ID: 651254
Sample Name: VBY5zBdZox
Cookbook: default.jbs
Time: 17:50:05
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

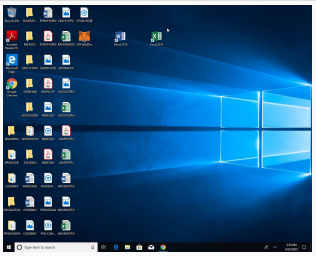
Windows Analysis Report

VBY5zBdZox

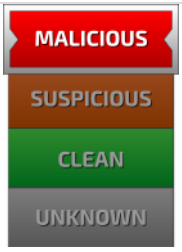
Overview

General Information

Sample Name:	VBY5zBdZox (renamed file extension from none to exe)
Analysis ID:	651254
MD5:	acc0fb4cb35df2d..
SHA1:	fff261da7332d1b..
SHA256:	907b6500dba0a0.
Tags:	32 exe
Infos:	



Detection



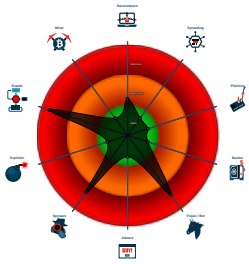
RedLine

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
- Tries to steal Crypto Currency Walle…
- Connects to many ports of the same…
- Machine Learning detection for sam…
- Yara detected Generic Downloader
- Queries sensitive video device infor…
- Queries sensitive disk information (v…

Classification



Process Tree

- **System is w10x64**
- VBY5zBdZox.exe (PID: 3176 cmdline: "C:\Users\user\Desktop\VBY5zBdZox.exe" MD5: ACC0FB4CB35DF2D49FC609F2E299ED5E)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "193.106.191.246:23196"
  ],
  "Bot Id": "RUZKI",
  "Authorization Header": "121027c094f768a0a0e9b562f6417952"
}
```


Yara Signatures

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.314646008.0000000005150000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.314646008.0000000005150000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
00000000.00000002.314646008.0000000005150000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x27856:$pat14: , CommandLine: • 0x1c01a:$v2_1: ListOfProcesses • 0x1b7bd:$v4_3: base64str • 0x1b78a:$v4_4: stringKey • 0x1b7c7:$v4_5: BytesToStringConverted • 0x1b7b2:$v4_6: FromBase64 • 0x1bcd5:$v4_8: procName • 0x1991d:$v5_7: RecordHeaderField • 0x19859:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
00000000.00000002.305431311.0000000002950000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.305431311.0000000002950000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.VBY5zBdZox.exe.27d0000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.VBY5zBdZox.exe.27d0000.0.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1d0b0:$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 • 0x80:$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E • 0x700:$s3: 83 EC 38 53 B0 87 88 44 24 2B 88 44 24 2F B0 AB 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x1ed8a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1e9d0:$s5: delete[] • 0x1de88:$s6: constructor or from DllMain.
0.2.VBY5zBdZox.exe.2950ee8.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.VBY5zBdZox.exe.2950ee8.2.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x25a56:$pat14: , CommandLine: • 0x1a21a:$v2_1: ListOfProcesses • 0x199bd:$v4_3: base64str • 0x1998a:$v4_4: stringKey • 0x199c7:$v4_5: BytesToStringConverted • 0x199b2:$v4_6: FromBase64 • 0x19ed5:$v4_8: procName • 0x17b1d:$v5_7: RecordHeaderField • 0x17a59:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.2.VBY5zBdZox.exe.2a63a26.5.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 33 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.4 - Destination IP: 193.106.191.246

Timestamp:	192.168.2.4193.106.191.24649758231962850027 06/23/22-17:51:27.182664
SID:	2850027
Source Port:	49758
Destination Port:	23196
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.4 - Destination IP: 193.106.191.246	
Timestamp:	192.168.2.4193.106.191.24649758231962850286 06/23/22-17:51:29.952462
SID:	2850286
Source Port:	49758
Destination Port:	23196
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 193.106.191.246 - Destination IP: 192.168.2.4	
Timestamp:	193.106.191.246192.168.2.423196497582850353 06/23/22-17:51:28.242070
SID:	2850353
Source Port:	23196
Destination Port:	49758
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

Connects to many ports of the same IP (likely port scanning)

Yara detected Generic Downloader

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)

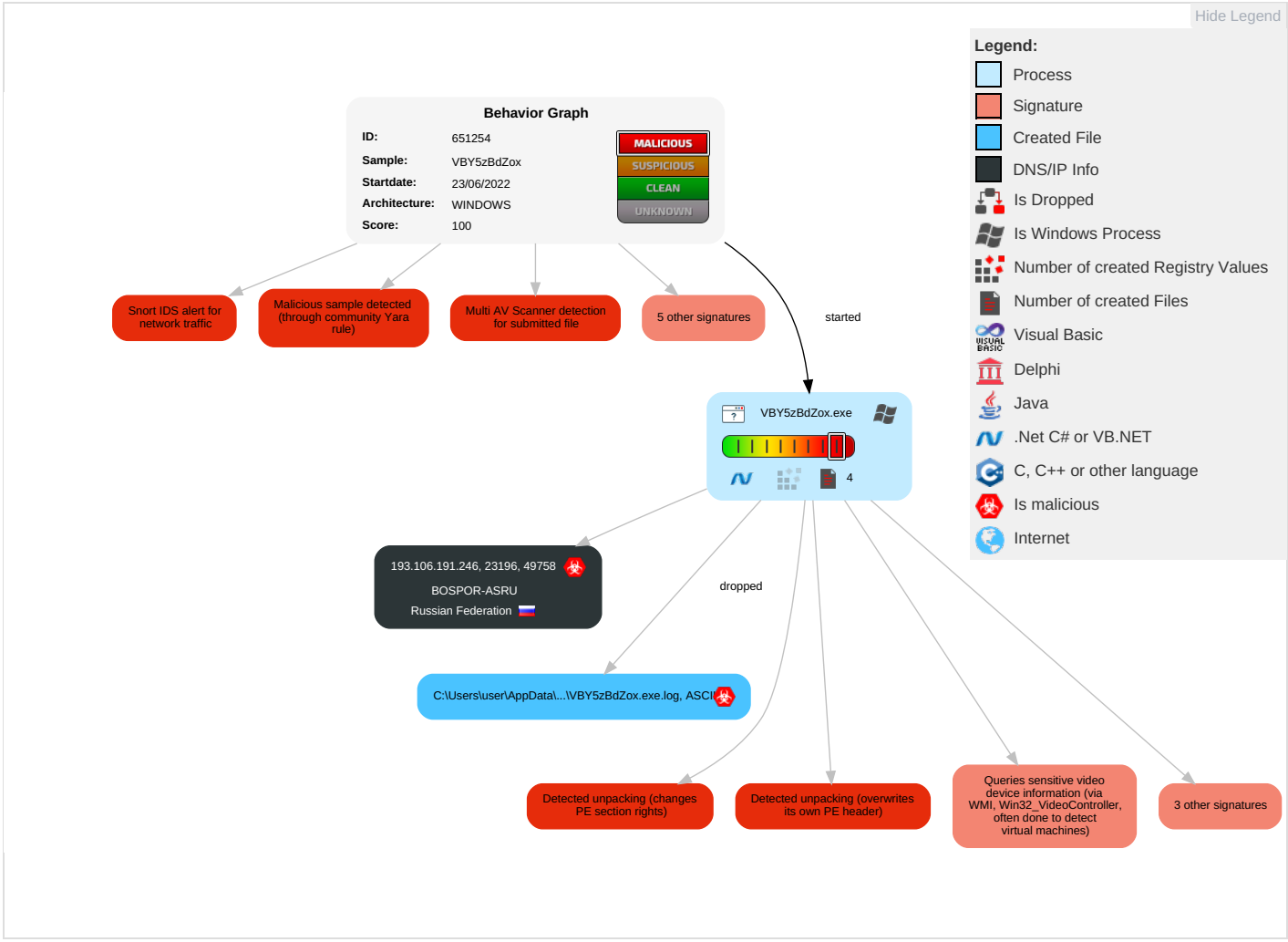
Tries to harvest and steal browser information (history, passwords, etc)

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 Archive Collected Data	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	LSASS Memory	2 6 Security Software Discovery	Remote Desktop Protocol	3 Data from Local System	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	Data from Network Shared Drive	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	2 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 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

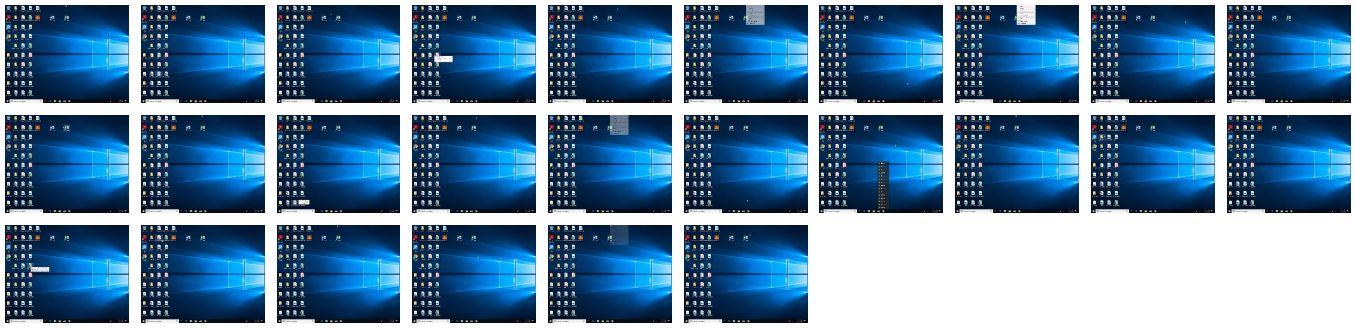
Behavior Graph



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
VBY5zBdZox.exe	35%	Virustotal		Browse
VBY5zBdZox.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	
http://tempuri.org/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://www.interoperabilitybridges.com/wmp-extension-for-chromea	0%	Avira URL Cloud	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	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312959266.00000000031D5000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314557209.0000000003FE9000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313959757.0000000003E42000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311668114.0000000002E91000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312555896.00000000030EC000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312182241.00000000003014000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312436650.00000000030D6000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314419518.0000000003F77000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314279019.0000000003F25000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312009501.0000000002F53000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313526639.0000000003D5A000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.00000000032B000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314105435.0000000003EB4000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://service.r	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312959266.00000000031D5000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314557209.0000000003FE9000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313959757.0000000003E42000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311668114.0000000002E91000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312555896.00000000030EC000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312182241.00000000003014000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312436650.00000000030D6000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314419518.0000000003F77000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314279019.0000000003F25000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312009501.0000000002F53000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313526639.0000000003D5A000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314105435.0000000003EB4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_real	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_pdf	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://forms.real.com/real/realone/download.html?type=rpsp_us	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://support.a	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	VBY5zBdZox.exe, 00000000.00000002.314646008.0000000005150000.00000004.08000000.00040000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.305431311.0000000029500000.00000004.08000000.00040000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000003.240106550.0000000000C15000.00000004.00000020.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313526639.0000000003D5A000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.306212179.0000000002A23000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_quicktime	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/sc	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high

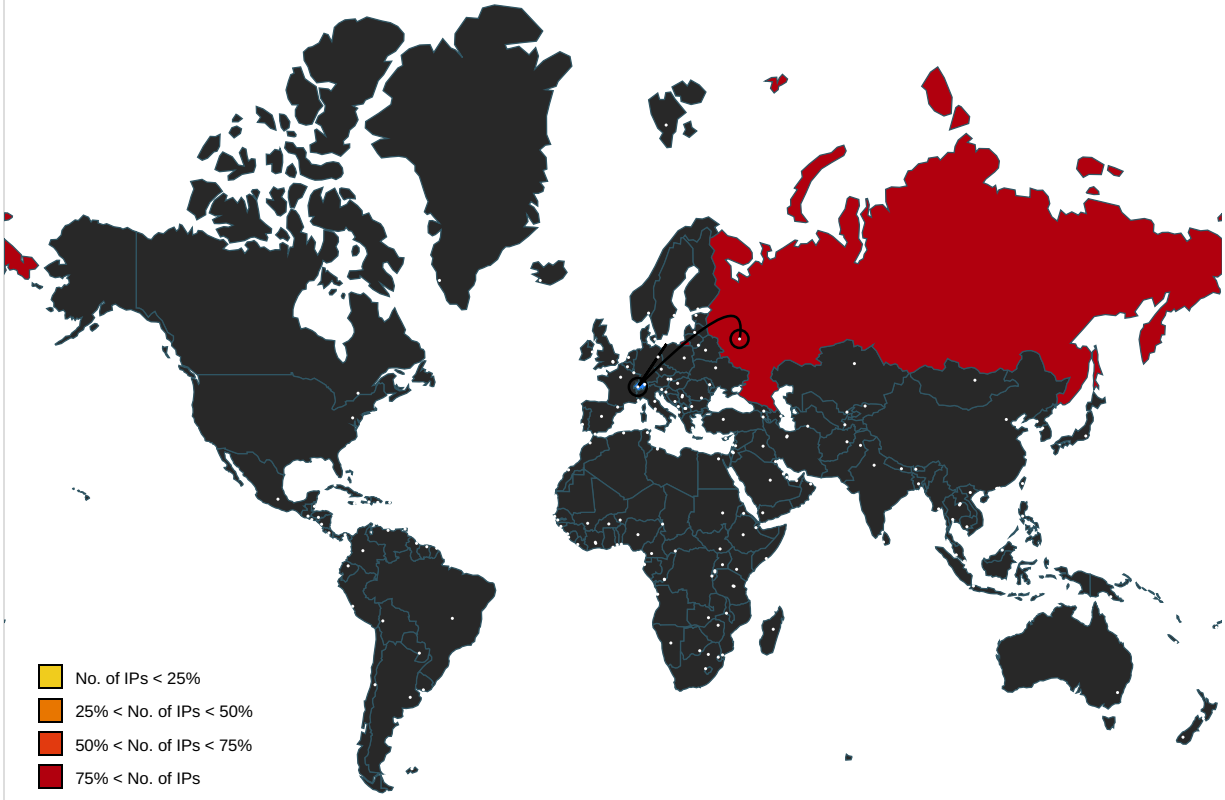
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312959266.00000000031D5000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314557209.0000000003FE9000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313959757.0000000003E42000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311668114.0000000002E91000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312555896.00000000030EC000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312182241.00000000003014000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312436650.00000000030D6000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314419518.0000000003F77000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314279019.0000000003F25000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312009501.0000000002F53000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313526639.0000000003D5A000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.00000000302B000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.314105435.0000000003EB4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome/?p=plugin_shockwave	VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://forms.rea	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.interoperabilitybridges.com/wmp-extension-for-chromea	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_wmp	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/answer/6258784	VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_flash	VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_java	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://go.micros	VBY5zBdZox.exe, 00000000.00000002.312070842.0000000002F69000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.313057637.00000000031EB000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.311765641.0000000002EA7000.00000004.00000800.00020000.00000000.sdmp, VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_divx	VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fpdownload.macromedia.com/get/shockwave/default/english/win95nt/latest/Shockwave_Installer_Sl	VBY5zBdZox.exe, 00000000.00000002.312246647.000000000302B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.w3.o	VBY5zBdZox.exe, 00000000.00000002.312555896.00000000030EC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentif	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Committed	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/fault	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/right/possessproperty	VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/sct	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/RegisterResponse	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Cancel	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/SequenceAcknowledgement	VBY5zBdZox.exe, 00000000.00000002.308467878.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT	VBY5zBdZox.exe, 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.106.191.246	unknown	Russian Federation		42238	BOSPOR-ASRU	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651254
Start date and time: 23/06/202217:50:05	2022-06-23 17:50:05 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VBY5zBdZox (renamed file extension from none to 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:	24
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: 38.5% (good quality ratio 36.9%) • 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:	• 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): www.bing.com, ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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
17:51:39	API Interceptor	11x Sleep call for process: VBY5zBdZox.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\VBY5zBdZox.exe.log

Process:	C:\Users\user\Desktop\VBY5zBdZox.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2932
Entropy (8bit):	5.334469918014252
Encrypted:	false
SSDEEP:	48:MIHK5HKXeHKlEHU0YHKhQnouHIWUfHK7HKhBHKdHKB1AHKzvQTHmtHoxHImHK1HQ:Pq5qXeqm00YqhQnouOq7qLqdqUqzcGtk
MD5:	E35A7613F21B0D1588DE4D14CF853427
SHA1:	18AE391E9AB0C970849150EE4D7111473EEE2BD3
SHA-256:	2EB260A8675B41093A7696456E8386F5D212A131BB298D9CC1C58D05E3DA8D49
SHA-512:	6E06C59608F8E491D69F66BB1E83DD522A48D1836CA6B03449822E7BD126ACB2EEEB08FA748CF6E2A524EED361738549B48712E3146AE3D3E958CD2ECD73D1E
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Cultu

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.236398485913625
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:	VBY5zBdZox.exe
File size:	423424
MD5:	acc0fb4cb35df2d49fc609f2e299ed5e
SHA1:	fff261da7332d1bef4253539c3217dcedce99a17
SHA256:	907b6500dba0a048d51a3381fafed7e8b6eb256381f53c6471ebb6d305fddfd4
SHA512:	117ac79355ca79948a050534b625d5bb757640429848a50ddf75fdff3095d03c5db66f74ec01bdc3c8296772b463cdf67963689aca323bedcc059c81ebf70d75
SSDEEP:	6144:RSgQqggOstPSlcWUBzn0Nt/uCkL4iXczObpZz7xVV667fyj7gV+vV:AnqgxuFN0Nt/uC1IczObHxVV6rdV
TLSH:	5094CF10BB90C435F1F711F49AB69668792E3EE15B3450CB62E55AEE5338AE0EC3131B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...3z..3z..3z...5..2z..-(..,z..-(...z.....4z..3z~..z..-(...z..-(..2z..-(..2z..Rich3z.....PE..L....:;`...

File Icon

Icon Hash:	9bf031f096136cf2

Static PE Info

General

Entrypoint:	0x40e770
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x603B3A0D [Sun Feb 28 06:37:01 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:	0bfee496a3ef5b77673533836f065911

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007F095CD0B66Bh
call 00007F095CCFE8D6h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 00430B88h
push 004122B0h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF94h

Instruction
push ebx
push esi
push edi
mov eax, dword ptr [0045D264h]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-70h], 00000000h
mov dword ptr [ebp-04h], 00000000h
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [00401250h]
mov dword ptr [ebp-04h], FFFFFFFEh
jmp 00007F095CCFE8E8h
mov eax, 00000001h
ret
mov esp, dword ptr [ebp-18h]
mov dword ptr [ebp-78h], 000000FFh
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, dword ptr [ebp-78h]
jmp 00007F095CCFEA18h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007F095CCFEA54h
mov dword ptr [ebp-6Ch], eax
push 00000001h
call 00007F095CD0CDCAh
add esp, 04h
test eax, eax
jne 00007F095CCFE8CCh
push 0000001Ch
call 00007F095CCFEA0Ch
add esp, 04h
call 00007F095CD06D14h
test eax, eax
jne 00007F095CCFE8CCh
push 00000010h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [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	0x312a4	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x750000	0x9f90	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1380	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xb2e0	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x328	.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	0x315ce	0x31600	False	0.4520767405063291	data	6.399579325671367	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x33000	0x71a808	0x2b800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.kuxo	0x74e000	0x4b	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pixihu	0x74f000	0x4a	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x750000	0x9f90	0xa000	False	0.6589599609375	data	6.073939237547317	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x7504e0	0x6c8	data	Kyrgyz	Cyrillic
RT_ICON	0x750ba8	0x568	GLS_BINARY_LSB_FIRST	Kyrgyz	Cyrillic
RT_ICON	0x751110	0x10a8	data	Kyrgyz	Cyrillic
RT_ICON	0x7521b8	0x988	dBase III DBT, version number 0, next free block index 40	Kyrgyz	Cyrillic
RT_ICON	0x752b40	0x468	GLS_BINARY_LSB_FIRST	Kyrgyz	Cyrillic
RT_ICON	0x752ff8	0xea8	data	Kyrgyz	Cyrillic
RT_ICON	0x753ea0	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	Kyrgyz	Cyrillic
RT_ICON	0x754748	0x6c8	data	Kyrgyz	Cyrillic
RT_ICON	0x754e10	0x568	GLS_BINARY_LSB_FIRST	Kyrgyz	Cyrillic
RT_ICON	0x755378	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	Kyrgyz	Cyrillic
RT_ICON	0x757920	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	Kyrgyz	Cyrillic
RT_ICON	0x7589c8	0x988	data	Kyrgyz	Cyrillic
RT_ICON	0x759350	0x468	GLS_BINARY_LSB_FIRST	Kyrgyz	Cyrillic
RT_STRING	0x759910	0x42	data	Kyrgyz	Cyrillic
RT_STRING	0x759958	0x4ac	data	Kyrgyz	Cyrillic
RT_STRING	0x759e08	0x188	data	Kyrgyz	Cyrillic
RT_ACCELERATOR	0x759870	0x70	data	Kyrgyz	Cyrillic
RT_ACCELERATOR	0x759830	0x40	data	Kyrgyz	Cyrillic
RT_GROUP_ICON	0x7597b8	0x76	data	Kyrgyz	Cyrillic
RT_GROUP_ICON	0x752fa8	0x4c	data	Kyrgyz	Cyrillic
None	0x7598f0	0xa	data	Kyrgyz	Cyrillic
None	0x7598e0	0xa	data	Kyrgyz	Cyrillic
None	0x759900	0xa	data	Kyrgyz	Cyrillic

Imports

DLL	Import

DLL	Import
KERNEL32.dll	DebugBreakProcess, FindFirstChangeNotificationA, GetNamedPipeHandleStateW, CreateIoCompletionPort, FillConsoleOutputCharacterW, DisableThreadLibraryCalls, TerminateProcess, GetProcessId, VerifyVersionInfoW, EnumDateFormatsW, FindNextFileW, CopyFileExA, BuildCommDCBAndTimeoutsW, VirtualUnlock, WriteProfileStringW, VerifyVersionInfoA, SetProcessPriorityBoost, GetFileType, DeleteFileA, FindNextVolumeMountPointA, OutputDebugStringA, ResetWriteWatch, WriteConsoleInputA, WriteConsoleInputW, GetConsoleTitleW, SetComputerNameExW, GetTimeZoneInformation, LoadLibraryA, GetSystemDirectoryA, GetDriveTypeW, BuildCommDCBAndTimeoutsA, GetShortPathNameW, ActivateActCtx, GetProfileSectionA, DeleteFileW, GetCommandLineW, InterlockedIncrement, InterlockedExchangeAdd, AddRefActCtx, FindResourceA, FormatMessageA, GetModuleFileNameW, CreateJobObjectW, InitializeCriticalSection, SetFirmwareEnvironmentVariableW, GetDllDirectoryA, GetExitCodeThread, WritePrivateProfileStringW, GetConsoleAliasesLengthW, WriteProfileSectionW, AddAtomA, InterlockedDecrement, GetVersionExA, HeapSize, _hwrite, InterlockedExchange, GetStartupInfoW, DisconnectNamedPipe, GetCPInfoExW, GetSystemWow64DirectoryW, SetLastError, GetPrivateProfileIntA, GetConsoleAliasExesW, DebugBreak, EndUpdateResourceW, GetLastError, GetStringTypeExW, DeleteVolumeMountPointA, OpenFileMappingA, SetDefaultCommConfigW, VirtualAlloc, lstrcpyA, TerminateThread, GetACP, lstrcatA, GetConsoleAliasA, _lwrite, GetQueuedCompletionStatus, GetNamedPipeHandleStateA, GetDiskFreeSpaceExW, RemoveVectoredExceptionHandler, WriteConsoleW, VirtualProtect, ReadConsoleOutputW, SetThreadContext, BuildCommDCBA, ReleaseActCtx, GetHandleInformation, GetComputerNameW, WritePrivateProfileSectionW, TryEnterCriticalSection, GetPrivateProfileSectionNamesW, OpenWaitableTimerW, CopyFileW, GetVolumePathNameW, SetConsoleMode, HeapSetInformation, SetComputerNameA, FindNextFileA, SetEvent, UnlockFileEx, GetProcAddress, DeleteTimerQueueTimer, MoveFileA, GlobalAlloc, SetCommMask, SetFileShortNameA, FreeEnvironmentStringsW, GetSystemWindowsDirectoryA, GetProfileStringA, GetConsoleTitleA, GlobalGetAtomNameA, SetComputerNameW, GetConsoleAliasesW, CreateMailslotA, EnumDateFormatsA, GetConsoleOutputCP, MoveFileWithProgressW, GetFileInformationByHandle, SetLocalTime, FoldStringW, CallNamedPipeA, GetConsoleAliasExesLengthW, GetCurrentActCtx, OpenSemaphoreW, GetModuleHandleExA, LoadLibraryW, WriteConsoleOutputCharacterW, GetFileAttributesA, GetTickCount, GetConsoleAliasesLengthA, LocalUnlock, GetFileTime, EnumResourceNamesW, OpenFileMappingW, UnhandledExceptionFilter, GetCompressedFileSizeW, GetThreadPriority, ReadConsoleA, AssignProcessToJobObject, Sleep, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, RaiseException, RtlUnwind, WideCharToMultiByte, GetCommandLineA, GetStartupInfoA, HeapValidate, IsBadReadPtr, SetUnhandledExceptionFilter, GetCurrentProcess, IsDebuggerPresent, GetModuleHandleA, TlsGetValue, GetModuleHandleW, TlsAlloc, TlsSetValue, GetCurrentThreadId, TlsFree, GetOEMCP, GetCPInfo, IsValidCodePage, SetStdHandle, WriteFile, GetConsoleCP, GetConsoleMode, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, ExitProcess, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, GetStdHandle, HeapDestroy, HeapCreate, HeapFree, VirtualFree, HeapAlloc, HeapReAlloc, FlushFileBuffers, OutputDebugStringW, InitializeCriticalSectionAndSpinCount, MultiByteToWideChar, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, LCMapStringA, LCMapStringW, WriteConsoleA, SetFilePointer, CreateFileA, CloseHandle
USER32.dll	CharUpperA
WINHTTP.dll	WinHttpWriteData

Possible Origin

Language of compilation system	Country where language is spoken	Map
Kyrgyz	Cyrillic	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4193.106.191.2464975823196285002706/23/22-17:51:27.182664	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49758	23196	192.168.2.4	193.106.191.246
192.168.2.4193.106.191.2464975823196285028606/23/22-17:51:29.952462	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49758	23196	192.168.2.4	193.106.191.246
193.106.191.246192.168.2.423196497582850353306/23/22-17:51:28.242070	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	23196	49758	193.106.191.246	192.168.2.4

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 17:51:26.879756927 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:26.941302061 CEST	23196	49758	193.106.191.246	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 17:51:26.941448927 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:27.182663918 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:27.244574070 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:27.327807903 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:28.180134058 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:28.242069960 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:28.327898979 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:29.952461958 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:30.016005993 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:30.016064882 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:30.016105890 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:30.016123056 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:30.016146898 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:30.016187906 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:30.016195059 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:30.016225100 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:30.016278982 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:40.401098013 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:40.462614059 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:40.462657928 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:40.462686062 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:40.470408916 CEST	23196	49758	193.106.191.246	192.168.2.4
Jun 23, 2022 17:51:40.641453028 CEST	49758	23196	192.168.2.4	193.106.191.246
Jun 23, 2022 17:51:40.885865927 CEST	49758	23196	192.168.2.4	193.106.191.246

Statistics

No statistics

System Behavior

Analysis Process: VBY5zBdZox.exe PID: **3176**, Parent PID: **2404**

General	
Target ID:	0
Start time:	17:51:07
Start date:	23/06/2022
Path:	C:\Users\user\Desktop\VBY5zBdZox.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\VBY5zBdZox.exe"
Imagebase:	0x400000
File size:	423424 bytes
MD5 hash:	ACC0FB4CB35DF2D49FC609F2E299ED5E
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: 00000000.00000002.314646008.0000000005150000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000000.00000002.314646008.0000000005150000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.314646008.0000000005150000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.305431311.0000000002950000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000000.00000002.305431311.0000000002950000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.305431311.0000000002950000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.239424643.00000000027D0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000003.239424643.00000000027D0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.301936626.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.301936626.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.303381786.0000000002790000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.306212179.0000000002A23000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.240106550.0000000000C15000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.310555251.0000000002D75000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBFCF06	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	6DBFCF06	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	6CA4BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VBY5zBdZox.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF0C78D	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\VBY5zBdZox.exe.log	0	2932	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 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 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	6DF0C907	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	6DBD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DB303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DB303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DB303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6DB303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	22	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	3	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	19	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	8	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	6CA41B4F	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	44	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	2	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	20	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	22	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	16	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	44	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	2	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	28	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	22	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	14	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	42	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	2	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	36	6CA41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6CA41B4F	ReadFile

Disassembly

No disassembly