ID: 876997
Sample Name: Igv6ymbAA3.exe
Cookbook: default.jbs
Time: 10:32:07
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

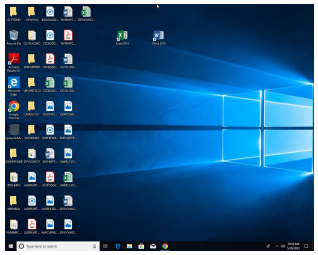
Windows Analysis Report

Igv6ymbAA3.exe

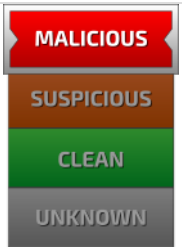
Overview

General Information

Sample Name:	Igv6ymbAA3.exe
Original Sample Name:	18ecf495a7e8d..
Analysis ID:	876997
MD5:	18ecf495a7e8d..
SHA1:	10a613527dc3...
SHA256:	f4e57d6160cc7..
Tags:	32 exe trojan
Infos:	



Detection



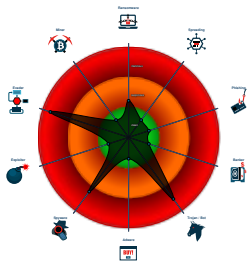
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Detected unpacking (overwrites its o...
- Detected unpacking (changes PE se...
- Snort IDS alert for network traffic
- Tries to steal Crypto Currency Walle...
- Machine Learning detection for sam...
- Queries sensitive video device infor...
- Queries sensitive disk information (v...
- C2 URLs / IPs found in malware con...

Classification



Process Tree

- **System is w10x64**
- Igv6ymbAA3.exe (PID: 5896 cmdline: C:\Users\user\Desktop\Igv6ymbAA3.exe MD5: 18ECF495A7E8DC91DE0F57F60C9896F8)
- **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": "51.210.170.199:23368",
  "Bot Id": "LogsDiller Cloud (Telegram: @logsdillabot)",
  "Authorization Header": "c2955ed3813a798683a185a82e949f88"
}
```

Yara Signatures

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.400990974.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.400990974.0000000000400000.00000040.00000001.01000000.00000003.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1e4b0:$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 • 0x80:$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E • 0x1300:$s3: 83 EC 38 53 B0 B8 88 44 24 2B 88 44 24 2F B0 A6 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x2018a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1fdd0:$s5: delete[] • 0x1f288:$s6: constructor or from DllMain.
00000000.00000002.402241386.0000000002850000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.402241386.0000000002850000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1e462:$pat14: , CommandLine: • 0x14a52:$v2_1: ListOfProcesses • 0x13170:$v4_3: base64str • 0x1312f:$v4_4: stringKey • 0x1317a:$v4_5: BytesToStringConverted • 0x13165:$v4_6: FromBase64 • 0x1470d:$v4_8: procName
00000000.00000003.350331599.0000000002450000.00000004.00001000.00020000.00000000.sdmp	MAL_Malware_Imphash_Mar23_1	Detects malware by known bad imphash or rich_pe_header_hash	Arnim Rupp	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.lgv6ymbAA3.exe.2450000.0.raw.unpack	MAL_Malware_Imphash_Mar23_1	Detects malware by known bad imphash or rich_pe_header_hash	Arnim Rupp	
0.3.lgv6ymbAA3.exe.2450000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.lgv6ymbAA3.exe.2450000.0.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1d0b0:$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 • 0x80:$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E • 0x700:$s3: 83 EC 38 53 B0 B8 88 44 24 2B 88 44 24 2F B0 A6 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x1ed8a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1e9d0:$s5: delete[] • 0x1de88:$s6: constructor or from DllMain.
0.2.lgv6ymbAA3.exe.400000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
0.2.lgv6ymbAA3.exe.400000.0.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1e4b0:$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 • 0x80:$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E • 0x1300:$s3: 83 EC 38 53 B0 B8 88 44 24 2B 88 44 24 2F B0 A6 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x2018a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1fdd0:$s5: delete[] • 0x1f288:$s6: constructor or from DllMain.
Click to see the 30 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.3 - Destination IP: 51.210.170.199

Timestamp:	192.168.2.351.210.170.19949701233682043233 05/28/23-10:33:05.871920
SID:	2043233
Source Port:	49701
Destination Port:	23368
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.3 - Destination IP: 51.210.170.199

Timestamp:	192.168.2.351.210.170.19949701233682043231 05/28/23-10:33:20.355629
SID:	2043231
Source Port:	49701
Destination Port:	23368
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 51.210.170.199 - Destination IP: 192.168.2.3

Timestamp:	51.210.170.199192.168.2.323368497012043234 05/28/23-10:33:06.698130
SID:	2043234
Source Port:	23368
Destination Port:	49701
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

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)

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

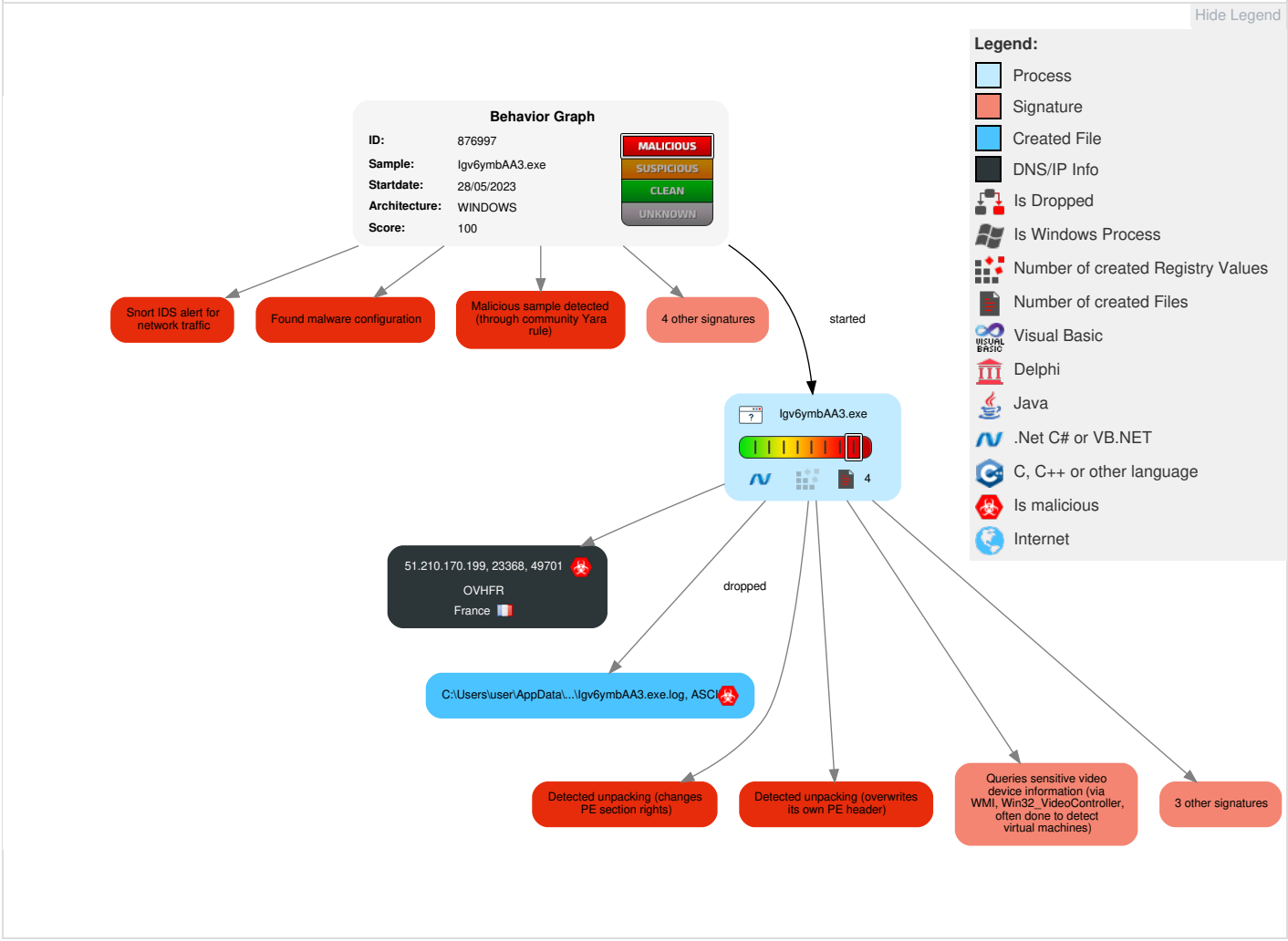
Yara detected RedLine Stealer

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	Path Interception	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 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	2 5 1 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	2 Native API	Logon Script (Windows)	Logon Script (Windows)	2 3 1 Virtualization/Sandbox Evasion	Security Account Manager	2 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	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)	1 Deobfuscate/Decode Files or Information	NTDS	1 2 Process Discovery	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	3 Obfuscated 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 2 Software Packing	Cached Domain Credentials	1 3 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
lgv6ymbAA3.exe	41%	Virustotal		Browse
lgv6ymbAA3.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
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/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/Id22Response(	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/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/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/Id19Response$9	0%	Avira URL Cloud	safe	
51.210.170.199:23368	0%	Avira URL Cloud	safe	
51.210.170.199:23368	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
51.210.170.199:23368	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	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	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003D22000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003D9F000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003BC5000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002E0B000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003D3F000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002C65000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003CA4000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003AC4000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003CC1000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003BA8000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003DBC000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002D7E000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003C43000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002BD8000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003AA7000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003C26000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003C43000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002BD8000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003AA7000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003C26000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id21Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id22Response(	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high

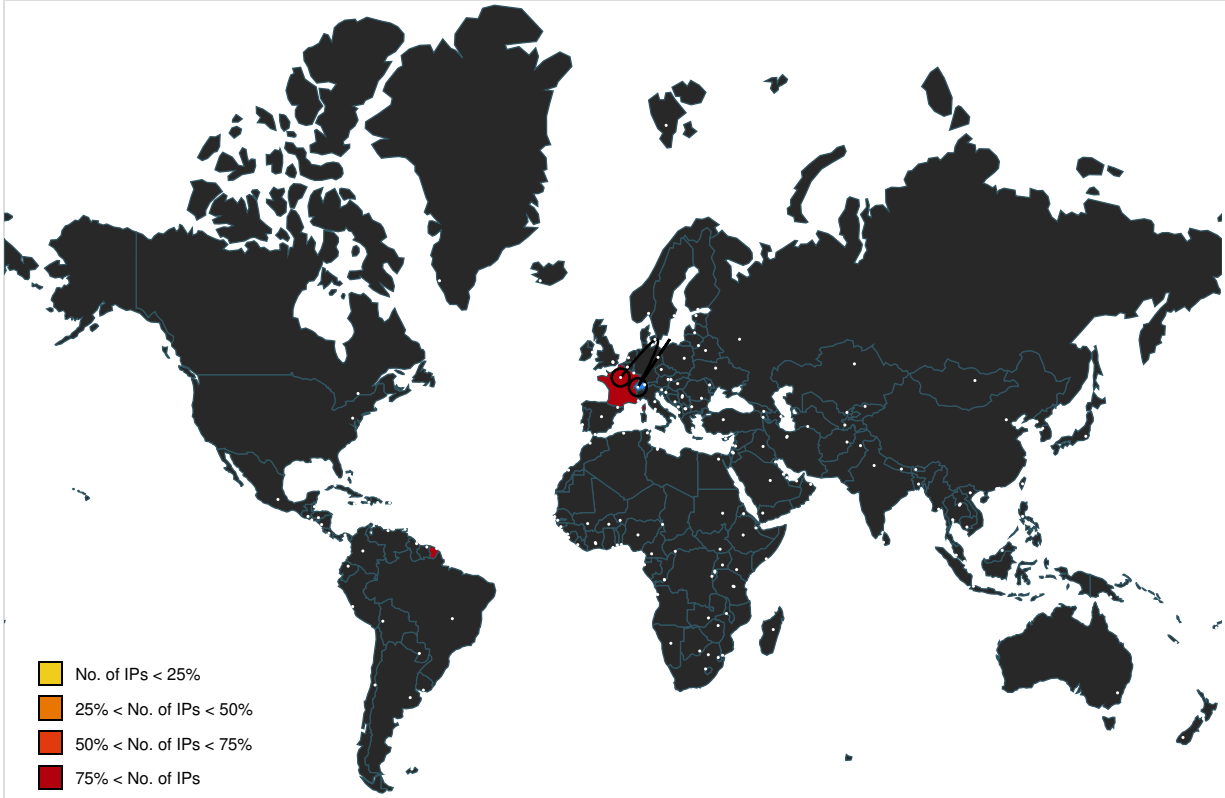
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	Igv6ymbAA3.exe, 00000000.00000002.402241386.0000000002850000.00000004.08000000.00040000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.401980636.00000000025EE000.00000004.00000020.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402147783.0000000002700000.00000004.08000000.00040000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000003.350614100.00000000009EE000.00000004.00000020.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19Response$9	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003C43000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002BD8000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003AA7000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003C26000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003D22000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003D9F000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003BC5000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.402656262.0000000002E0B000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003D3F000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.402656262.0000000002C65000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003CA4000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003AC4000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003CC1000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003BA8000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003DBC000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.402656262.0000000002D7E000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003C43000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.402656262.0000000002BD8000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003AA7000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.402656262.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp, lgv6ymbAA3.exe, 00000000.00000002.403988658.0000000003C26000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	lgv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	lgv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	lgv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	lgv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	lgv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	lgv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	lgv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	lgv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	lgv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	lgv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	lgv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	lgv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	lgv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id12	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm8D	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	Igv6ymbAA3.exe, 00000000.00000002.402656262.000000002A96000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003D22000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003D9F000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003BC5000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002E0B000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003D3F000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002C65000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003CA4000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003AC4000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003CC1000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003BA8000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003DBC000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002D7E000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003C43000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002BD8000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003AA7000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp, Igv6ymbAA3.exe, 00000000.00000002.403988658.0000000003C26000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	Igv6ymbAA3.exe, 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	Igv6ymbAA3.exe, 00000000.00000002.402656262.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.210.170.199	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876997
Start date and time:	2023-05-28 10:32:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 24s
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:	3
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:	lgv6ymbAA3.exe
Original Sample Name:	18ecf495a7e8dc91de0f57f60c9896f8.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@1/1@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 12.1% (good quality ratio 11.6%) • Quality average: 85% • Quality standard deviation: 24.9%
HCA Information:	• Successful, ratio: 100% • 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
- 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:33:16	API Interceptor	25x Sleep call for process: Igv6ymbAA3.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\Igv6ymbAA3.exe.log

Process:	C:\Users\user\Desktop\Igv6ymbAA3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2843
Entropy (8bit):	5.3371553026862095
Encrypted:	false
SSDEEP:	48:MIHK5HKXeHKIEHU0YHKhQnouHIWUfHKhBHKdHKBfHK5AHKzvQTHmtHoxHImHK1HI:Pq5qXeqm00YqhQnouOqLqdqNq2qzcGtx
MD5:	E9C2F4CC11CEA097B88D7D224F41A5B3

SHA1:	B16891C1E967E2803C1F994CA61ED82A52233C54
SHA-256:	843CF5780CF7C018F8431C1A69DB910BDC039E48C495A2C854A0C1A9C52CAF82
SHA-512:	2259C7E86AE80AC4CB26AB22FE50295D2C17E45BF31DF0BC3E91BCC9063300616764C1219E9B40A16EED0D2D63035B0EF1ED7B1BDBAEDF9408BF9D46E5A86D48
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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, Cultu

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.963681234872864
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:	lgv6ymbAA3.exe
File size:	356864
MD5:	18ecf495a7e8dc91de0f57f60c9896f8
SHA1:	10a613527dc3d67c40957b9ee2eb8e0a4dd79fcc
SHA256:	f4e57d6160cc7f2ad503c3b1627cb5176ccc6e20490399b3700cdf7eeef8beec
SHA512:	51d57cb2d51bd314252da33b35d8c3d40b83f783a9bfd3475fe4d34d3472d497e8fd02c915d5ce687d33f4770ec26c609de06c64d1607198aa0bba8d0c7a01ab
SSDEEP:	6144:Ofr4CTYnMaqblzRhIVpCaTLymSB+1Va/dliK+jzTtim:U/TYM7bhRhmCaTRSKqdAPTtim
TLSH:	C0745B1382A13E96E9A64B769E1FD6E8761EF1708F597769321CFA1F08700B2D173B10
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Richb.....PE..L....?.b.....

File Icon

Icon Hash:	454941454d55691d

Static PE Info

General

Entrypoint:	0x404e59
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x62E73FCE [Mon Aug 1 02:51:58 2022 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:	2d9ed3462f8a74bfd1231e2e9de56b43

Entrypoint Preview
Instruction
call 00007F4D3CD9DD53h
jmp 00007F4D3CD993EDh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F4D3CD99596h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F4D3CD995C0h
test ecx, 00000003h
jne 00007F4D3CD99561h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F4D3CD9955Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F4D3CD995A4h
test ah, ah
je 00007F4D3CD99596h
test eax, 00FF0000h
je 00007F4D3CD99585h
test eax, FF000000h
je 00007F4D3CD99574h
jmp 00007F4D3CD9953Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]

Instruction
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 004012D8h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x38ba8	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x280000	0x19398	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x29a000	0xddc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3150	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.text
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	0x3866a	0x38800	False	0.8478723036504425	data	7.755781377893314	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x3a000	0x245844	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x280000	0x19398	0x19400	False	0.3788869121287129	data	4.259520200570937	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x29a000	0x33d8	0x3400	False	0.22611177884615385	data	2.5254465339166545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x280730	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x2815d8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x281e80	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x284428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2854d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x285988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x286830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2870d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x287640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x289be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x28ac90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x28b618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x28bae8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x28c990	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x28d238	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x28d900	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x28de68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x290410	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2914b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x291988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x292830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2930d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x293640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x295be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x296c90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x297618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x297d20	0x664	data		
RT_STRING	0x298388	0x59e	data		
RT_STRING	0x298928	0x29a	data		
RT_STRING	0x298bc8	0x248	data		
RT_STRING	0x298e10	0x582	data		
RT_GROUP_ICON	0x297a80	0x68	data		
RT_GROUP_ICON	0x285938	0x4c	data		
RT_GROUP_ICON	0x291920	0x68	data		
RT_GROUP_ICON	0x28ba80	0x68	data		

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x297ae8	0x238	data		

Imports

DLL	Import
KERNEL32.dll	GetModuleHandleW, IsBadReadPtr, GetConsoleAliasesLengthA, WaitForMultipleObjectsEx, GetPrivateProfileIntA, FreeConsole, GetVersionExW, WritePrivateProfileStructW, MulDiv, GetModuleFileNameW, CreateActCtxA, WritePrivateProfileStringW, ReplaceFileA, GetStringTypeExA, GetStdHandle, GetLogicalDriveStringsA, OpenMutexW, GetLastError, ReadConsoleOutputCharacterA, GetProcAddress, AttachConsole, SleepEx, VirtualAlloc, _hwrite, LoadLibraryA, InterlockedExchangeAdd, LocalAlloc, GetFileType, CreateFileMappingW, FindFirstVolumeMountPointW, GetNumberFormatW, CreateEventW, GetModuleFileNameA, lstrcmpiW, GetModuleHandleA, CreateMutexA, GetFileAttributesExW, GetConsoleCursorInfo, ScrollConsoleScreenBufferA, GetCurrentThreadId, FindAtomW, EnumResourceLanguagesW, DebugBreak, FindNextVolumeA, AddConsoleAliasW, CancelWaitableTimer, GetCommState, WaitForSingleObject, GetLongPathNameA, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, WideCharToMultiByte, SetHandleCount, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, Sleep, ExitProcess, WriteFile, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, SetFilePointer, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, InitializeCriticalSectionAndSpinCount, HeapSize, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, CreateFileA, CloseHandle
USER32.dll	CharLowerBuffA
GDI32.dll	GetCharWidthW, EnumFontsW, GetCharABCWidthsFloatW
ADVAPI32.dll	MapGenericMask

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.351.210.170.19949470123368204323305/28/23-10:33:05.871920	TCP	2043233	ET TROJAN RedLine Stealer TCP CnC net.tcp Init	49701	23368	192.168.2.3	51.210.170.199
192.168.2.351.210.170.19949470123368204323105/28/23-10:33:20.355629	TCP	2043231	ET TROJAN Redline Stealer TCP CnC Activity	49701	23368	192.168.2.3	51.210.170.199
51.210.170.199192.168.2.323368497012043234 05/28/23-10:33:06.698130	TCP	2043234	ET MALWARE Redline Stealer TCP CnC - Id1Response	23368	49701	51.210.170.199	192.168.2.3

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:33:05.533560991 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:05.562397003 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:05.566582918 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:05.871920109 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:05.902595997 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:05.949218988 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:06.668385029 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:06.698129892 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:06.746134996 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:14.263818979 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:14.297100067 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:14.297166109 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:14.297219992 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:14.297239065 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:14.340572119 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:15.257227898 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:15.288314104 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.434360981 CEST	49701	23368	192.168.2.3	51.210.170.199

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:33:15.589613914 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:15.617861032 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.634917974 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:15.663518906 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.677033901 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:15.707966089 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.729003906 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:15.757349014 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.811477900 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:15.839639902 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.843931913 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:15.872005939 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.873869896 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:15.901968002 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.951283932 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:15.978918076 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.979000092 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.979039907 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.979079008 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.979975939 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:15.987600088 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.015773058 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.128205061 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.156337976 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.158643961 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.186841011 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.246958971 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.414422035 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.441956997 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.442012072 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.442051888 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.442087889 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.442123890 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.442158937 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.442244053 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.442317009 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.442323923 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.442359924 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.442436934 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.442529917 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.442540884 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.442781925 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.442909002 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.469741106 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.469794035 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.469836950 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.469872952 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.469911098 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.469947100 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.469993114 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.469994068 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.470072985 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.470109940 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.470113993 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.470175982 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.470210075 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.470283985 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.470377922 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.470400095 CEST	49701	23368	192.168.2.3	51.210.170.199

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:33:16.470482111 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.470524073 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.470558882 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.470627069 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.470649004 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.470662117 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.470798969 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.470835924 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.471026897 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.471116066 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.471204042 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.471309900 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.471580029 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.497410059 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.497462034 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.497500896 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.497575045 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.497670889 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.497778893 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.497778893 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.497801065 CEST	23368	49701	51.210.170.199	192.168.2.3
May 28, 2023 10:33:16.497898102 CEST	49701	23368	192.168.2.3	51.210.170.199
May 28, 2023 10:33:16.497925043 CEST	23368	49701	51.210.170.199	192.168.2.3

Statistics

No statistics

System Behavior

Analysis Process: Igv6ymbAA3.exe PID: **5896**, Parent PID: **3452**

General

Target ID:	0
Start time:	10:32:56
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\Igv6ymbAA3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Igv6ymbAA3.exe
Imagebase:	0x400000
File size:	356864 bytes
MD5 hash:	18ECF495A7E8DC91DE0F57F60C9896F8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.400990974.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.400990974.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.402241386.0000000002850000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.402241386.0000000002850000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: MAL_Malware_Imphash_Mar23_1, Description: Detects malware by known bad imphash or rich_pe_header_hash, Source: 00000000.00000003.350331599.0000000002450000.00000004.00001000.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.350331599.0000000002450000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000003.350331599.0000000002450000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.401980636.00000000025EE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.402147783.0000000002700000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.402147783.0000000002700000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.350614100.00000000009EE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.401518261.0000000002410000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.401518261.0000000002410000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.401246578.0000000000989000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.402656262.00000000029B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	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\SystemCache	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\lgv6ymbAA3.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\Igv6ymbAA3.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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	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\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\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\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	6135	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:\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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ZIPXYXWIOY.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\ZIPXYXWIOY.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\ZIPXYXWIOY.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
C:\Users\user\Documents\QCOILOQIKC.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\ZIPXYXWIOY.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\ZIPXYXWIOY.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\ZIPXYXWIOY.docx	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\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	5	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

Disassembly

No disassembly