ID: 679422
Sample Name:
K2Z6KZbzFS.exe
Cookbook: default.jbs
Time: 18:41:06
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

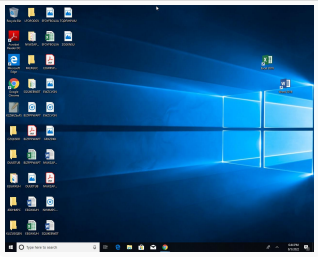
Windows Analysis Report

K2Z6KZbzFS.exe

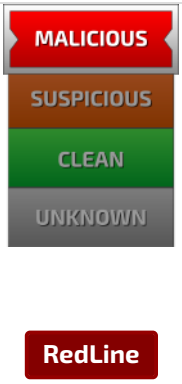
Overview

General Information

Sample Name:	K2Z6KZbzFS.exe
Analysis ID:	679422
MD5:	3333e40e61ff336.
SHA1:	7e314834674c7b..
SHA256:	a4bac13abfd454..
Tags:	exe RedLineStealer
Infos:	



Detection



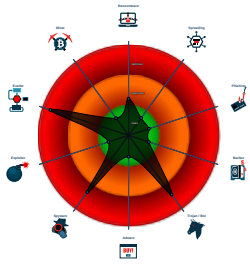
RedLine

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…
- Machine Learning detection for sam…
- Queries sensitive video device infor…
- Queries sensitive disk information (v…
- Found many strings related to Crypt…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- K2Z6KZbzFS.exe (PID: 5724 cmdline: "C:\Users\user\Desktop\K2Z6KZbzFS.exe" MD5: 3333E40E61FF33675C26E7A712A7808D)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "stcontact.top:80"
  ],
  "Bot Id": "AF2",
  "Authorization Header": "4d729a2faecb406a0eb1d6fcf30432fa"
}
```


Yara Signatures

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.492458153.0000000000698000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x1320:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000002.495750268.00000000022F0000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.495750268.00000000022F0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x28ec6:$pat14: , CommandLine: • 0x1d6a8:$v2_1: ListOfProcesses • 0x1ce4b:$v4_3: base64str • 0x1ce18:$v4_4: stringKey • 0x1ce55:$v4_5: BytesToStringConverted • 0x1ce40:$v4_6: FromBase64 • 0x1d363:$v4_8: procName • 0x1afab:$v5_7: RecordHeaderField • 0x1aee7:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.K2Z6KZbzFS.exe.4a20000.6.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.K2Z6KZbzFS.exe.4a20000.6.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x261de:$pat14: , CommandLine: • 0x1a9c0:$v2_1: ListOfProcesses • 0x1a163:$v4_3: base64str • 0x1a130:$v4_4: stringKey • 0x1a16d:$v4_5: BytesToStringConverted • 0x1a158:$v4_6: FromBase64 • 0x1a67b:$v4_8: procName • 0x182c3:$v5_7: RecordHeaderField • 0x181ff:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.2.K2Z6KZbzFS.exe.2204c9e.2.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.K2Z6KZbzFS.exe.2204c9e.2.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x27fde:$pat14: , CommandLine: • 0x1c7c0:$v2_1: ListOfProcesses • 0x1bf63:$v4_3: base64str • 0x1bf30:$v4_4: stringKey • 0x1bf6d:$v4_5: BytesToStringConverted • 0x1bf58:$v4_6: FromBase64 • 0x1c47b:$v4_8: procName • 0x1a0c3:$v5_7: RecordHeaderField • 0x19fff:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.2.K2Z6KZbzFS.exe.4a20000.6.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

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.861356532023883 08/05/22-18:42:26.812831
SID:	2023883
Source Port:	61356
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 91.203.192.233

Timestamp:	192.168.2.591.203.192.23349765802850286 08/05/22-18:42:31.139956

SID:	2850286
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 91.203.192.233 - Destination IP: 192.168.2.5	−
Timestamp:	91.203.192.233192.168.2.580497652850353 08/05/22-18:42:29.205624
SID:	2850353
Source Port:	80
Destination Port:	49765
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.5 - Destination IP: 91.203.192.233	−
Timestamp:	192.168.2.591.203.192.23349765802850027 08/05/22-18:42:27.425256
SID:	2850027
Source Port:	49765
Destination Port:	80
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

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)

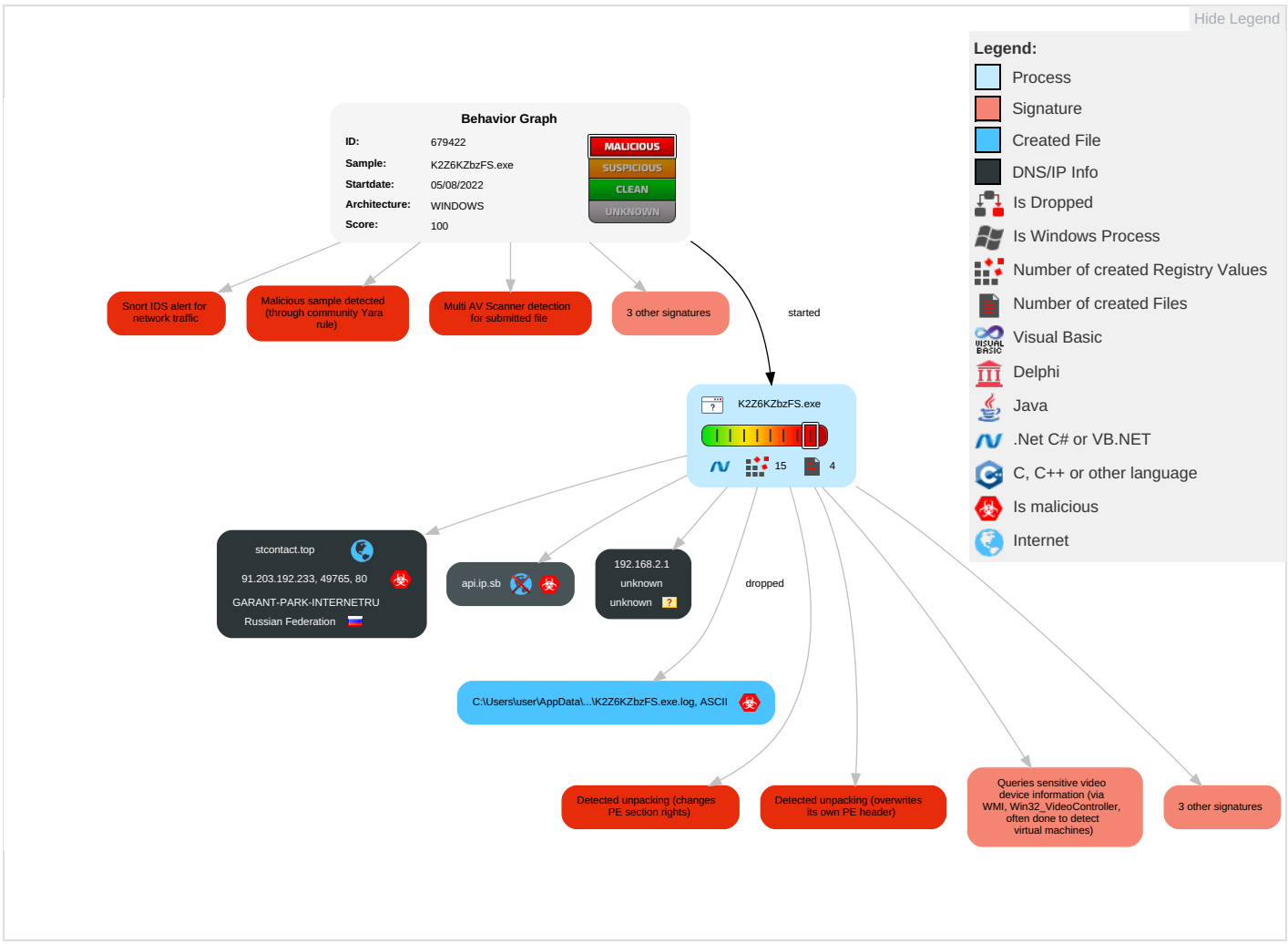
Remote Access Functionality

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 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 1 Security Software Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	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	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	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 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 3 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

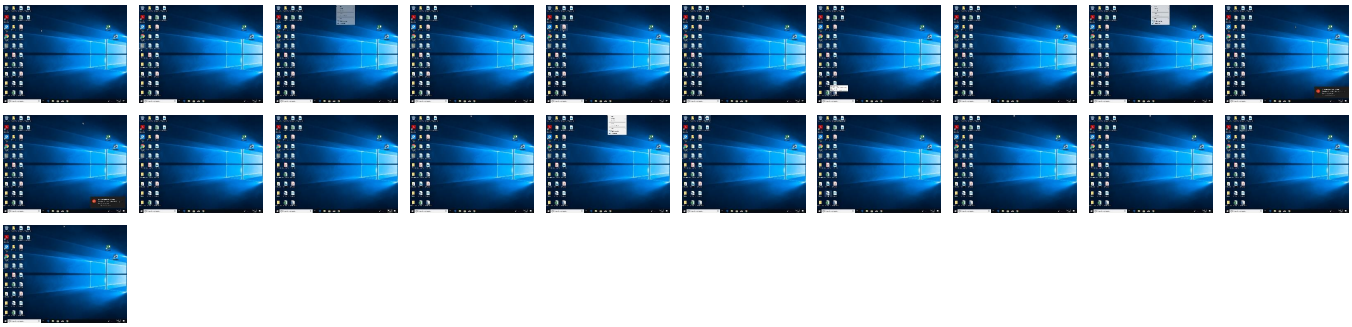
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
K2Z6KZbzFS.exe	34%	Virustotal		Browse
K2Z6KZbzFS.exe	43%	Metadefender		Browse
K2Z6KZbzFS.exe	69%	ReversingLabs	Win32.Trojan.Generic	
K2Z6KZbzFS.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.K2Z6KZbzFS.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1251498		Download File

Domains

Source	Detection	Scanner	Label	Link
stcontact.top	2%	Virustotal		Browse
api.ip.sb	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://www.w3.o	0%	URL Reputation	safe	
http://https://api.ip.sb	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stcontact.top	91.203.192.233	true	true	• 2%, Virustotal, Browse	unknown
api.ip.sb	unknown	unknown	true	• 5%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	K2Z6KZbzFS.exe, 00000000.00000002.499611932.00000000028D8000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501186472.0000000002AA5000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501429760.0000000003557000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501087449.0000000002A7F000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498120552.0000000002755000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.497981876.00000000272D000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498197742.000000000276B000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.503830670.00000000037CD000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499502052.00000000028B2000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501317171.0000000002ABC000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499769083.00000000028EF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/ac/?q=	K2Z6KZbzFS.exe, 00000000.00000002.499611932.00000000028D8000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501186472.0000000002AA5000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501429760.0000000003557000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501087449.0000000002A7F000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498120552.0000000002755000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.497981876.0000000002D2D000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498197742.000000000276B000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.503830670.00000000037CD000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499502052.000000000028B2000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501317171.0000000002ABC000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499769083.00000000028EF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.495750268.00000000022F0000.00000004.08000000.00040000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.506987183.0000000004A20000.00000004.08000000.00040000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501455685.000000000355B000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.495256402.00000000021C3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	K2Z6KZbzFS.exe, 00000000.00000002.499611932.00000000028D8000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501186472.0000000002AA5000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501429760.0000000003557000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501087449.0000000002A7F000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498120552.0000000002755000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.497981876.000000002772D000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498197742.000000000276B000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.503830670.00000000037CD000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499502052.00000000028B2000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501317171.0000000002ABC000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499769083.00000000028EF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high

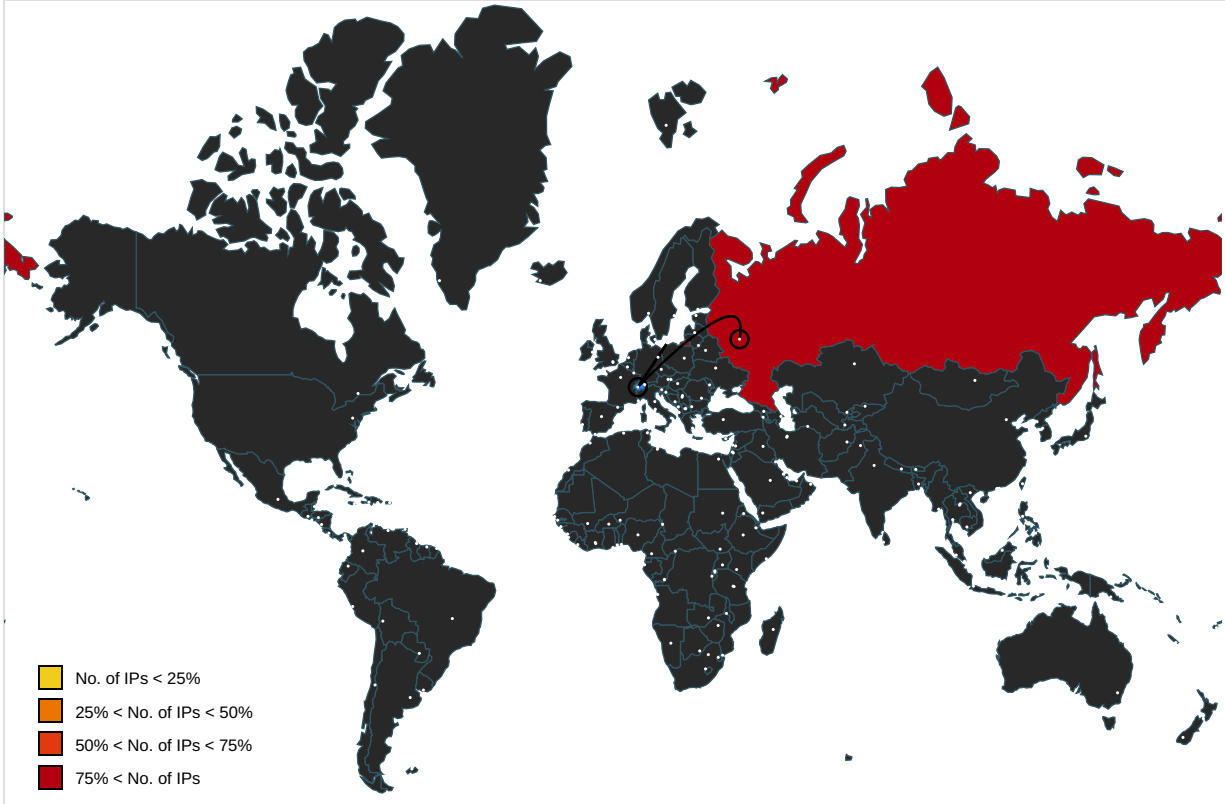
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/search	K2Z6KZbzFS.exe, 00000000.00000002.503830670.00000000037CD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.w3.o	K2Z6KZbzFS.exe, 00000000.00000002.498673203.00000000027D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentif	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Committed	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/fault	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/right/possessproperty	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/sct	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/RegisterResponse	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Cancel	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/SequenceAcknowledgement	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	K2Z6KZbzFS.exe, 00000000.00000002.499611932.00000000028D8000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501186472.0000000002AA5000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501429760.0000000003557000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501087449.0000000002A7F000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498120552.0000000002755000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.497981876.000000002D000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498197742.000000000276B000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.503830670.00000000037CD000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499502052.00000000028B2000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501317171.0000000002ABC000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499769083.00000000028EF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/tlsnego#TLS_Wrap	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2002/12/policy	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Issue	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	K2Z6KZbzFS.exe, 00000000.00000002.499611932.00000000028D8000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501186472.0000000002AA5000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501429760.0000000003557000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501087449.0000000002A7F000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498120552.0000000002755000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.497981876.000000002D000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498197742.000000000276B000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499502052.00000000028B2000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501317171.0000000002ABC000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499769083.00000000028EF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/Issue	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Commit	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContext	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/Issue	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1	K2Z6KZbzFS.exe, 00000000.00000002.496332551.0000000002531000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	K2Z6KZbzFS.exe, 00000000.00000002.499611932.00000000028D8000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501186472.0000000002AA5000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501429760.0000000003557000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501087449.0000000002A7F000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498120552.0000000002755000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.497981876.000000000272D000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.498197742.000000000276B000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.503830670.00000000037CD000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499502052.00000000028B2000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.501317171.0000000002ABC000.00000004.00000800.00020000.00000000.sdmp, K2Z6KZbzFS.exe, 00000000.00000002.499769083.00000000028EF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/spnego	K2Z6KZbzFS.exe, 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.203.192.233	stcontact.top	Russian Federation		47196	GARANT-PARK-INTERNETRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679422
Start date and time: 05/08/202218:41:06	2022-08-05 18:41:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	K2Z6KZbzFS.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:	22
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@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 13.3% (good quality ratio 12.7%) • Quality average: 84.9% • Quality standard deviation: 24.9%
HCA Information:	• Successful, ratio: 89% • 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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 104.26.13.31, 172.67.75.172, 104.26.12.31
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, api.ip.sb.cdn.cloudflare.net, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, licensing.mp.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:42:43	API Interceptor	21x Sleep call for process: K2Z6KZbzFS.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\K2Z6KZbzFS.exe.log

Process:	C:\Users\user\Desktop\K2Z6KZbzFS.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):	7.022503364619211

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:	K2Z6KZbzFS.exe
File size:	409088
MD5:	3333e40e61ff33675c26e7a712a7808d
SHA1:	7e314834674c7bf514f68790a0e88b014e9115a4
SHA256:	a4bac13abfd454b26ddd32a25d87080e7e4bf8b6a9e85e7e91736b3f944565c3
SHA512:	c9774df3adaa867ad7aee060db9451091686725570834eb1a06473d56f051fd40034471c8e76ad9d993b6e43d209bcc3704eed27b9d01a3d208ddd40bead2ec2
SSDEEP:	12288:SAAqMeiD2Fr/cJZtfc9GVM5tQHOBR/F+L412g:xAFDem3EMWPQHOL9X
TLSH:	5294BF01BB90D435E4F752F85A7683A8B52E7EA16B2550CF13D42AEE57386E1EC3130B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P3K.>`K.>`K.>`...`J.>`U..`\.>`U..`..>`I.E`L.>`K.? `..>`U..`t.>`U..`J.>`U..`J.>`RichK.>`.....PE..L.....a...

File Icon

Icon Hash:	aed8ae9ecea62aa2

Static PE Info

General

Entrypoint:	0x40b2b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x61810712 [Tue Nov 2 09:38:26 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:	dc0513b2e8e866ceee30009dd51093dc

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007F3D28CC157Bh
call 00007F3D28CB6856h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 00430E70h
push 0040EE20h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF94h
push ebx
push esi
push edi
mov eax, dword ptr [0045CB94h]
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 [00401208h]
mov dword ptr [ebp-04h], FFFFFFFEh
jmp 00007F3D28CB6868h
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 00007F3D28CB6998h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007F3D28CB69D4h
mov dword ptr [ebp-6Ch], eax
push 00000001h
call 00007F3D28CC2CEAh
add esp, 04h
test eax, eax
jne 00007F3D28CB684Ch
push 0000001Ch
call 00007F3D28CB698Ch
add esp, 04h
call 00007F3D28CBEB84h
test eax, eax
jne 00007F3D28CB684Ch
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	0x315d4	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6a000	0x69c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1350	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	0x8c60	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x2f4	.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	0x3174c	0x31800	False	0.3750542534722222	data	5.748787816924977	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x33000	0x33d68	0x2ae00	False	0.9716483691690962	data	7.941676038288415	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.gay	0x67000	0x400	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.gayeta	0x68000	0x400	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.kux	0x69000	0x96	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x6a000	0x69c8	0x6a00	False	0.7162072523584906	data	6.185660414732063	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6a330	0x6c8	data	Korean	North Korea
RT_ICON	0x6a330	0x6c8	data	Korean	South Korea
RT_ICON	0x6a9f8	0x568	GLS_BINARY_LSB_FIRST	Korean	North Korea
RT_ICON	0x6a9f8	0x568	GLS_BINARY_LSB_FIRST	Korean	South Korea
RT_ICON	0x6af60	0x10a8	data	Korean	North Korea
RT_ICON	0x6af60	0x10a8	data	Korean	South Korea
RT_ICON	0x6c008	0x988	dBase III DBT, version number 0, next free block index 40	Korean	North Korea
RT_ICON	0x6c008	0x988	dBase III DBT, version number 0, next free block index 40	Korean	South Korea
RT_ICON	0x6c990	0x468	GLS_BINARY_LSB_FIRST	Korean	North Korea
RT_ICON	0x6c990	0x468	GLS_BINARY_LSB_FIRST	Korean	South Korea
RT_ICON	0x6ce48	0x25a8	data	Korean	North Korea
RT_ICON	0x6ce48	0x25a8	data	Korean	South Korea

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6f3f0	0x10a8	data	Korean	North Korea
RT_ICON	0x6f3f0	0x10a8	data	Korean	South Korea
RT_STRING	0x706d0	0xac	data	Korean	North Korea
RT_STRING	0x706d0	0xac	data	Korean	South Korea
RT_STRING	0x70780	0x246	data	Korean	North Korea
RT_STRING	0x70780	0x246	data	Korean	South Korea
RT_ACCELERATOR	0x70530	0x60	data	Korean	North Korea
RT_ACCELERATOR	0x70530	0x60	data	Korean	South Korea
RT_ACCELERATOR	0x704c0	0x70	data	Korean	North Korea
RT_ACCELERATOR	0x704c0	0x70	data	Korean	South Korea
RT_GROUP_ICON	0x70498	0x22	data	Korean	North Korea
RT_GROUP_ICON	0x70498	0x22	data	Korean	South Korea
RT_GROUP_ICON	0x6cdf8	0x4c	data	Korean	North Korea
RT_GROUP_ICON	0x6cdf8	0x4c	data	Korean	South Korea
RT_VERSION	0x70590	0x13c	data	Korean	North Korea
RT_VERSION	0x70590	0x13c	data	Korean	South Korea

Imports

DLL	Import
KERNEL32.dll	VerifyVersionInfoW, WriteConsoleInputA, EnumDateFormatsW, CopyFileExW, DnsHostnameToComputerNameW, FindNextFileW, ReadConsoleOutputCharacterW, SetConsoleActiveScreenBuffer, LockFile, GetProfileSectionA, QueryDosDeviceW, RequestWakeupLatency, GetProcessPriorityBoost, GetDriveTypeW, GlobalGetAtomNameA, DeleteFileW, FindNextVolumeMountPointW, TlsSetValue, SizeofResource, WriteConsoleInputW, GetConsoleTitleW, GetComputerNameExW, OpenEventA, CallNamedPipeA, GetModuleHandleW, GetSystemDirectoryA, GetDriveTypeA, BuildCommDCBAndTimeoutsA, GetProcAddress, GetModuleHandleA, GetShortPathNameA, DeleteFileA, GetCommandLineW, InterlockedIncrement, InterlockedExchange, CopyFileW, CreateActCtxW, FormatMessageW, EnterCriticalSection, FindNextVolumeA, CreateIoCompletionPort, LoadLibraryA, CreateNamedPipeW, GetSystemDefaultLangID, GetConsoleAliasesLengthA, WriteProfileSectionW, AddAtomW, InterlockedDecrement, HeapFree, _hwrite, InterlockedCompareExchange, GetStartupInfoW, CreateMailslotW, GetCPInfoExW, GetSystemWow64DirectoryW, GetLastError, GetPrivateProfileIntW, GetConsoleAliasExesLengthW, WaitForDebugEvent, SetLastError, LoadLibraryW, VerifyVersionInfoA, VirtualAlloc, GetACP, lstrcpyA, GetConsoleAliasA, GetDiskFreeSpaceExA, TerminateProcess, EnumResourceLanguagesA, SetConsoleTextAttribute, GlobalGetAtomNameW, CreateJobSet, MoveFileW, lstrcpynA, EnumSystemLocalesA, GetPrivateProfileSectionNamesW, GetFileAttributesW, FileTimeToSystemTime, GetTapeParameters, lstrcmpW, SetEvent, MoveFileA, CreateMutexA, FindResourceW, GetCommState, FormatMessageA, CreateFiber, GetConsoleFontSize, LocalAlloc, SetFileShortNameA, lstrcpyW, HeapLock, GetFileAttributesA, SetCalendarInfoW, GetSystemWindowsDirectoryW, GetConsoleAliasesW, EnumDateFormatsExW, GetComputerNameW, GetPrivateProfileStructW, _hread, LocalFlags, OpenWaitableTimerA, EnumResourceNamesW, CreateFileMappingW, SetProcessShutdownParameters, lstrcpynW, GetFullPathNameW, WriteConsoleW, FreeUserPhysicalPages, WriteConsoleOutputCharacterW, OpenJobObjectW, CreateFileW, SetCurrentDirectoryA, GlobalWire, GetFileInformationByHandle, GetProfileSectionW, CommConfigDialogW, CreateFileA, GetDefaultCommConfigA, LocalFree, Sleep, InitializeCriticalSection, DeleteCriticalSection, LeaveCriticalSection, RaiseException, RtlUnwind, WideCharToMultiByte, GetCommandLineA, GetStartupInfoA, HeapValidate, IsBadReadPtr, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetModuleFileNameW, GetCurrentProcess, IsDebuggerPresent, TlsGetValue, TlsAlloc, GetCurrentThreadId, TlsFree, GetOEMCP, GetCPInfo, IsValidCodePage, SetFilePointer, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, ExitProcess, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetStdHandle, GetFileType, HeapDestroy, HeapCreate, VirtualFree, WriteFile, HeapAlloc, HeapSize, HeapReAlloc, FlushFileBuffers, GetConsoleCP, GetConsoleMode, DebugBreak, OutputDebugStringA, OutputDebugStringW, InitializeCriticalSectionAndSpinCount, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, CloseHandle
USER32.dll	CharToOemBuffW, CharUpperW, GetMessageTime, LoadMenuA
ADVAPI32.dll	AbortSystemShutdownW

Possible Origin

Language of compilation system	Country where language is spoken	Map
Korean	North Korea	
Korean	South Korea	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8.8613565 32023883 08/05/22-18:42:26.812831	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	61356	53	192.168.2.5	8.8.8.8
192.168.2.591.203.192.23 349765802850286 08/05/22-18:42:31.139956	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49765	80	192.168.2.5	91.203.192.233
91.203.192.233192.168.2. 580497652850353 08/05/22-18:42:29.205624	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	80	49765	91.203.192.233	192.168.2.5
192.168.2.591.203.192.23 349765802850027 08/05/22-18:42:27.425256	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49765	80	192.168.2.5	91.203.192.233

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 18:42:27.021713018 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:27.116420031 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:27.116735935 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:27.425256014 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:27.499471903 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:27.673376083 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:27.770121098 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:29.052510023 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:29.138519049 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:29.205624104 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:29.270282030 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:31.139955997 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:31.202965021 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:31.275098085 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:31.275167942 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:31.275218964 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:31.275249958 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:31.275278091 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:31.275337934 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:31.275342941 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:31.275413990 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:31.275490046 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:47.214340925 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:47.309964895 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.310009956 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.310075045 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:47.310091019 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.310291052 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.310446978 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.310657024 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.310667992 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.310811043 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.310852051 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.402631998 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.402652979 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.474572897 CEST	80	49765	91.203.192.233	192.168.2.5
Aug 5, 2022 18:42:47.584464073 CEST	49765	80	192.168.2.5	91.203.192.233
Aug 5, 2022 18:42:47.780308962 CEST	49765	80	192.168.2.5	91.203.192.233

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 18:42:26.812830925 CEST	61356	53	192.168.2.5	8.8.8.8
Aug 5, 2022 18:42:27.002224922 CEST	53	61356	8.8.8.8	192.168.2.5
Aug 5, 2022 18:42:32.649317026 CEST	59661	53	192.168.2.5	8.8.8.8
Aug 5, 2022 18:42:32.677098036 CEST	57278	53	192.168.2.5	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 18:42:26.812830925 CEST	192.168.2.5	8.8.8.8	0xb2ac	Standard query (0)	stcontact.top	A (IP address)	IN (0x0001)
Aug 5, 2022 18:42:32.649317026 CEST	192.168.2.5	8.8.8.8	0x83cb	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Aug 5, 2022 18:42:32.677098036 CEST	192.168.2.5	8.8.8.8	0x1080	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 18:42:27.002224922 CEST	8.8.8.8	192.168.2.5	0xb2ac	No error (0)	stcontact.top		91.203.192.233	A (IP address)	IN (0x0001)
Aug 5, 2022 18:42:32.670217991 CEST	8.8.8.8	192.168.2.5	0x83cb	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 18:42:32.699858904 CEST	8.8.8.8	192.168.2.5	0x1080	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

Statistics

No statistics

System Behavior

Analysis Process: K2Z6KZbzFS.exe PID: **5724**, Parent PID: **5652**

General

Target ID:	0
Start time:	18:42:05
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\K2Z6KZbzFS.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\K2Z6KZbzFS.exe"
Imagebase:	0x400000
File size:	409088 bytes
MD5 hash:	3333E40E61FF33675C26E7A712A7808D
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: 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.496646256.0000000002595000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.492458153.0000000000698000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.495750268.00000000022F0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.495750268.00000000022F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.408726056.0000000000704000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.491785643.0000000000610000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.491785643.0000000000610000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.490903331.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.490903331.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.506987183.0000000004A20000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000002.506987183.0000000004A20000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.408078605.0000000002120000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000003.408078605.0000000002120000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.495256402.00000000021C3000.00000004.00000800.00020000.00000000.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	6D7DCF06	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	6D7DCF06	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	6C62BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\K2Z6KZbzFS.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DAEC78D	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\K2Z6KZbzFS.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 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	6DAEC907	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	6D7B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D7103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D7103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D7103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D7103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C621B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\Desktop\EEGWXUHVUG.docx	unknown	4096	success or wait	1	6C621B4F	ReadFile
C:\Users\user\Desktop\EEGWXUHVUG.docx	unknown	1022	end of file	1	6C621B4F	ReadFile
C:\Users\user\Desktop\EEGWXUHVUG.docx	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\Desktop\NVWZAPQSQL.docx	unknown	4096	success or wait	1	6C621B4F	ReadFile
C:\Users\user\Desktop\NVWZAPQSQL.docx	unknown	1022	end of file	1	6C621B4F	ReadFile
C:\Users\user\Desktop\NVWZAPQSQL.docx	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.docx	unknown	4096	success or wait	1	6C621B4F	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.docx	unknown	1022	end of file	1	6C621B4F	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.docx	unknown	4096	end of file	1	6C621B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\EEGWXUHVUG.docx	unknown	4096	success or wait	1	6C621B4F	ReadFile
C:\Users\user\Documents\EEGWXUHVUG.docx	unknown	1022	end of file	1	6C621B4F	ReadFile
C:\Users\user\Documents\EEGWXUHVUG.docx	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\Documents\NVWZAPQSQL.docx	unknown	4096	success or wait	1	6C621B4F	ReadFile
C:\Users\user\Documents\NVWZAPQSQL.docx	unknown	1022	end of file	1	6C621B4F	ReadFile
C:\Users\user\Documents\NVWZAPQSQL.docx	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\Documents\SQSJKEBWDT.docx	unknown	4096	success or wait	1	6C621B4F	ReadFile
C:\Users\user\Documents\SQSJKEBWDT.docx	unknown	1022	end of file	1	6C621B4F	ReadFile
C:\Users\user\Documents\SQSJKEBWDT.docx	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	86	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	3	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	86	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	10	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	171	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	2	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	14	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	86	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	172	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	2	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	36	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	41	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	18	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	172	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	2	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	36	6C621B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6C621B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly