ID: 877006
Sample Name: Setup.exe
Cookbook: default.jbs
Time: 13:35:07
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

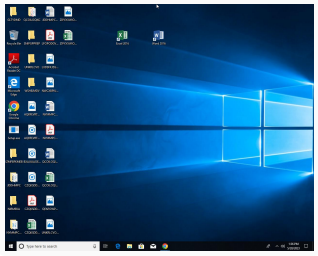
Windows Analysis Report

Setup.exe

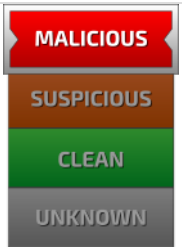
Overview

General Information

Sample Name:	Setup.exe
Analysis ID:	877006
MD5:	3694c18f01430..
SHA1:	25a1c807d62f2..
SHA256:	7fdba125f3d68...
Tags:	exe
Infos:	



Detection



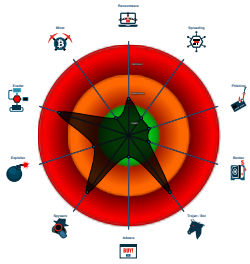
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom...
- 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...

Classification



Process Tree

- **System is w10x64**
- Setup.exe (PID: 6908 cmdline: C:\Users\user\Desktop\Setup.exe MD5: 3694C18F01430F213ACED163C75788A0)
  - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AppLaunch.exe (PID: 6868 cmdline: C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
RedLine Stealer	RedLine Stealer is a malware available on underground forums for sale apparently as standalone ($100/$150 depending on the version) or also on a subscription basis ($100/month). This malware harvests information from browsers such as saved credentials, autocomplete data, and credit card information. A system inventory is also taken when running on a target machine, to include details such as the username, location data, hardware configuration, and information regarding installed security software. More recent versions of RedLine added the ability to steal cryptocurrency. FTP and IM clients are also apparently targeted by this family, and this malware has the ability to upload and download files, execute commands, and periodically send back information about the infected computer.	No Attribution	**http://** https://asec.ahnlab.com/en/30445/https://asec.ahnlab.com/en/35981/https://asec.ahnlab.com/ko/25837/https://bartblaze.blogspot.com/2021/06/digital-artists-targeted-in-redline.htmlhttps://blog.avast.com/adobe-acrobat-sign-malware	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "94.142.138.4:80"
  ],
  "Bot Id": "@naralust2",
  "Message": "Click Close to exit the program. Error code: 1142",
  "Authorization Header": "684687f1439152a73e2a8b293ee8c64e"
}
```


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
00000000.00000003.351025860.0000000000562000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.408509605.00000000071A3000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000002.408509605.0000000007111000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.351304103.000000000042A000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.406792188.0000000000402000.00000020.00000400.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.Setup.exe.560000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
2.2.AppLaunch.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.Setup.exe.560000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1a08:$pat14: , CommandLine: • 0x19207:$v2_1: ListOfProcesses • 0x18fc4:$v4_3: base64str • 0x19c62:$v4_4: stringKey • 0x1760a:$v4_5: BytesToStringConverted • 0x165ad:$v4_6: FromBase64 • 0x17b28:$v4_8: procName
2.2.AppLaunch.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1a08:$pat14: , CommandLine: • 0x19207:$v2_1: ListOfProcesses • 0x18fc4:$v4_3: base64str • 0x19c62:$v4_4: stringKey • 0x1760a:$v4_5: BytesToStringConverted • 0x165ad:$v4_6: FromBase64 • 0x17b28:$v4_8: procName
0.2.Setup.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 94.142.138.4 - Destination IP: 192.168.2.3

Timestamp:	94.142.138.4192.168.2.380496982043234 05/28/23-13:36:08.316634
SID:	2043234
Source Port:	80
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.3 - Destination IP: 94.142.138.4	−
Timestamp:	192.168.2.394.142.138.449698802043231 05/28/23-13:36:15.171936
SID:	2043231
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.3 - Destination IP: 94.142.138.4	−
Timestamp:	192.168.2.394.142.138.449698802043233 05/28/23-13:36:07.137492
SID:	2043233
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Machine Learning detection for sample

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

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)

HIPS / PFW / Operating System Protection Evasion

- Writes to foreign memory regions
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes

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)

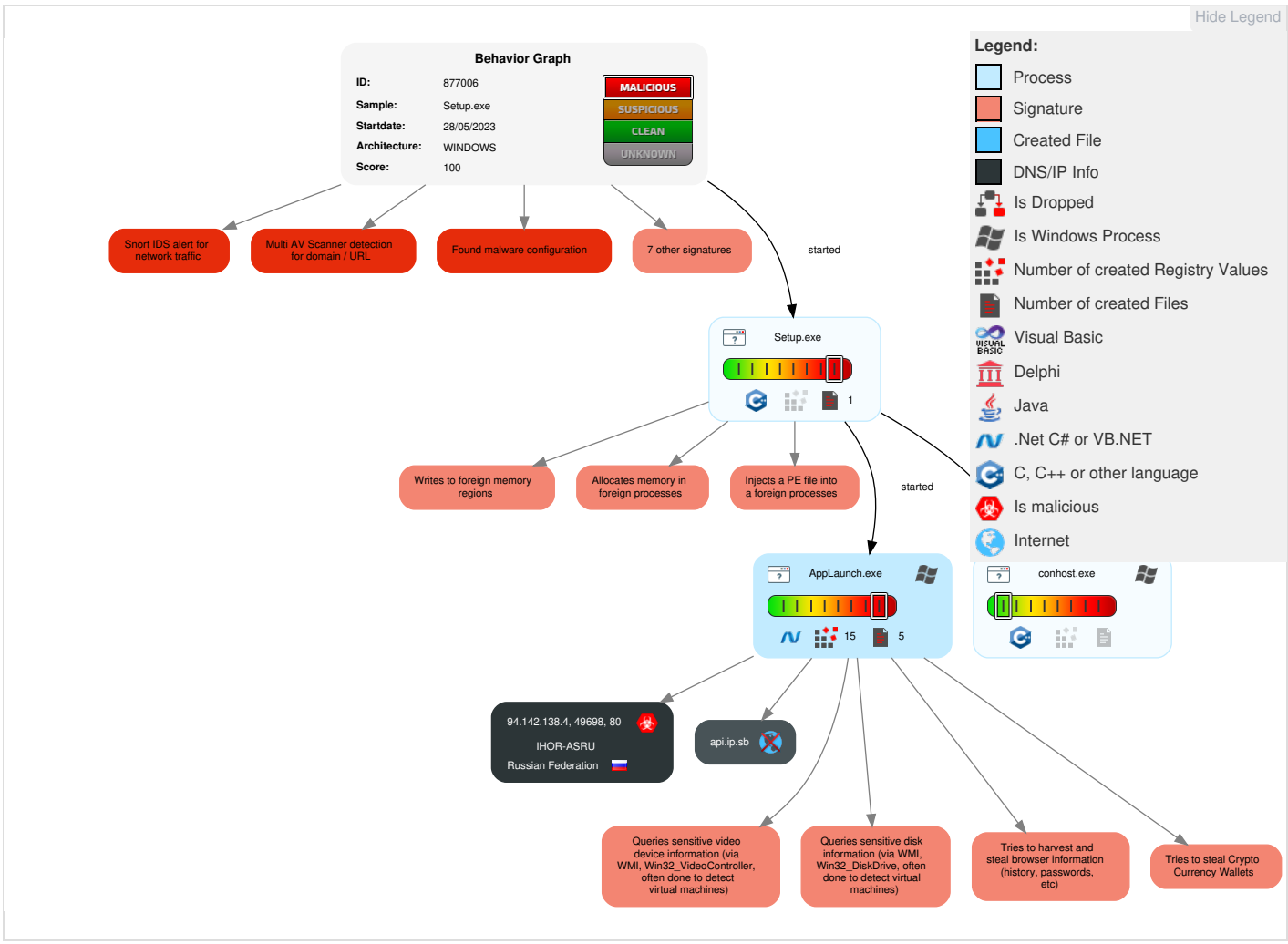
Remote Access Functionality

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	3 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	2 4 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	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 4 1 Virtualization/Sandbox Evasion	Security Account Manager	1 1 Process Discovery	SMB/Windows Admin Shares	3 Data from Local System	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 1 Process Injection	NTDS	2 4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	1 Clipboard Data	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	3 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System 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 4 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

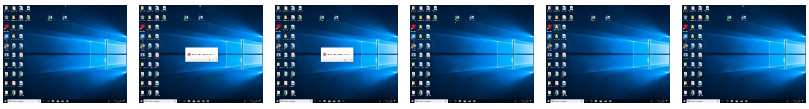
Behavior Graph



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
Setup.exe	45%	Virustotal		Browse
Setup.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
api.ip.sb	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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/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://tempuri.org/Entity/Id15Response	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/Id1Response	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	
http://tempuri.org/Entity/Id17Response	0%	URL Reputation	safe	
94.142.138.4:80	100%	Avira URL Cloud	malware	
94.142.138.4:80	18%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ip.sb	unknown	unknown	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
94.142.138.4:80	true	• 18%, Virustotal, Browse • Avira URL Cloud: malware	unknown

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, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	AppLaunch.exe, 00000002.00000002.412432062.0000000008BE1000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008BFE000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.408509605.0000000007502000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008D77000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008B63000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008DF5000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008D5A000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008DD8000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008C5F000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008CDD000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008B80000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008CFA000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.408509605.0000000007590000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0000000008C7C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	AppLaunch.exe, 00000002.00000002.408509605.00000000071A3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	AppLaunch.exe, 00000002.00000002.412432062.0000000008C7C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	AppLaunch.exe, 00000002.00000002.408509605.00000000071A3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	AppLaunch.exe, 00000002.00000002.408509605.0000000007111000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	AppLaunch.exe, 00000002.00000002.408509605.00000000071A3000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.408509605.000000000711000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	AppLaunch.exe, 00000002.00000002.408509605.00000000071A3000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.408509605.000000000711000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ns.adobe.c/g	AppLaunch.exe, 00000002.00000003.406634921.0000000014294000.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.406524312.0000000001428100.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.406581263.0000000014290000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	AppLaunch.exe, 00000002.00000002.408509605.00000000071A3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	AppLaunch.exe, 00000002.00000002.408509605.0000000007111000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	AppLaunch.exe, 00000002.00000002.408509605.00000000071A3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	AppLaunch.exe, 00000002.00000002.408509605.0000000007111000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	AppLaunch.exe, 00000002.00000002.408509605.00000000071A3000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id8	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultp	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.408509605.000000007111000 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high

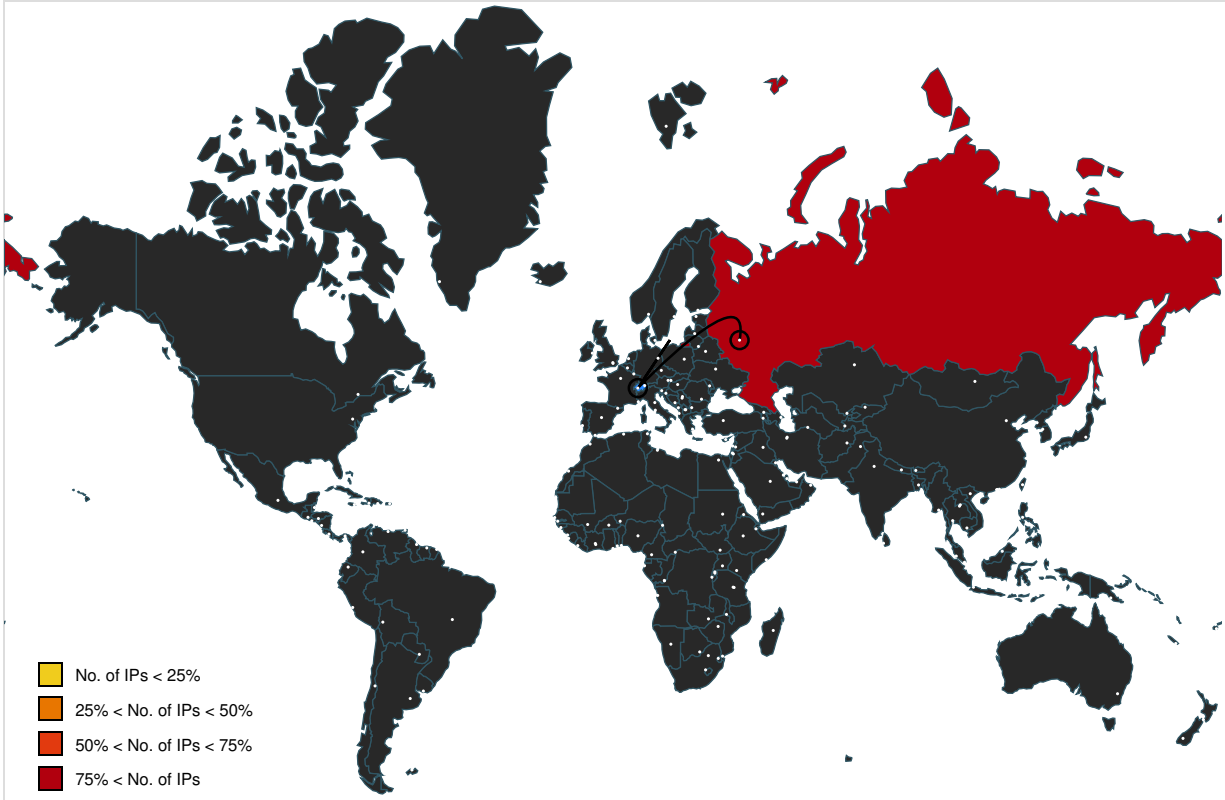
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	AppLaunch.exe, 00000002.00000002.4124320 62.0000000008C7C000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.408509605.000000007111000 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	AppLaunch.exe, 00000002.00000002.4124320 62.0000000008BE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.412432062.0000000008BFE00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.408509605.000 0000007502000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.412432062.0000000008D77000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.412432062 .0000000008B63000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.412432062.0000000008DF5000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.41243 2062.0000000008D5A000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000002.412432062.0000000008DD8 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0 000000008C5F000.00000004.00000800.000200 00.00000000.sdmp, AppLaunch.exe, 0000000 2.00000002.412432062.0000000008CDD000.00 000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.4124320 62.0000000008B80000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.412432062.0000000008CFA00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.408509605.000 0000007590000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.412432062.0000000008C7C000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	AppLaunch.exe, 00000002.00000002.4124320 62.0000000008BE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.412432062.0000000008BFE00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.408509605.000 0000007502000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.412432062.0000000008D77000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.412432062 .0000000008B63000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.412432062.0000000008DF5000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.41243 2062.0000000008D5A000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000002.412432062.0000000008DD8 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.412432062.0 000000008C5F000.00000004.00000800.000200 00.00000000.sdmp, AppLaunch.exe, 0000000 2.00000002.412432062.0000000008CDD000.00 000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.4124320 62.0000000008B80000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.412432062.0000000008CFA00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.408509605.000 0000007590000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.412432062.0000000008C7C000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequence Response	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	AppLaunch.exe, 00000002.00000002.4085096 05.00000000071A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17Response	AppLaunch.exe, 00000002.00000002.4085096 05.0000000007111000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.142.138.4	unknown	Russian Federation		35196	IHOR-ASRU	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877006
Start date and time:	2023-05-28 13:35:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
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
Sample file name:	Setup.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@4/1@2/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 99.5% (good quality ratio 97.4%) • Quality average: 82.9% • Quality standard deviation: 23.3%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 104.26.12.31, 172.67.75.172, 104.26.13.31
- Excluded domains from analysis (whitelisted): api.ip.sb.cdn.cloudflare.net
- Execution Graph export aborted for target AppLaunch.exe, PID 6868 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
13:36:17	API Interceptor	31x 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):	2843
Entropy (8bit):	5.3371553026862095
Encrypted:	false
SSDEEP:	48:MxHKXeHKIEHU0YHKhQnouHIWUfHKdHKBtBHK7HK5AHKzvQTHmtHoxHImHKoLHG1J:iqXeqm00YqhQnouOqdqxq7q2qzcGtlx+
MD5:	325E4B0634C6C9578C7D7D8197BD5BCA
SHA1:	1AD114002B0DDFF9C7C5175B0DA9E9FB40DD6BF0
SHA-256:	1B4A2571C8CD6A81820D851AF94A52502BEE6E4802EF4ADBF77F9F1E20F26601
SHA-512:	F03FC25705C318A8A26CD446B09A5FDD18EA8976854EECF26F7F02E9EF794C8A14711A556AA523DBC4FAFEA1377F1B46713554573C78A6471B490FE933751E52
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):	7.461973899099257
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:	Setup.exe
File size:	359160
MD5:	3694c18f01430f213aced163c75788a0
SHA1:	25a1c807d62f211e6adb38ed07e96e6bd309f8b8
SHA256:	7fdba125f3d682ea8b84cdc805f574789ebc8aecca3c5e20d20c8a8cd22e2bdb
SHA512:	9f718f0ef0bb7c8d4e779a8e94ebf84600ccfb0896dc9e33718f4ef09a40434b4f98cde43dfa53781b40654209fcd9fcc4290b5bec58024a366d84f43ce478b2
SSDEEP:	6144:yBmM2uzmMmVvV2KtLMMeWj286qoOEStQZ4lol3+uOD:KlzmRRYKtLMMx96NOESlK4zD
TLSH:	0374E1113248C13AF4AB347189E9DA79A6B9B5701B6F60DBFBC41A6D4F313D17A3021B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....J)...Hk..Hk..Hk.....Hk.....6Hk.....Hk.)....Hk..G6..Hk..Hj..Hk..0...Hk.....Hk..0...Hk.Rich.Hk.....PE..L..

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x4070ab
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE

DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x64726F2F [Sat May 27 20:59:27 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	ccf3d145fef27c23a1356d2673054011

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=Microsoft Code Signing PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 5/12/2022 1:45:59 PM 5/11/2023 1:45:59 PM
Subject Chain	• CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Version:	3
Thumbprint MD5:	EAF99B1CDFF361CB066EC1CDB5FD68ED
Thumbprint SHA-1:	F372C27F6E052A6BE8BAB3112B465C692196CD6F
Thumbprint SHA-256:	6DFB94C073BA075667FCC19AB327AE679D84F2A2BCF76CC21ABFC9B93FEE61A5
Serial:	33000002CBB77539FB027142360000000002CB

Entrypoint Preview
Instruction
call 00007FA65C6433A0h
jmp 00007FA65C63BA99h
cmp ecx, dword ptr [00454B30h]
jne 00007FA65C63BBF4h
rep ret
jmp 00007FA65C643422h
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [00454B30h]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [00454B30h]

Instruction
xor eax, ebp
push eax
mov dword ptr [ebp-10h], esp
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [00454B30h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
mov ecx, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C++] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 SP1 build 30729 • [RES] VS2008 build 21022 • [LNK] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x28aec	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x58000	0x610	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x54c00	0x2ef8	.data
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	0x27280	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x24000	0x220	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16d0f	0x16e00	False	0.5724363900273224	data	6.631366328323876	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.ueXxN	0x18000	0xbc1a	0xbe00	False	0.4510896381578947	data	6.220063968239562	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x24000	0x56ae	0x5800	False	0.37113813920454547	data	5.257116704784325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2a000	0x2db48	0x2bc00	False	0.9570368303571428	data	7.824578655735343	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x58000	0x610	0x800	False	0.33251953125	data	3.3303604724010856	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x58200	0x410	data	English	United States
RT_MANIFEST	0x580a0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetLocaleInfoW, SetStdHandle, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, LoadLibraryA, InitializeCriticalSectionAndSpinCount, GetStringTypeW, GetStringTypeA, IsValidLocale, EnumSystemLocalesA, GetLocaleInfoA, GetUserDefaultLCID, IsValidCodePage, GetOEMCP, GetACP, HeapSize, CloseHandle, CreateFileA, ReadFile, FlushFileBuffers, GetConsoleMode, GetConsoleCP, GetSystemTimeAsFileTime, GetCurrentProcessId, GetTickCount, QueryPerformanceCounter, GetStartupInfoA, GetFileType, SetHandleCount, FreeEnvironmentStringsW, GetEnvironmentStrings, FreeEnvironmentStringsA, GetModuleFileNameA, GetStdHandle, WriteFile, ExitProcess, HeapReAlloc, VirtualAlloc, VirtualFree, HeapCreate, GetEnvironmentStringsW, MultiByteToWideChar, GetModuleHandleA, SetFilePointer, GetProcAddress, InterlockedIncrement, InterlockedDecrement, WideCharToMultiByte, Sleep, InterlockedExchange, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RaiseException, GetLastError, HeapFree, GetCommandLineA, LCMapStringA, LCMapStringW, GetCPInfo, GetModuleHandleW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, HeapAlloc
USER32.dll	GetWindowRect, IsMenu, GetSubMenu, SetDlgItemInt, GetWindowPlacement, CharLowerBuffA, EnableMenuItem, CheckMenuRadioItem, GetSysColor, KillTimer, DestroyIcon, DestroyWindow, PostQuitMessage, GetClientRect, MoveWindow, GetSystemMenu, SetTimer, SetWindowPlacement, InsertMenuItemA, GetMenu, CheckMenuItem, SetMenuItemInfoA, SetActiveWindow, DefDlgProcA, RegisterClassA, EndDialog, SetDlgItemTextA, EnumClipboardFormats, GetClipboardData, CloseClipboard, GetClassInfoA, CallWindowProcA, SetWindowLongA, IsDlgButtonChecked, SetWindowTextA, CheckDlgButton, GetActiveWindow, LoadCursorA, MessageBoxA, wsprintfA, GetDlgItemTextA, SendMessageA, GetCursorPos, TrackPopupMenu, ClientToScreen, DestroyMenu, CreatePopupMenu, AppendMenuA, SendDlgItemMessageA, GetDlgItem
GDI32.dll	GetStockObject, DeleteObject, SetBkMode, SetTextColor, CreateFontIndirectA, SelectObject, GetObjectA

Possible Origin

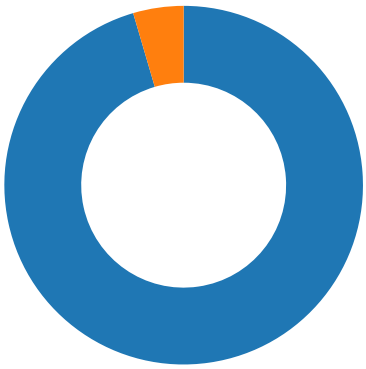
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
94.142.138.4192.168.2.380496982043234 05/28/23-13:36:08.316634	TCP	2043234	ET MALWARE Redline Stealer TCP CnC - Id1Response	80	49698	94.142.138.4	192.168.2.3
192.168.2.394.142.138.449698802043231 05/28/23-13:36:15.171936	TCP	2043231	ET TROJAN Redline Stealer TCP CnC Activity	49698	80	192.168.2.3	94.142.138.4
192.168.2.394.142.138.449698802043233 05/28/23-13:36:07.137492	TCP	2043233	ET TROJAN RedLine Stealer TCP CnC net.tcp Init	49698	80	192.168.2.3	94.142.138.4

Network Port Distribution



Total Packets: 44

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 13:36:06.782174110 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:06.820288897 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:06.820545912 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:07.137491941 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:07.175606966 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:07.215883970 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:07.269748926 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:08.237550020 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:08.275533915 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:08.316633940 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:08.363522053 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:15.171936035 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:15.209758043 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:15.252471924 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:15.252507925 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:15.252528906 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:15.252549887 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:15.252639055 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:15.252701044 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.073013067 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.111099005 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.111161947 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.111196041 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.111231089 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.111263037 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.111293077 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.111295938 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.111293077 CEST	49698	80	192.168.2.3	94.142.138.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 13:36:21.111293077 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.111330032 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.111392021 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.111392021 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.111392021 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.111430883 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.149200916 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149267912 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149301052 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149369955 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.149369955 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.149369955 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.149606943 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149641037 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149674892 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149705887 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149736881 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149749041 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.149770021 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149802923 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149826050 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.149826050 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.149895906 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.149897099 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.149897099 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.149976969 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.187588930 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.187645912 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.187684059 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.187716007 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.187748909 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.187815905 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.187815905 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.187815905 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.187941074 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.188739061 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.188774109 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.188807011 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.188839912 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.188967943 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.189002037 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.189174891 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.225701094 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.225815058 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.226106882 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.226140976 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.226428986 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264386892 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264441013 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264473915 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264486074 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264508009 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264542103 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264542103 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264548063 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264580965 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264580965 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264609098 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264614105 CEST	80	49698	94.142.138.4	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 13:36:21.264633894 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264647961 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264663935 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264683962 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264713049 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264772892 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264812946 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264846087 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264877081 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264882088 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264909029 CEST	80	49698	94.142.138.4	192.168.2.3
May 28, 2023 13:36:21.264923096 CEST	49698	80	192.168.2.3	94.142.138.4
May 28, 2023 13:36:21.264923096 CEST	49698	80	192.168.2.3	94.142.138.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 13:36:16.433954000 CEST	56924	53	192.168.2.3	8.8.8.8
May 28, 2023 13:36:16.476177931 CEST	60625	53	192.168.2.3	8.8.8.8

DNS Queries

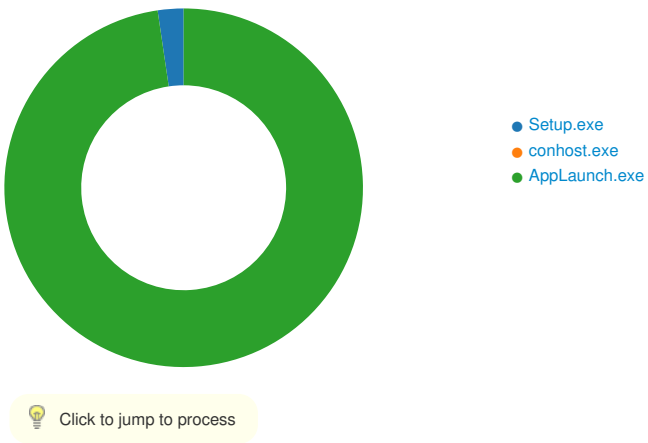
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 28, 2023 13:36:16.433954000 CEST	192.168.2.3	8.8.8.8	0x3b27	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)	false
May 28, 2023 13:36:16.476177931 CEST	192.168.2.3	8.8.8.8	0x28e5	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 13:36:16.468082905 CEST	8.8.8.8	192.168.2.3	0x3b27	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 13:36:16.511054039 CEST	8.8.8.8	192.168.2.3	0x28e5	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: Setup.exe PID: 6908, Parent PID: 3452

General

Target ID:	0
Start time:	13:35:56
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\Setup.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Setup.exe
Imagebase:	0x400000
File size:	359160 bytes
MD5 hash:	3694C18F01430F213ACED163C75788A0
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: 00000000.00000003.351025860.0000000000562000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.351304103.000000000042A000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	1			invalid handle	1	40EFEA	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
unknown	unknown	4096	invalid handle	1	414625	ReadFile

Analysis Process: conhost.exe PID: 7164, Parent PID: 6908

General

Target ID:	1
Start time:	13:35:56
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: 6868, Parent PID: 6908

General

Target ID:	2

Start time:	13:35:56
Start date:	28/05/2023
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:	0x130000
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_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.408509605.00000000071A3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.408509605.0000000007111000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.406792188.0000000000402000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.408509605.000000000759D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.408509605.0000000007233000.00000004.00000800.00020000.00000000.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	7299CF06	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	7299CF06	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	717EBEFF	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	717EBEFF	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	72CAC78D	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	2843	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	72CAC907	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	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	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	7	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	10	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	24	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\Desktop\JDDHMPCDUJ.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\JDDHMPCDUJ.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\JDDHMPCDUJ.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\NYMMPCEIMA.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\NYMMPCEIMA.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\NYMMPCEIMA.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\QCOILOQIKC.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\QCOILOQIKC.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\QCOILOQIKC.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\JDDHMPCDUJ.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\JDDHMPCDUJ.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\JDDHMPCDUJ.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\NYMMPCEIMA.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\NYMMPCEIMA.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\NYMMPCEIMA.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\QCOILOQIKC.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\QCOILOQIKC.docx	unknown	1022	end of file	1	717E1B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly