ID: 626607
Sample Name: 2sibxc6cB1.exe
Cookbook: default.jbs
Time: 15:37:08
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

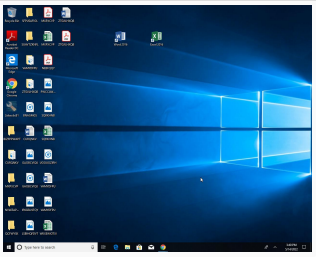
Windows Analysis Report

2sibxc6cB1.exe

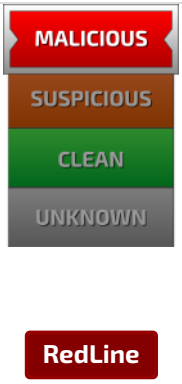
Overview

General Information

Sample Name:	2sibxc6cB1.exe
Analysis ID:	626607
MD5:	bba7db09449a22.
SHA1:	49ce80fb77d7a0..
SHA256:	ffd0e59168d8d32.
Tags:	exe RedLineStealer
Infos:	



Detection



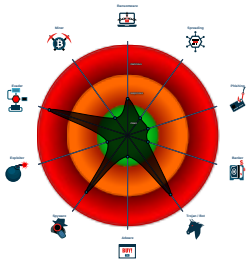
RedLine

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…
- Found many strings related to Crypt…

Classification



Process Tree

- **System is w10x64**
- 2sibxc6cB1.exe (PID: 6204 cmdline: "C:\Users\user\Desktop\2sibxc6cB1.exe" MD5: BBA7DB09449A22CFE8F3310BF1238210)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "185.215.113.75:4531"
  ],
  "Bot Id": "swttestmet",
  "Authorization Header": "adc5dc30debab8d39a706f26a199fa7e"
}
```


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
00000000.00000003.246398659.0000000000A30000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.246398659.0000000000A30000.00000004.00001000.00020000.00000000.sdmp	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:$s3: 83 EC 38 53 B0 9A 88 44 24 2B 88 44 24 2F B0 67 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x1ed8a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1e9d0:$s5: delete[] • 0x1de88:$s6: constructor or from DllMain.
00000000.00000002.306736738.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.306736738.0000000000400000.00000040.00000001.01000000.00000003.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1e4b0:$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 9A 88 44 24 2B 88 44 24 2F B0 67 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.
00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.2sibxc6cB1.exe.400000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.2sibxc6cB1.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:$s3: 83 EC 38 53 B0 9A 88 44 24 2B 88 44 24 2F B0 67 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x2018a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1fdd0:$s5: delete[] • 0x1f288:$s6: constructor or from DllMain.
0.2.2sibxc6cB1.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.2sibxc6cB1.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1d0b0:$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 9A 88 44 24 2B 88 44 24 2F B0 67 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.
0.3.2sibxc6cB1.exe.a30000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 27 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 185.215.113.75 - Destination IP: 192.168.2.4

Timestamp:	185.215.113.75192.168.2.44531497602850353 05/14/22-15:38:34.055550
SID:	2850353
Source Port:	4531
Destination Port:	49760
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.4 - Destination IP: 185.215.113.75

Timestamp:	192.168.2.4185.215.113.754976045312850027 05/14/22-15:38:32.157673
SID:	2850027
Source Port:	49760
Destination Port:	4531
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.4 - Destination IP: 185.215.113.75

Timestamp:	192.168.2.4185.215.113.754976045312850286 05/14/22-15:38:35.355126
SID:	2850286
Source Port:	49760
Destination Port:	4531
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

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

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

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

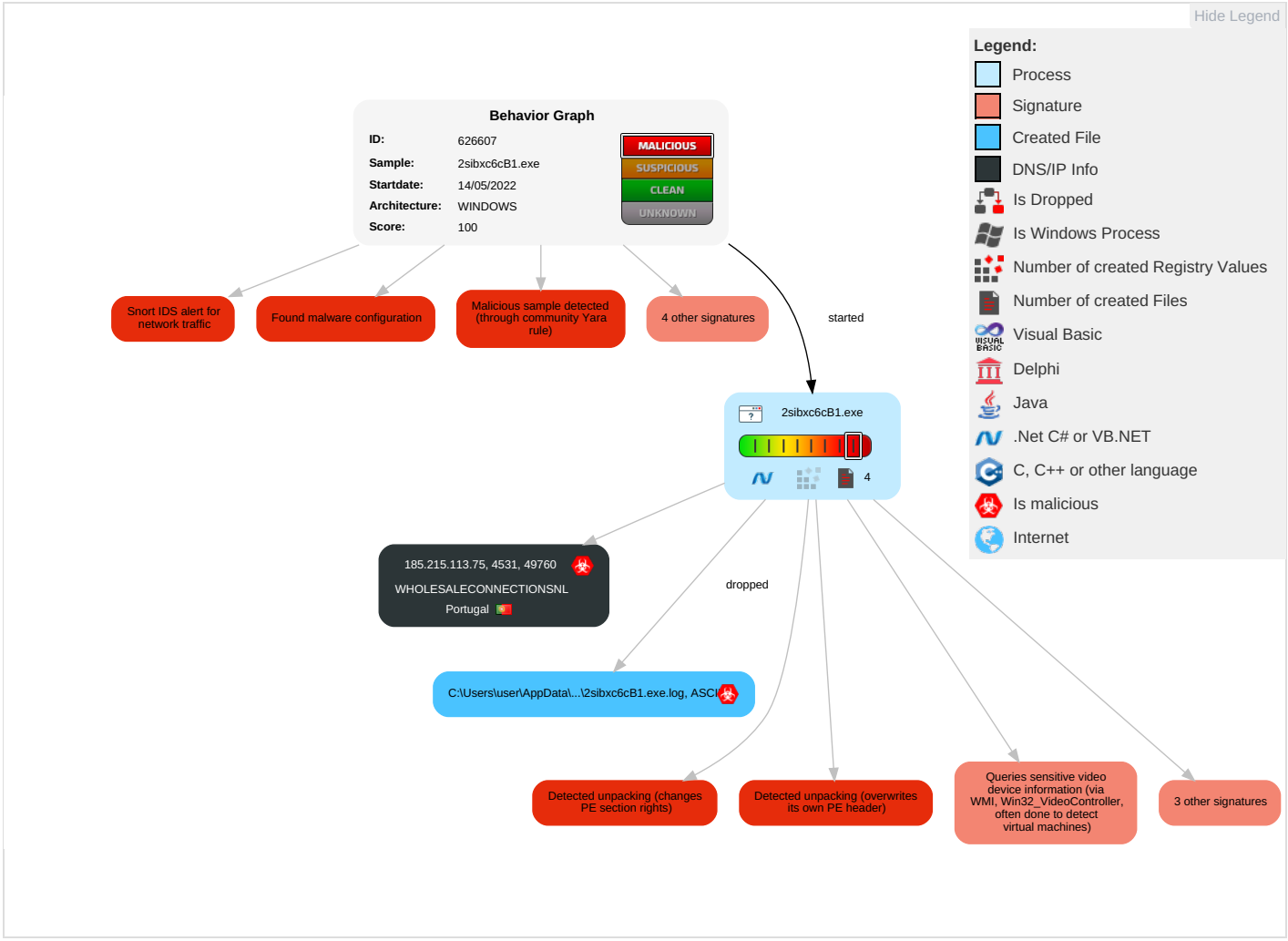
Remote Access Functionality

Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 2 1 Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	1 OS Credential Dumping	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 4 1 Virtualization/Sandbox Evasion	Security Account Manager	2 4 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	3 Data from Local System	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	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
2sibxc6cB1.exe	46%	ReversingLabs	Win32.Infostealer.Generic	
2sibxc6cB1.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://service.r	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://go.micros	0%	URL Reputation	safe	
http://www.w3.o	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310209713.0000000002A45000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310717466.0000000002B37000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.311202864.0000000003717000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000003.304581848.00000000039BA000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.312021174.00000000038CC000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309239992.00000000027FD000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000003.304495912.0000000003949000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310367494.0000000002A5B000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309879444.0000000002983000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.311581188.00000000037E9000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.311814941.000000000385A000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309571126.00000000028C1000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://service.r	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	2sibxc6cB1.exe, 00000000.00000002.310367494.0000000002A5B000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309879444.0000000002983000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.311581188.00000000037E9000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.311814941.000000000385A000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309571126.00000000028C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_real	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_pdf	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://forms.real.com/real/realone/download.html?type=rpsp_us	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://support.a	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.308048938.0000000002343000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000003.246882548.00000000007B2000.00000004.00000020.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.308192150.00000000024D0000.00000004.08000000.00040000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.308507932.0000000002650000.00000004.08000000.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome/?p=plugin_quicktime	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/sc	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	2sibxc6cB1.exe, 00000000.00000002.310367494.000000002A5B000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309879444.0000000002983000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.311581188.00000000037E9000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.311814941.000000000385A000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309571126.00000000028C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_shockwave	2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://forms.rea	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_wmp	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/answer/6258784	2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_flash	2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_java	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://go.micros	2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_divx	2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fpdownload.macromedia.com/get/shockwave/default/english/win95nt/latest/Shockwave_Installer_Sl	2sibxc6cB1.exe, 00000000.00000002.310900982.0000000002B9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.w3.o	2sibxc6cB1.exe, 00000000.00000002.310367494.000000002A5B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentif	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Committed	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/fault	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/right/possessproperty	2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/sct	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/RegisterResponse	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Cancel	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/SequenceAcknowledgement	2sibxc6cB1.exe, 00000000.00000002.308838013.00000000026F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	2sibxc6cB1.exe, 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310209713.0000000002A45000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310717466.0000000002B37000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.311202864.0000000003717000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309998781.0000000002999000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000003.304581848.00000000039BA000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.312021174.00000000038CC000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309322720.0000000002813000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309239992.00000000027FD000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000003.304495912.0000000003949000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309657760.00000000028D7000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.310367494.0000000002A5B000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309879444.0000000002983000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.311581188.00000000037E9000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.311814941.000000000385A000.00000004.00000800.00020000.00000000.sdmp, 2sibxc6cB1.exe, 00000000.00000002.309571126.00000000028C1000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.215.113.75	unknown	Portugal		206894	WHOLESALECONNECTIONSNL	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626607
Start date and time: 14/05/202215:37:08	2022-05-14 15:37:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2sibxc6cB1.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@1/1@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 42.3% (good quality ratio 40.6%) • Quality average: 84.9% • 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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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.
- VT rate limit hit for: 2sibxc6cB1.exe

Simulations

Behavior and APIs

Time	Type	Description
15:38:44	API Interceptor	14x Sleep call for process: 2sibxc6cB1.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\2sibxc6cB1.exe.log

Process:	C:\Users\user\Desktop\2sibxc6cB1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHK5HKXRfHK7HKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKoLHG1qHqHAH5HX:Pq5qXdq7qLqdqUqzcGYqhQnoPtlxHbq4
MD5:	924DEA6470CAC502B24442CF377CE6A7

SHA1:	133C304912A1DF4AF62F6EDCA3EA21F3E0CE7F4F
SHA-256:	2B2572C7D0134EEF12644AF90D61302A50E7B550FFB4629666F8C566F34BED0D
SHA-512:	34C817F3F4D87AAD5F6902BB80522B59FE8F9935C86819B575B6139EBDEF3026866ED802DB1D36765CF7ECCF323692705DCA3D799FC7CFF7C0114B08CBE9F7A9
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.Runtime92aa12#\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):	5.9584871530039845
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:	2sibxc6cB1.exe
File size:	379904
MD5:	bba7db09449a22cfe8f3310bf1238210
SHA1:	49ce80fb77d7a06c4de52ddf2457e1dfceb7661c
SHA256:	ffd0e59168d8d32c26f16e557b26d7fc45a748ae3d2621f40c740848762249a6
SHA512:	930a6dae0d84521584022956aa8f6fffc2f1bd17d4b009647fd23dfc600da9936360ac56f3b5c393a9a61e1f6f1c9846d29b3786f6713383c7cf060653fc5168
SSDEEP:	6144:toaV+vVYmvkH1MA3ggu8otbXz+q+yUshZUsx8:toaV+tPvk/gZ8oN+jyLHUsx8
TLSH:	C584F121B3A0C035E493163054B5E2B16E7EB8A7A531458B67A8AF3D6F703C05FB9367
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j....sS..sS..sS.}.S..sS.}.S..sS.}.S..sS.s.S..sS..rS..sS.}.S..sS.}.S..sS.}.S..sSRich..sS.....PE..L....^.`...

File Icon

Icon Hash:	d0e4e6b6e4cce134

Static PE Info

General

Entrypoint:	0x405fd9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x60065E96 [Tue Jan 19 04:22:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	3b1349984d3f2d24d6b47d7a7e833ab3

Entrypoint Preview
Instruction
call 00007FFB54F07E42h
jmp 00007FFB54F03D7Eh
sub eax, 000003A4h
je 00007FFB54F03F14h
sub eax, 04h
je 00007FFB54F03F09h
sub eax, 0Dh
je 00007FFB54F03EFEh
dec eax
je 00007FFB54F03EF5h
xor eax, eax
ret
mov eax, 00000404h
ret
mov eax, 00000412h
ret
mov eax, 00000804h
ret
mov eax, 00000411h
ret
mov edi, edi
push esi
push edi
mov esi, eax
push 00000101h
xor edi, edi
lea eax, dword ptr [esi+1Ch]
push edi
push eax
call 00007FFB54F07E9Ch
xor eax, eax
movzx ecx, ax
mov eax, ecx
mov dword ptr [esi+04h], edi
mov dword ptr [esi+08h], edi
mov dword ptr [esi+0Ch], edi
shl ecx, 10h
or eax, ecx
lea edi, dword ptr [esi+10h]
stosd
stosd
stosd
mov ecx, 00447018h
add esp, 0Ch
lea eax, dword ptr [esi+1Ch]
sub ecx, esi
mov edi, 00000101h
mov dl, byte ptr [ecx+eax]
mov byte ptr [eax], dl
inc eax
dec edi
jne 00007FFB54F03EE9h
lea eax, dword ptr [esi+0000011Dh]
mov esi, 00000100h
mov dl, byte ptr [eax+ecx]
mov byte ptr [eax], dl
inc eax
dec esi

Instruction
jne 00007FFB54F03EE9h
pop edi
pop esi
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 0000051Ch
mov eax, dword ptr [00447BE0h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
push edi
lea eax, dword ptr [ebp-00000518h]
push eax
push dword ptr [esi+04h]
call dword ptr [0040108Ch]
mov edi, 00000100h

Rich Headers

Programming Language:	• [LNK] VS2010 build 30319 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x45864	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xec000	0x3ce0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf0000	0x9c4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11b0	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	0x3480	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x168	.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	0x45074	0x45200	False	0.735741834313	data	7.03896581857	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x47000	0xa19e4	0x10c00	False	0.0268481809701	data	0.355626057246	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.xatoc	0xe9000	0xbb8	0xc00	False	0.00813802083333	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kecizu	0xea000	0x270	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hig	0xeb000	0x17	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xec000	0x3ce0	0x3e00	False	0.632371471774	data	5.68983329755	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	0xf0000	0x1834	0x1a00	False	0.328425480769	data	3.31415310491	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xec1f0	0x6c8	dBase III DBT, version number 0, next free block index 40, 1st item "\235\242\225"	Marathi	India
RT_ICON	0xec8b8	0x25a8	data	Marathi	India
RT_ICON	0xeee60	0x468	GLS_BINARY_LSB_FIRST	Marathi	India
RT_STRING	0xef498	0x272	data	French	Switzerland
RT_STRING	0xef710	0x21c	data	French	Switzerland
RT_STRING	0xef930	0x3ae	data	French	Switzerland
RT_GROUP_ICON	0xef2c8	0x30	data	Marathi	India
RT_VERSION	0xef2f8	0x1a0	data	French	Switzerland

Imports

DLL	Import
KERNEL32.dll	FreeLibrary, InterlockedIncrement, OpenJobObjectA, GetCurrentProcess, SetDefaultCommConfigW, GetConsoleAliasesLengthA, GetGeoInfoW, GetUserDefaultLangID, GetEnvironmentStrings, GlobalAlloc, SetConsoleMode, GetAtomNameW, GetModuleFileNameW, GetSystemDirectoryA, GetBinaryTypeW, MoveFileExA, LCMapStringA, GetLastError, GetProcAddress, GetDiskFreeSpaceW, LoadLibraryA, LocalAlloc, CreateEventW, GetCommTimeouts, EnumCalendarInfoExA, lstrcmpW, FindResourceA, MultiByteToWideChar, HeapFree, HeapAlloc, GetCommandLineA, HeapSetInformation, GetStartupInfoW, GetCPInfo, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, EncodePointer, TlsAlloc, TlsGetValue, TlsSetValue, DecodePointer, TlsFree, GetModuleHandleW, SetLastError, GetCurrentThreadId, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, TerminateProcess, IsProcessorFeaturePresent, HeapCreate, ExitProcess, WriteFile, GetStdHandle, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, InitializeCriticalSectionAndSpinCount, GetFileType, DeleteCriticalSection, SetFilePointer, GetModuleFileNameA, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, LCMapStringW, GetStringTypeW, Sleep, GetConsoleCP, GetConsoleMode, LoadLibraryW, ReadFile, RtlUnwind, SetStdHandle, FlushFileBuffers, HeapReAlloc, WriteConsoleW, RaiseException, HeapSize, CreateFileW, CloseHandle
ADVAPI32.dll	ImpersonateAnonymousToken

Version Infos

Description	Data
Copyrighz	Copyright (C) 2022, pozkarte
ProjectVersion	28.82.74.73
FileVersion	69.47.75.23

Possible Origin

Language of compilation system	Country where language is spoken	Map
Marathi	India	
French	Switzerland	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
185.215.113.75192.168.2.44531497602850353 05/14/22-15:38:34.055550	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	4531	49760	185.215.113.75	192.168.2.4
192.168.2.4185.215.113.754976045312850027 05/14/22-15:38:32.157673	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49760	4531	192.168.2.4	185.215.113.75
192.168.2.4185.215.113.754976045312850286 05/14/22-15:38:35.355126	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49760	4531	192.168.2.4	185.215.113.75

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:38:31.719527960 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:31.774760962 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:31.774909019 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:32.157672882 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:32.214399099 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:32.284423113 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:33.990946054 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:34.055550098 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:34.284590960 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:35.355125904 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:35.431688070 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:35.431745052 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:35.431785107 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:35.431827068 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:35.431855917 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:35.431907892 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:35.486258030 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:35.486289024 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:35.486402988 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:46.709021091 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:46.777354002 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:46.790785074 CEST	4531	49760	185.215.113.75	192.168.2.4
May 14, 2022 15:38:46.879378080 CEST	49760	4531	192.168.2.4	185.215.113.75
May 14, 2022 15:38:47.161674976 CEST	49760	4531	192.168.2.4	185.215.113.75

Statistics

No statistics

System Behavior

Analysis Process: 2sibxc6cB1.exe PID: 6204, Parent PID: 3328

General

Target ID:	0
Start time:	15:38:13
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\2sibxc6cB1.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\2sibxc6cB1.exe"
Imagebase:	0x400000

File size:	379904 bytes
MD5 hash:	BBA7DB09449A22CFE8F3310BF1238210
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: 00000000.00000003.246398659.0000000000A30000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000003.246398659.0000000000A30000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.306736738.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.306736738.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.308928908.0000000002752000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.308048938.0000000002343000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.246882548.00000000007B2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.308192150.00000000024D0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.308192150.00000000024D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.307296199.00000000006D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.308507932.0000000002650000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.308507932.0000000002650000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
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	6DB4CF06	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	6DB4CF06	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	6C99BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2sibxc6cB1.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE5C78D	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\2sibxc6cB1.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	6DE5C907	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	6DB25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6DA803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C991B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	22	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	22	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	44	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	2	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	18	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	6C991B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	22	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	16	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	44	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	2	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	36	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	22	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	44	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	2	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	36	6C991B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6C991B4F	ReadFile

Disassembly

No disassembly