ID: 829694
Sample Name: o6B2U4HjCJ.exe
Cookbook: default.jbs
Time: 22:05:06
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

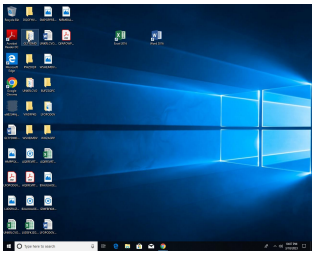
Windows Analysis Report

o6B2U4HjCJ.exe

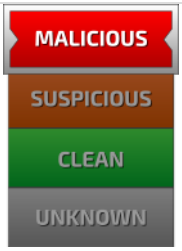
Overview

General Information

Sample Name:	o6B2U4HjCJ.exe
Original Sample Name:	dcb518ed1ed6…
Analysis ID:	829694
MD5:	dcb518ed1ed6…
SHA1:	c770b74ee42b…
SHA256:	38f88f2119c82…
Tags:	32 exe trojan
Infos:	



Detection



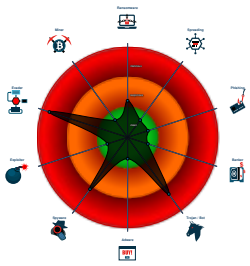
RedLine

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

Signatures

- Yara detected RedLine Stealer
- 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
- Machine Learning detection for sam…
- Queries sensitive video device infor…
- Queries sensitive disk information (v…
- C2 URLs / IPs found in malware con…
- Tries to harvest and steal browser in…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- o6B2U4HjCJ.exe (PID: 5604 cmdline: C:\Users\user\Desktop\o6B2U4HjCJ.exe MD5: DCB518ED1ED68C30A11CB79D50A0FE69)
- **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.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": "185.11.61.125:22344",
  "Bot Id": "@chicago",
  "Message": "Error",
  "Authorization Header": "21f863e0cbd09d0681058e068d0d1d7f"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.295675318.0000000004DD0000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.295675318.0000000004DD0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x282c4:$pat14: , CommandLine: • 0x1c8c4:$v2_1: ListOfProcesses • 0x1c09f:$v4_3: base64str • 0x1c06c:$v4_4: stringKey • 0x1c0a9:$v4_5: BytesToStringConverted • 0x1c094:$v4_6: FromBase64 • 0x1c578:$v4_8: procName • 0x1a09f:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
00000000.00000002.295096246.0000000004955000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.295520420.0000000004C40000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.295520420.0000000004C40000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x291ac:$pat14: , CommandLine: • 0x1d7ac:$v2_1: ListOfProcesses • 0x1cf87:$v4_3: base64str • 0x1cf54:$v4_4: stringKey • 0x1cf91:$v4_5: BytesToStringConverted • 0x1cf7c:$v4_6: FromBase64 • 0x1d460:$v4_8: procName • 0x1af87:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT

Click to see the 9 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.o6B2U4HjCJ.exe.400000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.o6B2U4HjCJ.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:$s3: 83 EC 38 53 B0 C7 88 44 24 2B 88 44 24 2F B0 43 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x2018a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1fdd0:$s5: delete[] • 0x1f288:$s6: constructor or from DllMain.
0.2.o6B2U4HjCJ.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.o6B2U4HjCJ.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1d0b0:$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 C7 88 44 24 2B 88 44 24 2F B0 43 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.o6B2U4HjCJ.exe.2c80e67.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 23 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: 185.11.61.125

Timestamp:	192.168.2.3185.11.61.12549701223442043233 03/18/23-22:06:06.966690
SID:	2043233
Source Port:	49701
Destination Port:	22344
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

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

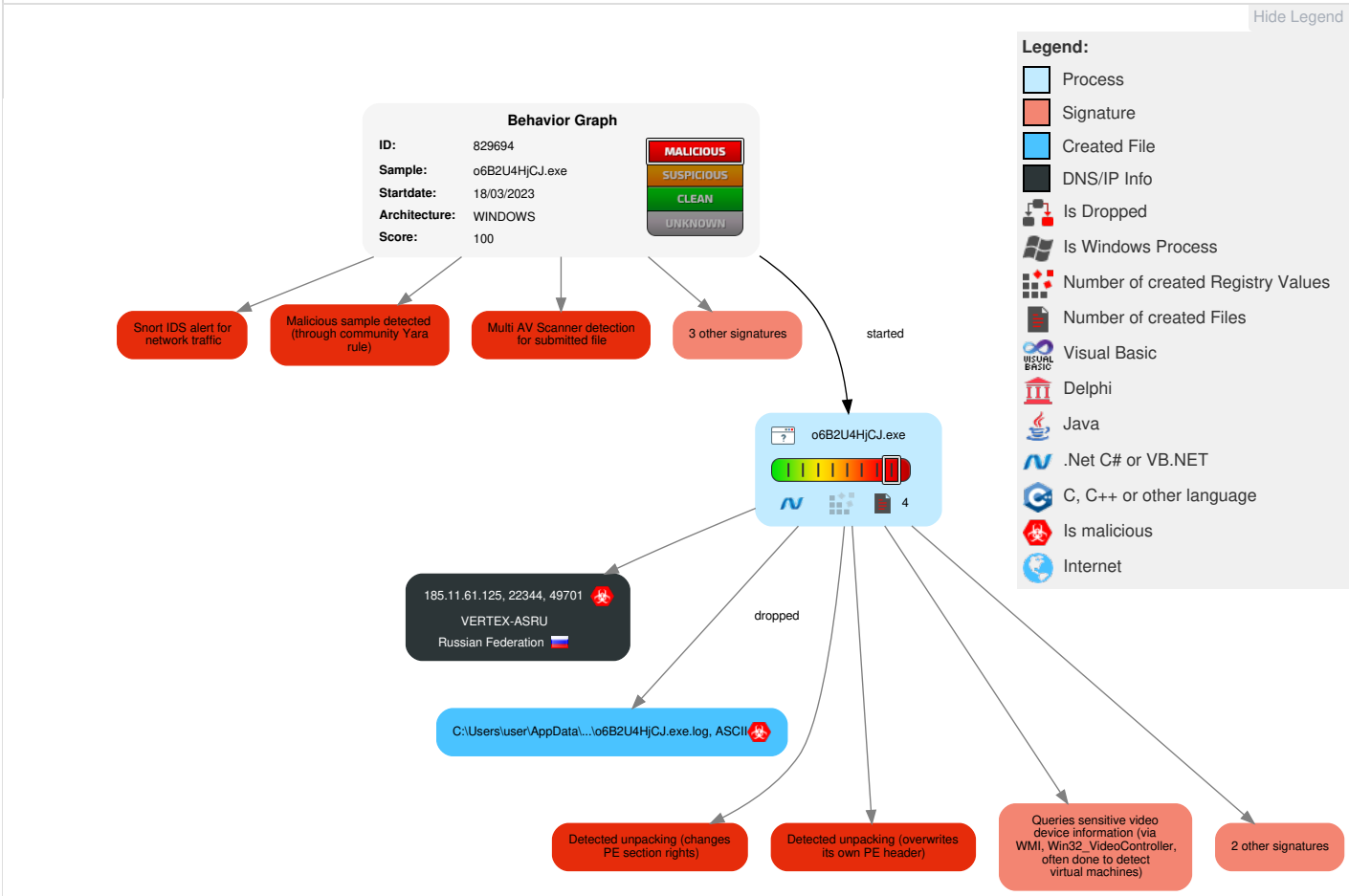
Remote Access Functionality

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 6 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	1 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
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
o6B2U4HjCJ.exe	38%	ReversingLabs	Win32.Trojan.Generic	
o6B2U4HjCJ.exe	39%	Virustotal		Browse
o6B2U4HjCJ.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/Contract/MSValue2Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Contract/MSValue3Response	0%	URL Reputation	safe	
185.11.61.125:22344	0%	URL Reputation	safe	
http://tempuri.org/Contract/MSValue1	0%	URL Reputation	safe	
http://tempuri.org/Contract/MSValue2	0%	URL Reputation	safe	
http://tempuri.org/Contract/MSValue3	0%	URL Reputation	safe	
http://www.w3.o	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
185.11.61.125:22344	true	• URL Reputation: 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	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000613D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000050B8000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000525C000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000005144000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005F4D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000502D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000005FE1000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000605F000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000051D0000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061B8000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000615A000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005FC4000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000006042000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061D5000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060C0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061D5000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060C0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Contract/MSValue2Response	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	o6B2U4HjCJ.exe, 00000000.00000002.295675318.0000000004DD0000.00000004.08000000.00040000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.295096246.0000000004955000.00000004.00000020.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.295520420.0000000004C40000.00000004.08000000.00040000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.239241764.0000000002F47000.00000004.00000020.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061D5000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060C0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Contract/MSValue3Response	o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000547B000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000613D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000050B8000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000525C000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000005144000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005F4D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000502D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000005FE1000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000605F000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000051D0000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061B8000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000615A000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005FC4000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000006042000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061D5000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060C0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high

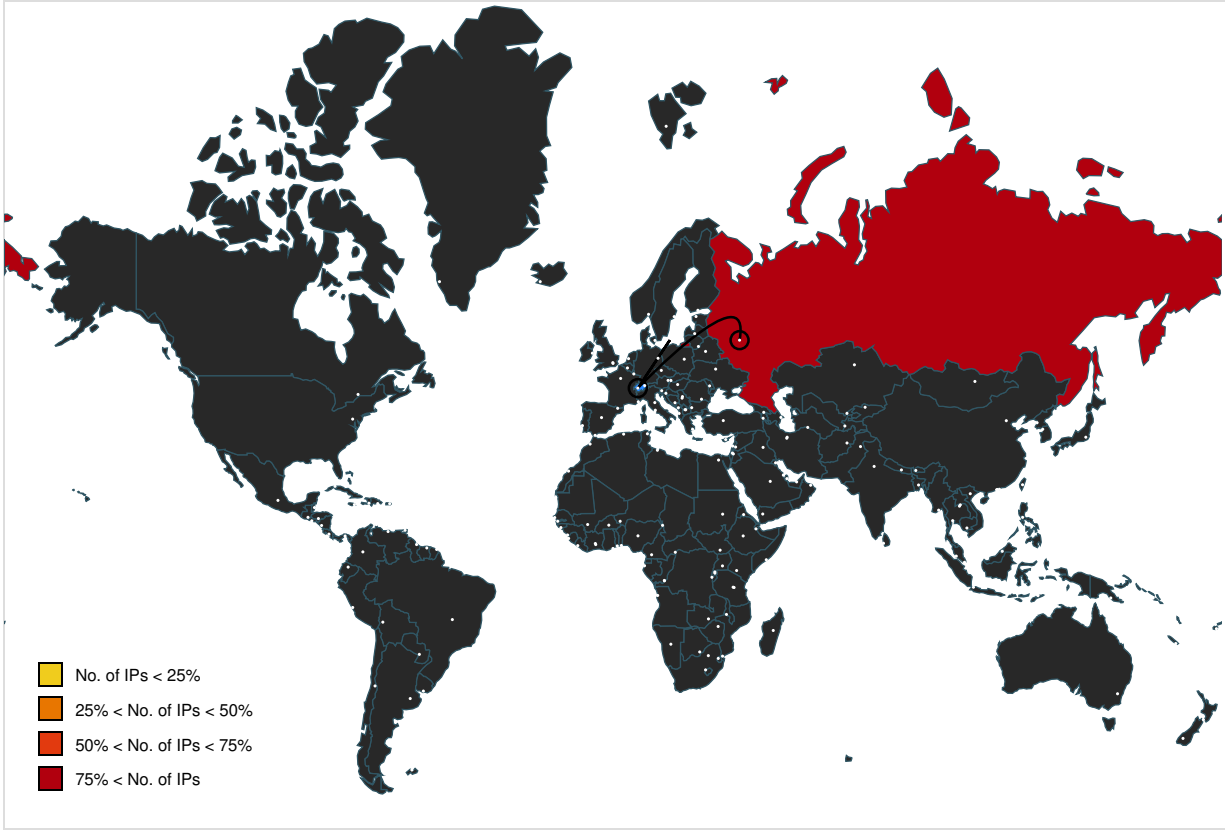
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000613D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000050B8000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000525C000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000005144000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005F4D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000502D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005FE1000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000605F000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000051D0000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061B8000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000615A000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005FC4000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000006042000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061D5000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060C0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Contract/MSValue1	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Contract/MSValue2	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Contract/MSValue3	o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000547B000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.w3.o	o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000053FA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentif	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Committed	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/fault	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/right/possessproperty	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/sct	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/RegisterResponse	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Cancel	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/rm/SequenceAcknowledgement	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000613D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000050B8000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000525C000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000005144000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005F4D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000502D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000005FE1000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000605F000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000051D0000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061B8000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000615A000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005FC4000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000006042000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061D5000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060C0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/tlsnego#TLS_Wrap	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2002/12/policy	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/dk	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Issue	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000613D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000050B8000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000525C000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000005144000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005F4D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.000000000502D000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000005FE1000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000605F000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.296405357.00000000051D0000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061B8000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.000000000615A000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000005FC4000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.0000000006042000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000003.284064494.00000000061D5000.00000004.00000800.00020000.00000000.sdmp, o6B2U4HjCJ.exe, 00000000.00000002.298158758.00000000060C0000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2004/04/security/trust/RST/Issue	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Commit	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContext	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Issue	o6B2U4HjCJ.exe, 00000000.00000002.296405357.0000000004F32000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.11.61.125	unknown	Russian Federation		199539	VERTEX-ASRU	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829694
Start date and time:	2023-03-18 22:05:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 15s
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:	12
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:	o6B2U4HjCJ.exe
Original Sample Name:	dcb518ed1ed68c30a11cb79d50a0fe69.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@1/1@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 15.9% (good quality ratio 15.2%) • Quality average: 84.9% • Quality standard deviation: 24.9%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 93.184.221.240, 209.197.3.8
- Excluded domains from analysis (whitelisted): fs.microsoft.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:06:13	API Interceptor	55x Sleep call for process: o6B2U4HjCJ.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\o6B2U4HjCJ.exe.log

Process:	C:\Users\user\Desktop\o6B2U4HjCJ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHK5HKXRfHK7HKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHK1HG1qHxLH5HZHu:Pq5qXdq7qLqdqUqzcGYqhQnoPtlxHbqs

MD5:	D7EF19655FC3FB2B87FA63100FBBD255
SHA1:	5959AAD372EAEA1B7B74F9D6471842D30E3316FD
SHA-256:	460A28FAAA1701DEDEFD31077A122992C13E5F6D7DD9EBBE481100F67D1721DD
SHA-512:	EEF0AF31D3D233905CF3C38C9ACE054117E36EF40C6C7FAFB68268749E917D1DA4DF0A8FE9C7CA4A486C77AA083B6437EA7AFCB235A5C24D25B6AD4AB5A0104E
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..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.6860198334423
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:	o6B2U4HjCJ.exe
File size:	435712
MD5:	dcb518ed1ed68c30a11cb79d50a0fe69
SHA1:	c770b74ee42bba7f1699341e8b03923b93a60789
SHA256:	38f88f2119c82d04462c902771d27d1ec546b3d556081a6103d844add1a9af09
SHA512:	69cf914141ba3d01aeaedf40da8a546aa1dbd9bcc9027018edc80a3bbbca564e45b91f62877167bd049915571bedd0542d16b34559b8c8a2b672d57be2a8479c
SSDEEP:	6144:CJcavfLvJ3Vx3AxSqFPt+HTUVe64wGz/wWpNV/DXqOxI:Yvf7J3Vx3AEqFPdVzpGEWpzLII
TLSH:	75946C8392A17D59E9264B33DE1FCAE8B71DF270DF49776632189A2B04701F2C163B94
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B...,..,...,.....,.....,.....,..0W..,..-...,.....,.....,.....,.Rich..,.....PE..L.....Ma.....

File Icon

Icon Hash:	94a4a49480a4a4e2

Static PE Info

General

Entrypoint:	0x406ee1
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:	0x614DF0F8 [Fri Sep 24 15:38:32 2021 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:	6aedf45f51642709580c9dc83560f5b5

Entrypoint Preview
Instruction
call 00007F350C94D4F4h
jmp 00007F350C94804Eh
mov edi, edi
push ebp
mov ebp, esp
push ecx
push ebx
push esi
push edi
push dword ptr [02AF4010h]
call 00007F350C94CF89h
push dword ptr [02AF400Ch]
mov edi, eax
mov dword ptr [ebp-04h], edi
call 00007F350C94CF79h
mov esi, eax
pop ecx
pop ecx
cmp esi, edi
jc 00007F350C948259h
mov ebx, esi
sub ebx, edi
lea eax, dword ptr [ebx+04h]
cmp eax, 04h
jc 00007F350C948249h
push edi
call 00007F350C94D622h
mov edi, eax
lea eax, dword ptr [ebx+04h]
pop ecx
cmp edi, eax
jnc 00007F350C94821Ah
mov eax, 00000800h
cmp edi, eax
jnc 00007F350C9481D4h
mov eax, edi
add eax, edi
cmp eax, edi
jc 00007F350C9481E1h
push eax
push dword ptr [ebp-04h]
call 00007F350C94D5B0h
pop ecx
pop ecx
test eax, eax
jne 00007F350C9481E8h
lea eax, dword ptr [edi+10h]
cmp eax, edi
jc 00007F350C948212h
push eax
push dword ptr [ebp-04h]
call 00007F350C94D59Ah
pop ecx
pop ecx
test eax, eax
je 00007F350C948203h
sar ebx, 02h
push eax

Instruction
lea esi, dword ptr [eax+ebx*4]
call 00007F350C94CE94h
pop ecx
mov dword ptr [02AF4010h], eax
push dword ptr [ebp+08h]
call 00007F350C94CE86h
mov dword ptr [esi], eax
add esi, 04h
push esi
call 00007F350C94CE7Bh
pop ecx
mov dword ptr [02AF400Ch], eax
mov eax, dword ptr [ebp+08h]
pop ecx
jmp 00007F350C9481D4h
xor eax, eax
pop edi
pop esi
pop ebx
leave
ret
mov edi, edi
push 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	0x4285c	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26f6000	0x19d70	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2710000	0xe80	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1210	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	0x2fe8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1b4	.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	0x42260	0x42400	False	0.859655070754717	data	7.764807118496576	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x44000	0x26b1148	0x4200	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x26f6000	0x19d70	0x19e00	False	0.3816519474637681	data	4.236556234424828	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2710000	0x9d20	0x9e00	False	0.08086926424050633	data	1.0065032619882839	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x26f67e0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Mexico
RT_ICON	0x26f7688	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Spanish	Mexico
RT_ICON	0x26f7f30	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Mexico
RT_ICON	0x26fa4d8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Mexico
RT_ICON	0x26fb580	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Mexico
RT_ICON	0x26fba38	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Spanish	Mexico
RT_ICON	0x26fc8e0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Spanish	Mexico
RT_ICON	0x26fd188	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Spanish	Mexico
RT_ICON	0x26fd850	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Spanish	Mexico
RT_ICON	0x26fddb8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Spanish	Mexico
RT_ICON	0x2700360	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Spanish	Mexico
RT_ICON	0x2701408	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Spanish	Mexico
RT_ICON	0x2701d90	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Spanish	Mexico
RT_ICON	0x2702270	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Mexico
RT_ICON	0x2703118	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27039c0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Mexico
RT_ICON	0x2703f28	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27064d0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Mexico
RT_ICON	0x2707578	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Spanish	Mexico
RT_ICON	0x2707f00	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27083d0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Mexico
RT_ICON	0x2709278	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Spanish	Mexico
RT_ICON	0x2709b20	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Spanish	Mexico
RT_ICON	0x270a1e8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Mexico
RT_ICON	0x270a750	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Mexico
RT_ICON	0x270ccf8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Mexico
RT_ICON	0x270dda0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Spanish	Mexico
RT_ICON	0x270e728	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Mexico
RT_STRING	0x270ec78	0x490	data		
RT_STRING	0x270f108	0x3d6	data		
RT_STRING	0x270f4e0	0x492	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0x270f978	0x3f8	data		
RT_ACCELERATOR	0x270ec08	0x48	data	Spanish	Mexico
RT_ACCELERATOR	0x270ec50	0x18	data	Spanish	Mexico
RT_GROUP_ICON	0x2708368	0x68	data	Spanish	Mexico
RT_GROUP_ICON	0x26fb9e8	0x4c	data	Spanish	Mexico
RT_GROUP_ICON	0x27021f8	0x76	data	Spanish	Mexico
RT_GROUP_ICON	0x270eb90	0x76	data	Spanish	Mexico
None	0x270ec68	0xa	data		

Imports

DLL	Import
KERNEL32.dll	GetLogicalDriveStringsW, SetDefaultCommConfigW, CreateHardLinkA, GetConsoleAliasesA, LoadLibraryW, _hread, IsBadCodePtr, CreateEventA, FormatMessageW, GetFileAttributesA, GetExitCodeProcess, SetConsoleMode, WriteConsoleW, WritePrivateProfileSectionW, ChangeTimerQueueTimer, SetLastError, GetProcAddress, GlobalAddAtomA, EnumSystemCodePagesW, LocalAlloc, FoldStringA, FreeEnvironmentStringsW, VirtualProtect, EndUpdateResourceA, GetWindowsDirectoryW, GetFileInformationByHandle, InterlockedPushEntrySList, LCMapStringW, CloseHandle, CreateFileA, GetModuleHandleA, LCMapStringA, lstrcpynA, CallNamedPipeA, VirtualAlloc, GetVolumeNameForVolumeMountPointA, InterlockedIncrement, InterlockedDecrement, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetStartupInfoW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetLastError, HeapFree, RtlUnwind, RaiseException, TerminateProcess, GetCurrentProcess, IsDebuggerPresent, HeapAlloc, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, WriteFile, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, FlushFileBuffers, GetModuleHandleW, ExitProcess, GetModuleFileNameA, GetModuleFileNameW, GetEnvironmentStringsW, GetCommandLineW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, GetCurrentThreadId, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapSize, HeapReAlloc, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, GetLocaleInfoA, GetStringTypeA, MultiByteToWideChar, GetStringTypeW, SetFilePointer, InitializeCriticalSectionAndSpinCount, WriteConsoleA, GetConsoleOutputCP, SetStdHandle, LoadLibraryA
USER32.dll	ClientToScreen, LoadMenuA, InvalidateRgn, GetMenuInfo, MessageBoxIndirectW, CountClipboardFormats, SetScrollInfo
GDI32.dll	GetGlyphIndicesW
ADVAPI32.dll	RegOpenKeyA

Possible Origin

Language of compilation system	Country where language is spoken	Map
Spanish	Mexico	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3185.11.61.125 49701223442043233 03/18/23-22:06:06.966690	TCP	2043233	ET TROJAN RedLine Stealer TCP CnC net.tcp Init	49701	22344	192.168.2.3	185.11.61.125

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 22:06:06.592199087 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:06.655941010 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:06.658765078 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:06.966690063 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:07.029198885 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:07.077758074 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:07.997076988 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:08.103241920 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:08.316272974 CET	22344	49701	185.11.61.125	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 22:06:08.359060049 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:09.933237076 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:10.037476063 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:10.411091089 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:10.411191940 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:10.411237955 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:10.411282063 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:10.411313057 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:10.411329031 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:10.411367893 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:10.468873978 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:21.734165907 CET	49701	22344	192.168.2.3	185.11.61.125
Mar 18, 2023 22:06:21.796538115 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:21.796591997 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:21.796624899 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:21.796658993 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:21.798943996 CET	22344	49701	185.11.61.125	192.168.2.3
Mar 18, 2023 22:06:21.815443039 CET	49701	22344	192.168.2.3	185.11.61.125

Statistics

No statistics

System Behavior

Analysis Process: o6B2U4HjCJ.exe PID: **5604**, Parent PID: **3452**

General

Target ID:	0
Start time:	22:05:55
Start date:	18/03/2023
Path:	C:\Users\user\Desktop\o6B2U4HjCJ.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\o6B2U4HjCJ.exe
Imagebase:	0x400000
File size:	435712 bytes
MD5 hash:	DCB518ED1ED68C30A11CB79D50A0FE69
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: 00000000.00000002.295675318.0000000004DD0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.295675318.0000000004DD0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.295096246.0000000004955000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.295520420.0000000004C40000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.295520420.0000000004C40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.239241764.0000000002F47000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.294617353.0000000002ED8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.238934056.0000000002E10000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000003.238934056.0000000002E10000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.293546962.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.293546962.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.294046050.0000000002C80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.294046050.0000000002C80000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
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\Microsoft\Wind?ws	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\o6B2U4HjCJ.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\o6B2U4HjCJ.exe.log	0	2291	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\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	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\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\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:\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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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

Disassembly

No disassembly