

Instruction
call 00007F32C4D7A4E8h
jmp 00007F32C4D79CA9h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ecx
lea ecx, dword ptr [esp+08h]
sub ecx, eax
and ecx, 0Fh
add eax, ecx
sbb ecx, ecx
or eax, ecx
pop ecx
jmp 00007F32C4D7A5DFh
push ecx
lea ecx, dword ptr [esp+08h]
sub ecx, eax
and ecx, 07h
add eax, ecx
sbb ecx, ecx
or eax, ecx
pop ecx
jmp 00007F32C4D7A5C9h
int3

Instruction
int3
int3
int3
push ebx
push esi
mov eax, dword ptr [esp+18h]
or eax, eax
jne 00007F32C4D79E4Ah
mov ecx, dword ptr [esp+14h]
mov eax, dword ptr [esp+10h]
xor edx, edx
div ecx
mov ebx, eax
mov eax, dword ptr [esp+0Ch]
div ecx
mov edx, ebx
jmp 00007F32C4D79E73h
mov ecx, eax
mov ebx, dword ptr [esp+14h]
mov edx, dword ptr [esp+10h]
mov eax, dword ptr [esp+0Ch]
shr ecx, 1
rcr ebx, 1
shr edx, 1
rcr eax, 1
or ecx, ecx
jne 00007F32C4D79E26h
div ebx
mov esi, eax
mul dword ptr [esp+18h]
mov ecx, eax
mov eax, dword ptr [esp+14h]
mul esi
add edx, ecx
jc 00007F32C4D79E40h
cmp edx, dword ptr [esp+10h]
jnbe 00007F32C4D79E3Ah
jc 00007F32C4D79E39h
cmp eax, dword ptr [esp+0Ch]
jbe 00007F32C4D79E33h
dec esi
xor edx, edx
mov eax, esi
pop esi
pop ebx
retn 0010h
int3
int3
int3
int3
int3
int3
int3
int3
push ebx
mov eax, dword ptr [esp+14h]
or eax, eax
jne 00007F32C4D79E4Ah
mov ecx, dword ptr [esp+10h]

Instruction
mov eax, dword ptr [esp+0Ch]
xor edx, edx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1c5c4	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3b000	0x1a14	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1a2b0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x1a300	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x1a1f0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x14000	0x170	.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	0x121de	0x12200	False	0.5988011853448276	data	6.603446862369813	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x14000	0x8e86	0x9000	False	0.3971354166666667	data	4.70611488497576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1d000	0x1db98	0x1ce00	False	0.5036356872294372	data	6.591282203310851	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x3b000	0x1a14	0x1c00	False	0.7007533482142857	data	6.340378099422768	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
USER32.dll	ShowWindow
KERNEL32.dll	CreateEventW, WriteConsoleW, IsDebuggerPresent, CheckRemoteDebuggerPresent, GetCurrentProcess, GetSystemInfo, GetConsoleWindow, RaiseException, InitializeSRWLock, ReleaseSRWLockExclusive, AcquireSRWLockExclusive, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, TryEnterCriticalSection, DeleteCriticalSection, GetCurrentThreadId, InitializeConditionVariable, WakeConditionVariable, WakeAllConditionVariable, SleepConditionVariableCS, SleepConditionVariableSRW, InitOnceBeginInitialize, InitOnceComplete, GetLastError, FreeLibraryWhenCallbackReturns, CreateThreadpoolWork, SubmitThreadpoolWork, CloseThreadpoolWork, GetModuleHandleExW, IsProcessorFeaturePresent, QueryPerformanceCounter, GetSystemTimeAsFileTime, GetModuleHandleW, GetProcAddress, CloseHandle, WaitForSingleObjectEx, CreateFileW, InitializeCriticalSectionAndSpinCount, SetEvent, ResetEvent, DecodePointer, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, TerminateProcess, GetCurrentProcessId, InitializeSListHead, RtlUnwind, SetLastError, EncodePointer, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, ExitProcess, GetModuleFileNameW, GetStdHandle, WriteFile, GetCommandLineA, GetCommandLineW, CompareStringW, LCMapStringW, HeapFree, HeapAlloc, GetFileType, SetFilePointerEx, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, GetProcessHeap, SetStdHandle, GetStringTypeW, FlushFileBuffers, GetConsoleOutputCP, GetConsoleMode, HeapSize, HeapReAlloc

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
193.233.193.55192.168.2.448403497582850353 06/26/22-09:44:57.292264	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	48403	49758	193.233.193.55	192.168.2.4
192.168.2.4193.233.193.549758484032850286 06/26/22-09:45:16.984458	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49758	48403	192.168.2.4	193.233.193.55
192.168.2.4193.233.193.549758484032850027 06/26/22-09:44:55.578726	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49758	48403	192.168.2.4	193.233.193.55

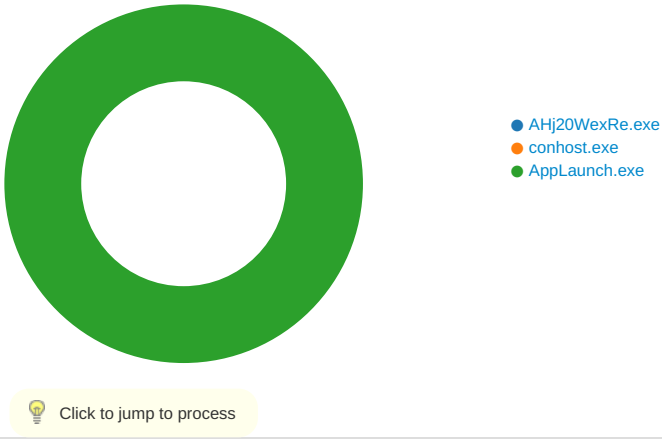
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:44:55.012095928 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:44:55.034389973 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:44:55.034513950 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:44:55.578726053 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:44:55.600933075 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:44:55.615884066 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:44:55.703222990 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:44:57.240299940 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:44:57.264451027 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:44:57.292263985 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:44:57.413984060 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:04.204436064 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:04.231043100 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:04.247549057 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:04.247607946 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:04.247648001 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:04.247771025 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:04.414612055 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:12.210522890 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:12.252036095 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:12.356772900 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.431720018 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.456154108 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.456183910 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.456196070 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.456305981 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.456343889 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.456680059 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.456696987 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.456787109 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.481261015 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.481300116 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.481314898 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.481326103 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.481338978 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.481349945 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.481363058 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.481390953 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.481482983 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.481514931 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.481535912 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.481794119 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.482584953 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.506062031 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.506165981 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.506258965 CEST	48403	49758	193.233.193.55	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:45:13.506277084 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.506294012 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.506355047 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.506361008 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.506385088 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.506417036 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.506423950 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.506428003 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.506439924 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.506498098 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.506515026 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.506761074 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.507008076 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.507035017 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.507080078 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.507091999 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.507117033 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.507363081 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.507410049 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.507572889 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.507586002 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.507661104 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.531019926 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531049013 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531060934 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531080961 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531095028 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531107903 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531121016 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531120062 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.531152010 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.531167984 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531181097 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531656027 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531683922 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531729937 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531740904 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531769991 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531783104 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531802893 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.531850100 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.532274961 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.532337904 CEST	49758	48403	192.168.2.4	193.233.193.55
Jun 26, 2022 09:45:13.532454014 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.532468081 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.532497883 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.532541037 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.532563925 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.532577991 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.534832954 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.534847021 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.534858942 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.534895897 CEST	48403	49758	193.233.193.55	192.168.2.4
Jun 26, 2022 09:45:13.534914970 CEST	48403	49758	193.233.193.55	192.168.2.4

Statistics

Behavior



System Behavior

Analysis Process: AHj20WexRe.exe PID: **5964**, Parent PID: **5116**

General

Target ID:	0
Start time:	09:44:36
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\AHj20WexRe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\AHj20WexRe.exe"
Imagebase:	0x800000
File size:	237568 bytes
MD5 hash:	FEED21EBD82979E5638211CA7B5F9F02
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.265307308.0000000000EB2000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.266075212.00000000010EC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4220**, Parent PID: **5964**

General

Target ID:	1
Start time:	09:44:39
Start date:	26/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AppLaunch.exe PID: **5308**, Parent PID: **5964**

General

Target ID:	2
Start time:	09:44:39
Start date:	26/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x1090000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
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: 00000002.00000002.342959659.0000000000402000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000000.265590293.0000000000402000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000000.265268925.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.344552548.0000000007201000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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	6DADCF06	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	6DADCF06	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	6C92BEFF	CreateDirectoryW
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	6C92BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDEC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.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	6DDEC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DABCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DABCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DABCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DAB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DAB5705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	22	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	6C921B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	3	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	51	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	3	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	28	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	3	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	57	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	3	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	47	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	3	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	66	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	3	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	54	6C921B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	3	6C921B4F	ReadFile

Disassembly

No disassembly