ID: 736967
Sample Name: StZAEFSb2j.exe
Cookbook: default.jbs
Time: 12:43:40
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

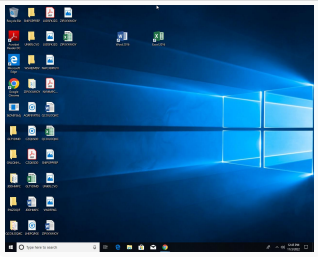
Windows Analysis Report

StZAEFSb2j.exe

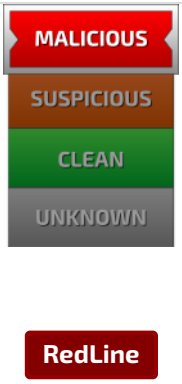
Overview

General Information

Sample Name:	StZAEFSb2j.exe
Analysis ID:	736967
MD5:	c71616e2b7cedf…
SHA1:	896a4c41792c73..
SHA256:	4a9f8a3b847fa9d.
Tags:	exe RedLineStealer
Infos:	



Detection



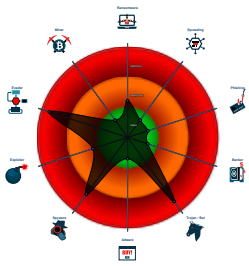
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Tries to steal Crypto Currency Walle…
- .NET source code references suspic…
- Uses known network protocols on n…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- StZAEFSb2j.exe (PID: 780 cmdline: C:\Users\user\Desktop\StZAEFSb2j.exe MD5: C71616E2B7CEDF9FC8E2CA6F6929ABDF)
  - aspnet_compiler.exe (PID: 1592 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - conhost.exe (PID: 6120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "194.55.186.201:6008"
  ],
  "Bot Id": "xxxPROFxxx"
}
```

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
00000000.00000002.321721404.00000000042B9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.321721404.00000000042B9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.321721404.00000000042B9000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_f54632eb	unknown	unknown	• 0x535ca:$a4: get_ScannedWallets • 0x6b1ea:$a4: get_ScannedWallets • 0x52428:$a5: get_ScanTelegram • 0x6a048:$a5: get_ScanTelegram • 0x5324e:$a6: get_ScanGeckoBrowsersPaths • 0x6ae6e:$a6: get_ScanGeckoBrowsersPaths • 0x5106a:$a7: <Processes>k__BackingField • 0x68c8a:$a7: <Processes>k__BackingField • 0x4ef7c:$a8: <GetWindowsVersion>g__HKLM_GetString\|11_0 • 0x66b9c:$a8: <GetWindowsVersion>g__HKLM_GetString|11_0 • 0x5099e:$a9: <ScanFTP>k__BackingField • 0x685be:$a9: <ScanFTP>k__BackingField
00000001.00000000.316565039.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000000.316565039.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.StZAEFSb2j.exe.42f9000.5.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.StZAEFSb2j.exe.42f9000.5.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.StZAEFSb2j.exe.42f9000.5.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0xe68a:$u7: RunPE • 0x11d41:$u8: DownloadAndEx • 0x7330:$pat14: , CommandLine: • 0x11279:$v2_1: ListOfProcesses • 0xe88b:$v2_2: get_ScanVPN • 0xe92e:$v2_2: get_ScanFTP • 0xf61e:$v2_2: get_ScanDiscord • 0x1060c:$v2_2: get_ScanSteam • 0x10628:$v2_2: get_ScanTelegram • 0x106ce:$v2_2: get_ScanScreen • 0x11416:$v2_2: get_ScanChromeBrowsersPaths • 0x1144e:$v2_2: get_ScanGeckoBrowsersPaths • 0x11709:$v2_2: get_ScanBrowsers • 0x117ca:$v2_2: get_ScannedWallets • 0x117f0:$v2_2: get_ScanWallets • 0x11810:$v2_3: GetArguments • 0xfed9:$v2_4: VerifyUpdate • 0x147f6:$v2_4: VerifyUpdate • 0x11bca:$v2_5: VerifyScanRequest • 0x112c6:$v2_6: GetUpdates • 0x147d7:$v2_6: GetUpdates
0.2.StZAEFSb2j.exe.42f9000.5.unpack	Windows_Trojan_RedLineStealer_f54632eb	unknown	unknown	• 0x117ca:$a4: get_ScannedWallets • 0x10628:$a5: get_ScanTelegram • 0x1144e:$a6: get_ScanGeckoBrowsersPaths • 0xf26a:$a7: <Processes>k__BackingField • 0xd17c:$a8: <GetWindowsVersion>g__HKLM_GetString\|11_0 • 0xeb9e:$a9: <ScanFTP>k__BackingField
1.0.aspnet_compiler.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 7 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query to a .tk domain - Likely Hostile - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.48.8.8.856572532012811 11/03/22-12:44:38.337914
SID:	2012811
Source Port:	56572
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN Windows executable base64 encoded - Source IP: 50.115.174.192 - Destination IP: 192.168.2.4 −

Timestamp:	50.115.174.192192.168.2.4443496952018856 11/03/22-12:44:39.556293
SID:	2018856
Source Port:	443
Destination Port:	49695
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Windows executable base64 encoded - Source IP: 50.115.174.192 - Destination IP: 192.168.2.4 −

Timestamp:	50.115.174.192192.168.2.4443496962018856 11/03/22-12:44:40.820043
SID:	2018856
Source Port:	443
Destination Port:	49696
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Uses known network protocols on non-standard ports

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

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)

Anti Debugging

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

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)

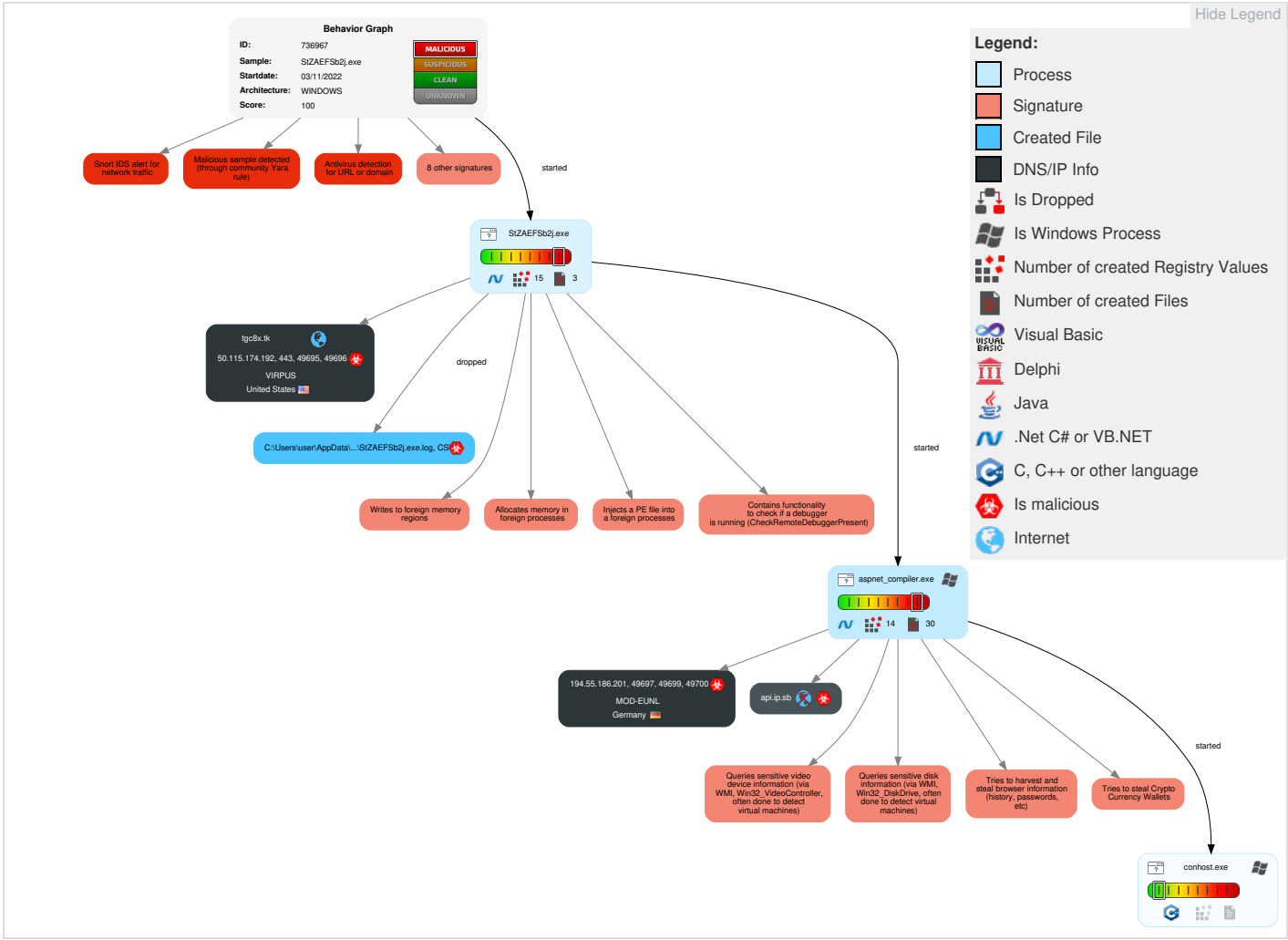
Remote Access Functionality

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	3 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	3 3 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 2 Process Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 5 1 Virtualization/Sandbox Evasion	Security Account Manager	2 5 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Software Packing	Cached Domain Credentials	1 2 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

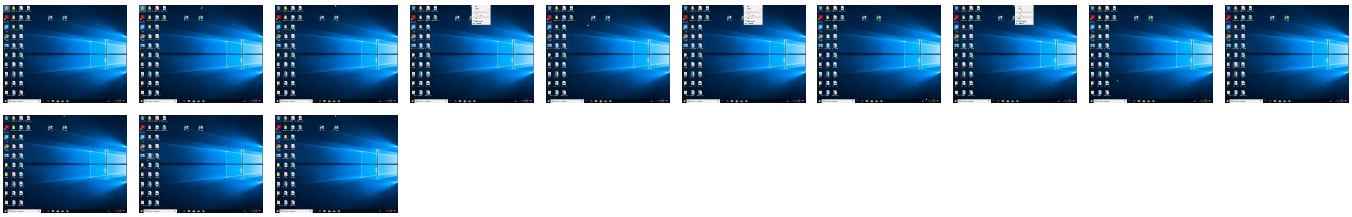
Behavior Graph



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
StZAEFSb2j.exe	34%	ReversingLabs	ByteCode-MSIL.Infostealer.Generic	
StZAEFSb2j.exe	26%	Virustotal		Browse
StZAEFSb2j.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.aspnet_compiler.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1234943		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Endpoint/CheckConnectResponse	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/EnvironmentSettings	0%	URL Reputation	safe	
http://tempuri.org/t_	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/CheckConnect	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/VerifyUpdateResponse	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/SetEnviron	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/SetEnvironment	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	URL Reputation	safe	
http://tgc8x.tk	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetUpdates	0%	URL Reputation	safe	
http://https://api.ipify.orgcookies//settinString.Removeg	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/GetUpdatesResponse	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/VerifyUpdate	0%	URL Reputation	safe	
http://https://tgc8x.tk/tt/BLACKDEV.txt	100%	Avira URL Cloud	phishing	
http://https://tgc8x.tk4	0%	Avira URL Cloud	safe	
http://tempuri.org/0	0%	URL Reputation	safe	
http://https://tgc8x.tkD8	0%	Avira URL Cloud	safe	
http://194.55.186.201:6008	0%	Avira URL Cloud	safe	
194.55.186.201:6008	0%	Avira URL Cloud	safe	
http://194.55.186.201:	0%	Avira URL Cloud	safe	
http://https://tgc8x.tk/tt/lamb.txt	100%	Avira URL Cloud	phishing	
http://https://tgc8x.tk	0%	Avira URL Cloud	safe	
http://194.55.186.201:6008/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tgc8x.tk	50.115.174.192	true	true		unknown
api.ip.sb	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://tgc8x.tk/tt/BLACKDEV.txt	true	• Avira URL Cloud: phishing	unknown
194.55.186.201:6008	true	• Avira URL Cloud: safe	unknown
http://https://tgc8x.tk/tt/lamb.txt	true	• Avira URL Cloud: phishing	unknown
http://194.55.186.201:6008/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

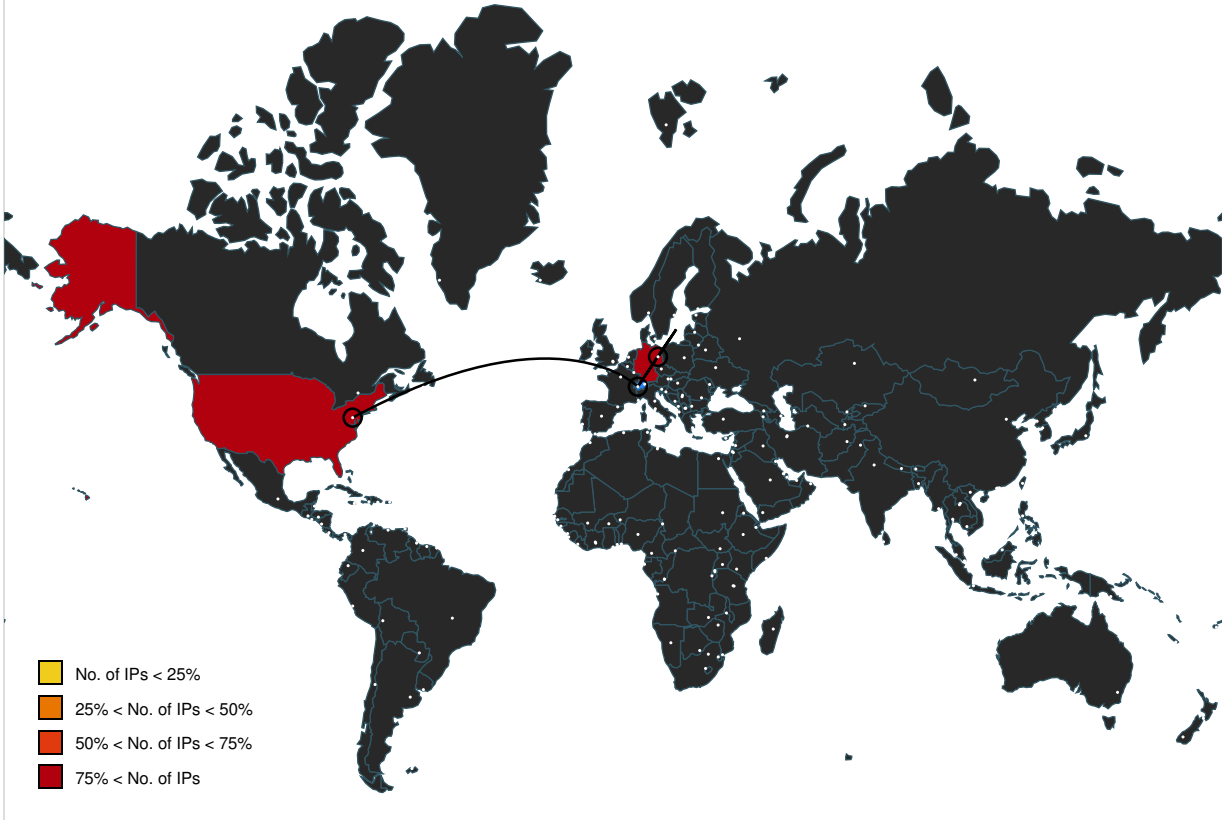
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ipinfo.io/ip%appdata%	StZAEFSb2j.exe, 00000000.00000002.321721404.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000000.316565039.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	aspnet_compiler.exe, 00000001.00000003.399325054.00000000080B1000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.430638568.0000000004243000.00000004.00000800.00020000.00000000.sdmp, tmpB95.tmp.1.dr, tmpD30.tmp.1.dr, tmpC92.tmp.1.dr, tmpC33.tmp.1.dr, tmpCC2.tmp.1.dr, tmpDBF.tmp.1.dr, tmpBF4.tmp.1.dr, tmpEBC.tmp.1.dr, tmpE8C.tmp.1.dr, tmpF80C.tmp.1.dr, tmpD60.tmp.1.dr, tmpE2D.tmp.1.dr	false		high
http://https://duckduckgo.com/ac/?q=	tmpE2D.tmp.1.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	aspnet_compiler.exe, 00000001.00000003.399325054.00000000080B1000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.430638568.0000000004243000.00000004.00000800.00020000.00000000.sdmp, tmpB95.tmp.1.dr, tmpD30.tmp.1.dr, tmpC92.tmp.1.dr, tmpC33.tmp.1.dr, tmpCC2.tmp.1.dr, tmpDBF.tmp.1.dr, tmpBF4.tmp.1.dr, tmpEBC.tmp.1.dr, tmpE8C.tmp.1.dr, tmpF80C.tmp.1.dr, tmpD60.tmp.1.dr, tmpE2D.tmp.1.dr	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Endpoint/CheckConnectResponse	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.datacontract.org/2004/07/	aspnet_compiler.exe, 00000001.00000002.416441450.000000000309B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/EnvironmentSettings	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/t_	aspnet_compiler.exe, 00000001.00000002.415555604.0000000002FAF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	StZAEFSb2j.exe, 00000000.00000002.321721404.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000000.316565039.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	aspnet_compiler.exe, 00000001.00000003.399325054.00000000080B1000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.430638568.0000000004243000.00000004.00000800.00020000.00000000.sdmp, tmpB95.tmp.1.dr, tmpD30.tmp.1.dr, tmpC92.tmp.1.dr, tmpC33.tmp.1.dr, tmpCC2.tmp.1.dr, tmpDBF.tmp.1.dr, tmpBF4.tmp.1.dr, tmpEBC.tmp.1.dr, tmpE8C.tmp.1.dr, tmpF80C.tmp.1.dr, tmpD60.tmp.1.dr, tmpE2D.tmp.1.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	tmpE2D.tmp.1.dr	false		high
http://schemas.xmlsoap.org/soap/envelope/D	aspnet_compiler.exe, 00000001.00000002.415555604.0000000002FAF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/CheckConnect	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	aspnet_compiler.exe, 00000001.00000003.399325054.00000000080B1000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.430638568.0000000004243000.00000004.00000800.00020000.00000000.sdmp, tmpB95.tmp.1.dr, tmpD30.tmp.1.dr, tmpC92.tmp.1.dr, tmpC33.tmp.1.dr, tmpCC2.tmp.1.dr, tmpDBF.tmp.1.dr, tmpBF4.tmp.1.dr, tmpEBC.tmp.1.dr, tmpE8C.tmp.1.dr, tmpF80C.tmp.1.dr, tmpD60.tmp.1.dr, tmpE2D.tmp.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobe.c/g	aspnet_compiler.exe, 00000001.00000003.4 12663066.0000000008CB2000.00000004.00000 800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000003.412625368.0000000008CB0 000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000003.41257 5103.0000000008CB0000.00000004.00000800. 00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000003.402236725.0000000008CA1000. 00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000003.412702825 .000000000152D000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://tgc8x.tk4	StZAEFSb2j.exe, 00000000.00000002.320562 361.0000000002B54000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/VerifyUpdateResponse	aspnet_compiler.exe, 00000001.00000002.4 14887349.0000000002F61000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/SetEnviron	aspnet_compiler.exe, 00000001.00000002.4 16745991.00000000030DB000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	aspnet_compiler.exe, 00000001.00000003.3 99325054.00000000080B1000.00000004.00000 800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.430638568.0000000004243 000.00000004.00000800.00020000.00000000.sdmp, tmpB95.tmp.1.dr, tmpD30.tmp.1.dr, tmpC92.tmp.1.dr, tmpC33.tmp.1.dr, tmpCC2.tmp.1.dr, tmpDBF.tmp.1.dr, tmpBF4.tmp.1.dr, tmpEBC.tmp.1.dr, tmpE8C.tmp.1.dr, tmpF80C.tmp.1.dr, tmpD60.tmp.1.dr, tmpE2D.tmp.1.dr	false		high
http://tempuri.org/Endpoint/SetEnvironment	aspnet_compiler.exe, 00000001.00000002.4 16745991.00000000030DB000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/SetEnvironmentResponse	aspnet_compiler.exe, 00000001.00000002.4 14887349.0000000002F61000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tgc8x.tk	StZAEFSb2j.exe, 00000000.00000002.320604 810.0000000002B5D000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://tgc8x.tkD8	StZAEFSb2j.exe, 00000000.00000002.321171 028.0000000002BC4000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://194.55.186.201:6008	aspnet_compiler.exe, 00000001.00000002.4 15787658.0000000002FF2000.00000004.00000 800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61 000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/Endpoint/GetUpdates	aspnet_compiler.exe, 00000001.00000002.4 15787658.0000000002FF2000.00000004.00000 800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.415555604.0000000002FAF 000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.41488 7349.0000000002F61000.00000004.00000800. 00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.415687042.0000000002FDA000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	tmpE2D.tmp.1.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	aspnet_compiler.exe, 00000001.00000003.3 99325054.00000000080B1000.00000004.00000 800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.430638568.0000000004243 000.00000004.00000800.00020000.00000000.sdmp, tmpB95.tmp.1.dr, tmpD30.tmp.1.dr, tmpC92.tmp.1.dr, tmpC33.tmp.1.dr, tmpCC2.tmp.1.dr, tmpDBF.tmp.1.dr, tmpBF4.tmp.1.dr, tmpEBC.tmp.1.dr, tmpE8C.tmp.1.dr, tmpF80C.tmp.1.dr, tmpD60.tmp.1.dr, tmpE2D.tmp.1.dr	false		high
http://https://api.ipify.orgcookies//settinString.Removeg	StZAEFSb2j.exe, 00000000.00000002.321721 404.00000000042B9000.00000004.00000800.0 0020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000000.316565039.00000000 00402000.00000040.00000400.00020000.0000 0000.sdmp	true	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing	aspnet_compiler.exe, 00000001.00000002.4 14887349.0000000002F61000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://194.55.186.201:	aspnet_compiler.exe, 00000001.00000002.4 16745991.00000000030DB000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Endpoint/GetUpdatesResponse	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/VerifyUpdate	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/0	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://tgc8x.tk	StZAEFSb2j.exe, 00000000.00000002.320164097.0000000002B46000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	StZAEFSb2j.exe, 00000000.00000002.320164097.0000000002B46000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	tmpE2D.tmp.1.dr	false		high
http://schemas.xmlsoap.org/soap/actor/next	aspnet_compiler.exe, 00000001.00000002.414887349.0000000002F61000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.115.174.192	tgc8x.tk	United States		32875	VIRPUS	true
194.55.186.201	unknown	Germany		39855	MOD-EUNL	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736967
Start date and time:	2022-11-03 12:43:40 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	StZAEFSb2j.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
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@4/26@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.67.75.172, 104.26.13.31, 104.26.12.31
- Excluded domains from analysis (whitelisted): api.ip.sb.cdn.cloudflare.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
12:44:40	API Interceptor	1x Sleep call for process: StZAEFSb2j.exe modified
12:45:08	API Interceptor	74x Sleep call for process: aspnet_compiler.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\StZAEFSb2j.exe.log

Process:	C:\Users\user\Desktop\StZAEFSb2j.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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,"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,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\aspnet_compiler.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2412
Entropy (8bit):	5.341108361394489
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKdHKBSTHaAHKzvRYHKhQnoPtHoxHImHKhBHKoHaHZHAHjHKoLHG1V:vq5qXAqdqslqzJYqhQnoPtIxHbqLqo67
MD5:	5D4B4A6BFACB854E7F2C4ADB625D1F71
SHA1:	FC542A0C19178B77638600EA36378BA3F64BC677
SHA-256:	170BA6EFCB3905EA4870D3771B9F38F64D079F8E3871032023B5EB6CAEF618B0
SHA-512:	BBC9AA745C2F44B5572EFA2B15FA45494E786F69339FC9ED8C52AAF7DA8AB3D48C24EF4106850892B9A711BA968DE71F11321CD1CAFE2F745A9CA7BAE4F197EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral,

C:\Users\user\AppData\Local\Temp\tmp1881.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.687055908915499
Encrypted:	false
SSDEEP:	24:X3rfasg2Tpd/zBJY+q9FZP0DJR6BdqWD5gB8H36D6jXLiUk2ZTV:X+52L/dJYBjYJRoddD5C8HqD8ZDZTV
MD5:	94EDB575C55407C555A3F710DF2A8CB3
SHA1:	3AB8DF4B92C320D7D4C661EAB608E24B43F3DD13
SHA-256:	DD3A4A93D60E4B7840557A44DAAF77F6B6F85032C7DD5FB10BE54C07B0E1E261
SHA-512:	F8F78D10AE19735413AF11F0C8DAC41644479D345DC6B300412DEDA9779A01DDFC7150FBFD54F2582A0DF8524B7E507886DBC49E59B084320017E9E64FC8DBF A
Malicious:	false
Preview:	JDDHMPCDUJFORBKGTIFQHFPQNEKFAIHGBDYZBWNZMVTSZXTGRUOCZPQRXMGXBNMAHGODCTVNAHQHZMJYIYXLTVDMEAVEXSWFQCDVPRSSLREITY MWHUXVVKLPJXQJOHYPAVYXSIMBBOTIWYDKNCDVKZZMEIFEDNNXHAHMYLPOUGNKMPZVDEQRUPZBQCKZDQINFECCUZINROAFGLIAMVWHXPPXOWZM WTITWBJFIENEHRXRHRPVUAIUAJUYDBBSQQMTJJXOAAMHVKJEOIQRSNKKQSGCHAUKUYPJEBZIGZTVKUXZEQOUSZPQBHKFHECDNFGTGIDHSJFVLA KZPDYVJVWECRIKKUCCFNNHBLBFCJEKSUZTITTTLQVOHKFHXFIIYDOZNAIBCDIRXJAYKHCOEXBOGSGEGGQEMHFXIZREOFZJSAFXTGSSZLVKYOAN MZNPNESDZMFYWTZHIKUSMZXACWZEIMGTFRSZCGICPOSTZRECQYWZECQVLAWXESWPCDXLHIMJHSZJSDAXNXHETAWLZDXTZAPKBHSMKMYYGVSJCU IJSIFUHHMPIRBASPUOUXKKPQCECQBBZUSIXEOXLFFSQIFCTAIRASCMWEHFOXGEJRXFGJODUTKITHEAKFFJQTQNWWKXXDELWDHHEDWUTMSLXQJP VGOBKELYSRBQFYKXFHWGSCVLTCFKOEJMLUXIZVDPFHXHTSMTDRTVCNLISGJFVQRUTMZDYPUYBAEASZCSEUVHWRIQDEJIZQQHJNTIIICFMMPVLX OIVTPCTDKFPDVWXSBXZDXFUMBJTJMKOOHIMIOAKEJSIDIOJSRMRYXLDVGDBBYXARBNHXOXMBXYOTEFOAXRAUKXTWKYYGWNAHHCIIKQHYAETGBW ABTEMJKNTEUQAWGHRIKDGGNHUIVVPPYPYTZERZKDPLUSIKPBDPJOCBYQJDEKAVQKHFTPBZJQOUCVBHAHZZGEXOCYGYDCZICBOETRSJSMVEZKIN DRIKZYTUIS

C:\Users\user\AppData\Local\Temp\tmp18B1.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697125102277996
Encrypted:	false
SSDEEP:	24:uVOXLU7xwK58ZsokCVVZGi4eW0ZFJVPNR+x:c7xR8mwGi4sbv+x
MD5:	207485EFCE70435971C31586A1E4CF97
SHA1:	245A410AEB767B099944A8E81F75FC9A4B270DFB
SHA-256:	BF45E8FD687DC0E63FD40F32F2279152430579EDE044C3BB0852A1AC460D4B09
SHA-512:	A7F01CBBAFE9EA12B4C820F5E1A107D4C6FBD57CFF41C4AC679485F2B7DAFA4E9148AF830A39A083EC866E988A8E279FEB39D5EB58593E75D22253BED4DEF A19
Malicious:	false
Preview:	QCOILOQIKCUYMAHQLCLSCUGPPLVTJEARXPXBWFLOFHRVUSXLZVWHDQNKEMGPPQAGBLIPFAECDZNKKHITNQJASUXZAYMZIQCEHAQMCVZBMFUDBN QEKCBNCGMUWXDJLMJKVRKYBLRGNWGBGEVIGVROENGUXKJERNJSJJEMVLDKUXDFUWUPQNWUYRIEPUFOQKPDSZXXCKNQVBEAVMDMBR ZSWYPCNALGHTDFWFNDXKSHXCRLYPVFVYVEOFRHUFZZGNIXSJQCPZGONOYWWUQLBEBGALPOGZBXJUYXTHWOKWNKJYPSELALXQYIKAHXCELBTKSQ FTNYWBHRPQFULPLOCWEQAXEQNXOBIQOYFSEEZWHQQLZPBQOUMVZIMRWRLSPDKEBXSTPZLAGVYIORHCDBXTBHYOFKACXVGKKSIFHPOLDOQGIDQP FPVIPGUCGUCQLFFBYAGFJYFOMBUMPAHPQLDOHYAMKEGSDPXEYBQJUOWZOPFYRTLYUYDJHPLVEXBXUGVUEYIBUTUABUIHROFHZMLJUXWGZILWRH VKGOSZXXCIWGRGUZQDKQMTXRRWHDLJPPIRDALEIAYYTEEONIAELEISEOGNTDSALVOZDMFPLJSJMKJYMWGSKCTXHTLYYFJSXNZMDELRTJBNXSGA OEPKCPEEPFZKCAATOWHUWGQAEQNZHTKQEUCFRXVJWOGAEQDIWARNNFKCHEDRWTKEOVTURBKPDMQPPDCJGTYCTIRELHGRIRLWAPLC EHANSMGDZZYCXXDOTQVOSDZJAEBOTEVLSMHXCOWDPVQPSGDIDBAWUTDPIYPVBFSUMFBUYOPRXLECFHENURLSLKGPFWXDUFYOAKNTFKOYFUZEKL RZOLPYKMCKVZOIMDCCSGPQNCQXJOTJDKUQEPVHFKRSGZYJBNUHVTOEMNLTDXGZHTDQFQZCOULTNVZRAVLOIOVIKUTWPYLRJUCUDMYVYFWSBLJT JKMSJEIJXWYNPKGTYLKDAEVBUQUIJX

C:\Users\user\AppData\Local\Temp\tmp18B2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697427014915338
Encrypted:	false
SSDEEP:	24:J87vGcgdreYqco0NFLg5elatTFj9qVUq2Z:J83gAYq8NFRtx7Z
MD5:	2D7ACA56B5F340F28DD1D2B46D700BA6
SHA1:	3966684FF029665614B8DC948349178FB9E8C078
SHA-256:	B227E5E45D28AC063349BC70CC01A3F6DB15C101432A8609E0202064F7E5936D
SHA-512:	D4BFC2BB839DAEBAE8C894A0B8EB2314D2BE0304C82EB89BE16D6C820874952534CE0D93AE62EEF3DD2BE8A4D1E828B883E50BD204D04624AB945119D2FAE 4F0
Malicious:	false

Preview:	ZIPXYXWIOYFFJDUIEBFLHIUBYNNMJGYPFQONGOLQHGMFRFYQGSVGNDSCQJYWDCIKWJWNYHFUEMJVEPAFIPAROVFAVARCOHESRJKUIUYDXNZOER BEQGHQNKYMVMEEMKKKEYXXPAKWYGCIXNFSVDOOEUTNGSDXMYEZKQTRDCZXZXIFSRMNAEPZWJKKYULUPGZCQORNOJBGAAOPLYNJCP FWSASJWTLALTQZLWOGFWQVOXGYBCMNEBDESHLNZZBETDIGNLTNPZEPEQAMYCNYWEKKQKDVZPNYLWAFZIPSSVNHOPUMIBTFXVVCNCPUSOKETVBD NZLCRKBRLGSHFSQLECHUOWGFFEMDWHASNSMAXKZZMDLZVQLADFBDUCCIJERQXKRXUCTKGDGKPESHHXUPKZSGNKOITMVITFCBELJVTCKENQCMCJ EDZJDQDSKAYFGQEYICXDUOIJRYIMVXRKNBYXQEHUHYSPGEDSJBOQNXHFTSSRTPOXDVFXEPQUGWNEAKZJOKYPEYKXMOMKTKOBVISHMUGELPJCXB YNEXOAWOXHSEELVSCFMZYAMOLTGIWURMTZTRNGMWQZBRQHAIXVJIAFPZGWJZIOQLOAXJSGKMZNZCAVJWFGUFMQWQICMPVNAYRUHA MQLWLJMBERSFPEZHMNVAZFQAJEGYJQOMQWFTQVXZYTDPYVGZZPSNSOJWWKZDRPZKGTXYSENWOIQFXDIRWPJEYALOOEYQPHOPKSIZFNHPOXOKST DVPNBSCDDKPOUVXMFBUNBMEUYGOSYMHMUNKKADTAEIUEMXYPOPMUVBHTBVKYAHHJXFUJPFZJZARAFLARBIWKXMNKXJLVBLJSZYYVIBZHROONQE NYZGGMMETTMOFHCCQNUHPDEUTVVGUDBCKVXVUMRWPGZIPPUXJEJQIEQWLBUQBUODMWPSBFOYIQZWMYWPHWSKTRCKCRXWZUOTDTDR LLUSSQZXZZEATFSHBUWQUYHDLRMVVWFCPAZNSBXA

C:\Users\user\AppData\Local\Temp\tmp1920.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.687055908915499
Encrypted:	false
SSDEEP:	24:X3rfasg2Tpd/zBJY+q9FZP0DJR6BdqWD5gB8H36D6jXLiUk2ZTV:X+52L/dJYBjYJRoddD5C8HqD8ZDZTV
MD5:	94EDB575C55407C555A3F710DF2A8CB3
SHA1:	3AB8DF4B92C320D7D4C661EAB608E24B43F3DD13
SHA-256:	DD3A4A93D60E4B7840557A44DAAF77F6B6F85032C7DD5FB10BE54C07B0E1E261
SHA-512:	F8F78D10AE19735413AF11F0C8DAC41644479D345DC6B300412DEDA9779A01DDFC7150FBFD54F2582A0DF8524B7E507886DBC49E59B084320017E9E64FC8DBF A
Malicious:	false
Preview:	JDDHMPCDUJFORBKGTIFQHFPQNEKFAIHGBDYZBWNZMVTSZXTGRUOCZPQRXMGXBNMAHGODCTVNAHQHZMJYIYXLTVDMEAVEXSWFQCDVPRSSLREITY MWHUXVVKLPJXQJOHYPAVYXSIMBBOTIWYDKNCDVKZZMEIFEDNNXHAHMYLPOUGNKMPZVDEQRUPZBQCKZDQINFECCUZINROAFGLIAMVWHXPPXOWZM WTITWBJFIENEHRXRHRPVUAIUAJUYDBBSQQMTJJXOAAMHVKJEOIQRSNKKQSGCHAUKUYPJEBZIGZTVKUXZEQOUSZPQBHKFHECDNFGTGIDHSJFVLA KZPDYVJVWECRIKKUCCFNNHBLBFCJEKSUZTITTTLQVOHKFHXFIIYDOZNAIBCDIRXJAYKHCOEXBOGSGEGGQEMHFXIZREOFZJSAFXTGSSZLVKYOAN MZNPNESDZMFYWTZHIKUSMZXACWZEIMGTFRSZCGICPOSTZRECQYWZECQVLAWXESWPCDXLHIMJHSZJSDAXNXHETAWLZDXTZAPKBHSMKMYYGVSJCU IJSIFUHHMPIRBASPUOUXKKPQCECQBBZUSIXEOXLFFSQIFCTAIRASCMWEHFOXGEJRXFGJODUTKITHEAKFFJQTQNWWKXXDELWDHHEDWUTMSLXQJP VGOBKELYSRBQFYKXFHWGSCVLTCFKOEJMLUXIZVDPFHXHTSMTDRTVCNLISGJFVQRUTMZDYPUYBAEASZCSEUVHWRIQDEJIZQQHJNTIIICFMMPVLX OIVTPCTDKFPDVWXSBXZDXFUMBJTJMKOOHIMIOAKEJSIDIOJSRMRYXLDVGDBBYXARBNHXOXMBXYOTEFOAXRAUKXTWKYYGWNAHHCIIKQHYAETGBW ABTEMJKNTEUQAWGHRIKDGGNHUIVVPPYPYTZERZKDPLUSIKPBDPJOCBYQJDEKAVQKHFTPBZJQOUCVBHAHZZGEXOCYGYDCZICBOETRSJSMVEZKIN DRIKZYTUIS

C:\Users\user\AppData\Local\Temp\tmp1921.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697125102277996
Encrypted:	false
SSDEEP:	24:uVOXLU7xwK58ZsokCVVZGi4eW0ZFJVPNR+x:c7xR8mwGi4sbv+x
MD5:	207485EFCE70435971C31586A1E4CF97
SHA1:	245A410AEB767B099944A8E81F75FC9A4B270DFB
SHA-256:	BF45E8FD687DC0E63FD40F32F2279152430579EDE044C3BB0852A1AC460D4B09
SHA-512:	A7F01CBBAFE9EA12B4C820F5E1A107D4C6FBD57CFF41C4AC679485F2B7DAFA4E9148AF830A39A083EC866E988A8E279FEB39D5EB58593E75D22253BED4DEF A19
Malicious:	false
Preview:	QCOILOQIKCUYMAHQLCLSCUGPPLVTJEARXPXBWFLOFHRVUSXLZVWHDQNKEMGPPQAGBLIPFAECDZNKKHITNQJASUXZAYMZIQCEHAQMCVZBMFUDBN QEKCBNCGMUWXDJLMJKVRKYBLRGNWGBGEVIGVROENGUXKJERNJSJJEMVLDKUXDFUWUPQNWUYRIEPUFOQKPDSZXXCKNQVBEAVMDMBR ZSWYPCNALGHTDFWFNDXKSHXCRLYPVFVYVEOFRHUFZZGNIXSJQCPZGONOYWWUQLBEBGALPOGZBXJUYXTHWOKWNKJYPSELALXQYIKAHXCELBTKSQ FTNYWBHRPQFULPLOCWEQAXEQNXOBIQOYFSEEZWHQQLZPBQOUMVZIMRWRLSPDKEBXSTPZLAGVYIORHCDBXTBHYOFKACXVGKKSIFHPOLDOQGIDQP FPVIPGUCGUCQLFFBYAGFJYFOMBUMPAHPQLDOHYAMKEGSDPXEYBQJUOWZOPFYRTLYUYDJHPLVEXBXUGVUEYIBUTUABUIHROFHZMLJUXWGZILWRH VKGOSZXXCIWGRGUZQDKQMTXRRWHDLJPPIRDALEIAYYTEEONIAELEISEOGNTDSALVOZDMFPLJSJMKJYMWGSKCTXHTLYYFJSXNZMDELRTJBNXSGA OEPKCPEEPFZKCAATOWHUWGQAEQNZHTKQEUCFRXVJWOGAEQDIWARNNFKCHEDRWTKEOVTURBKPDMQPPDCJGTYCTIRELHGRIRLWAPLC EHANSMGDZZYCXXDOTQVOSDZJAEBOTEVLSMHXCOWDPVQPSGDIDBAWUTDPIYPVBFSUMFBUYOPRXLECFHENURLSLKGPFWXDUFYOAKNTFKOYFUZEKL RZOLPYKMCKVZOIMDCCSGPQNCQXJOTJDKUQEPVHFKRSGZYJBNUHVTOEMNLTDXGZHTDQFQZCOULTNVZRAVLOIOVIKUTWPYLRJUCUDMYVYFWSBLJT JKMSJEIJXWYNPKGTYLKDAEVBUQUIJX

C:\Users\user\AppData\Local\Temp\tmp1951.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697427014915338
Encrypted:	false

SSDEEP:	24:J87vGcgdreYqco0NFLg5eIatTFj9qVUq2Z:J83gAYq8NFRtx7Z
MD5:	2D7ACA56B5F340F28DD1D2B46D700BA6
SHA1:	3966684FF029665614B8DC948349178FB9E8C078
SHA-256:	B227E5E45D28AC063349BC70CC01A3F6DB15C101432A8609E0202064F7E5936D
SHA-512:	D4BFC2BB839DAEBAE8C894A0B8EB2314D2BE0304C82EB89BE16D6C820874952534CE0D93AE62EEF3DD2BE8A4D1E828B883E50BD204D04624AB945119D2FAB4F0
Malicious:	false
Preview:	ZIPXYXWIOYFFJDUIEBFLHIUBYNNMJGYPFQONGOLQHGMFRFYQGSVGNDSCQJYWDCIKWJWNYHFUEMJVEPAFIPAROVFAVARCOHESRJKUIUYDXNZOER BEQGHQNKYMVMEEMKKKEYXXPAKWYGCIXNFSVDOOEUTNGSDXMYEZKQTRDCZXZXIFSRMNAEPZWJKKYULUPGZCQORNOJBGAAOPLYNJCP FWSASJWTLALTQZLWOGFWQVOXGYBCMNEBDESHLNZZBETDIGNLTNPZEPEQAMYCNYWEKKQKDVZPNYLWAFZIPSSVNHOPUMIBTFXVVCNCPUSOKETVBD NZLCRKBRLGSHFSQLECHUOWGFFEMDWHASNSMAXKZZMDLZVQLADFBDUCCIJERQXKRXUCTKGDGKPESHHXUPKZSGNKOITMVITFCBELJVTCKENQCMCJ EDZJDQDSKAYFGQEYICXDUOIJRYIMVXRKNBYXQEHUHYSPGEDSJBOQNXHFTSSRTPOXDVFXEPQUGWNEAKZJOKYPEYKXMOMKTKOBVISHMUGELPJCXB YNEXOAWOXHSEELVSCFMZYAMOLTGIWURMTZTRNGMWQZBRQHAIXVJIAFPZGWJZIOQLOAXJSGKMZNZCAVJWFGUFMQWQICMPVNAYRUHA MQLWLJMBERSFPEZHMNVAZFQAJEGYJQOMQWFTQVXZYTDPYVGZZPSNSOJWWKZDRPZKGTXYSENWOIQFXDIRWPJEYALOOEYQPHOPKSIZFNHPOXOKST DVPNBSCDDKPOUVXMFBUNBMEUYGOSYMHMUNKKADTAEIUEMXYPOPMUVBHTBVKYAHHJXFUJPFZJZARAFLARBIWKXMNKXJLVBLJSZYYVIBZHROONQE NYZGGMMETTMOFHCCQNUHPDEUTVVGUDBCKVXVUMRWPGZIPPUXJEJQIEQWLBUQBUODMWPSBFOYIQZWMYWPHWSKTRCKCRXWZUOTDTDR LLUSSQZXZZEATFSHBUWQUYHDLRMVVWFCPAZNSBXA

C:\Users\user\AppData\Local\Temp\tmpA487.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\tmpA4F5.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\tmpB95.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944

MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpBF4.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpC33.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpC92.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false

Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpCC2.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpCF62.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\tmpD30.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpD60.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpDBF.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpE2D.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpE3B6.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041

Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\tmpE3D6.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\tmpE406.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\tmpE8C.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA

SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpEBC.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpF80C.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.433796373508295
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	StZAEFSb2j.exe
File size:	43520
MD5:	c71616e2b7cedf9fc8e2ca6f6929abdf
SHA1:	896a4c41792c73db51074ccff5ef3f0577f510c5
SHA256:	4a9f8a3b847fa9d2e854d3a7235ddee8e4c093d04c3901f006d430be1060fae5
SHA512:	bcf06478805a8c0b047304989a76a9a6d5380b148524c12eb8e1e2acebead20bc42a969992a332b9ab33e6644ef2e0aaf4d1933f84cbcfccd2d86995310f58ef

SSDEEP:	768:A5588dpB2Gaq7kvl4VPNznshp/xzVmzOMdcGMN75H16U8S4riXzjla:C58K97kuVPRn+/xJm65GMN7FMuBzjo
TLSH:	9113B99D766072DFC85BC0729EA82C68EB60747B931B8243942715ADDE0DA97CF080F3
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....^cc..............0.................. ....@.. ....`................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40bebe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63635E1E [Thu Nov 3 06:22:22 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbe70	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc000	0x5a6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xbe2c	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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9ec4	0xa000	False	0.41630859375	data	5.4639881643435775	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc000	0x5a6	0x600	False	0.4186197916666667	data	4.114149153750449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc0a0	0x31c	data		
RT_MANIFEST	0xc3bc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

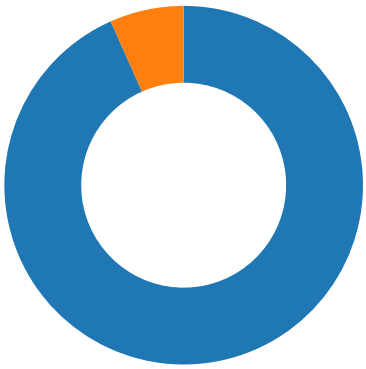
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.48.8.8.8.856572532012811 11/03/22-12:44:38.337914	UDP	2012811	ET DNS Query to a .tk domain - Likely Hostile	56572	53	192.168.2.4	8.8.8.8
50.115.174.192192.168.2.4443496952018856 11/03/22-12:44:39.556293	TCP	2018856	ET TROJAN Windows executable base64 encoded	443	49695	50.115.174.192	192.168.2.4
50.115.174.192192.168.2.4443496962018856 11/03/22-12:44:40.820043	TCP	2018856	ET TROJAN Windows executable base64 encoded	443	49696	50.115.174.192	192.168.2.4

Network Port Distribution



Total Packets: 45

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:44:38.407645941 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:38.407692909 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:38.407783985 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:38.469727039 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:38.469760895 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:38.837925911 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:38.838049889 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:38.853115082 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:38.853154898 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:38.853569031 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:38.896302938 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:39.378637075 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:39.378685951 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.556324959 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.556360006 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.556368113 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.556541920 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:39.556580067 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.604000092 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:39.732975006 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.732997894 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.733069897 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.733079910 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.733130932 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.733139992 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.733177900 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:39.733206987 CET	443	49695	50.115.174.192	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:44:39.733226061 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:39.787089109 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:39.907883883 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.907963991 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.907995939 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.908026934 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.908195972 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.908226967 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.908267975 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:39.908303022 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.908324957 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:39.908340931 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.908396006 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:39.908418894 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:39.959028006 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.083826065 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.083920956 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.083951950 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.083975077 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084000111 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084011078 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084038019 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084050894 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084079981 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084084988 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084095001 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084135056 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084188938 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084243059 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084292889 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084342957 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084368944 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084418058 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084441900 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084495068 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084501028 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084513903 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084549904 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084567070 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084568024 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084578991 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084625959 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.084633112 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084681034 CET	443	49695	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.084712029 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.093774080 CET	49695	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.098267078 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.098331928 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.098745108 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.099368095 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.099400997 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.465075970 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.496548891 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.496577024 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.820102930 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.820142984 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.820180893 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.820293903 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.820327997 CET	443	49696	50.115.174.192	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:44:40.820374012 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.865231991 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.997716904 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.997739077 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.997828007 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.997838974 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.997839928 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.997905970 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.997910976 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.997925043 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.997952938 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.998018026 CET	443	49696	50.115.174.192	192.168.2.4
Nov 3, 2022 12:44:40.998064995 CET	49696	443	192.168.2.4	50.115.174.192
Nov 3, 2022 12:44:40.999274969 CET	49696	443	192.168.2.4	50.115.174.192

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:44:38.337913990 CET	56572	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:44:38.365986109 CET	53	56572	8.8.8.8	192.168.2.4
Nov 3, 2022 12:45:07.954663992 CET	50911	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:45:07.986056089 CET	59683	53	192.168.2.4	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:44:38.337913990 CET	192.168.2.4	8.8.8.8	0x53e5	Standard query (0)	tgc8x.tk	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:45:07.954663992 CET	192.168.2.4	8.8.8.8	0x5f34	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:45:07.986056089 CET	192.168.2.4	8.8.8.8	0x3a	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)	false

DNS Answers

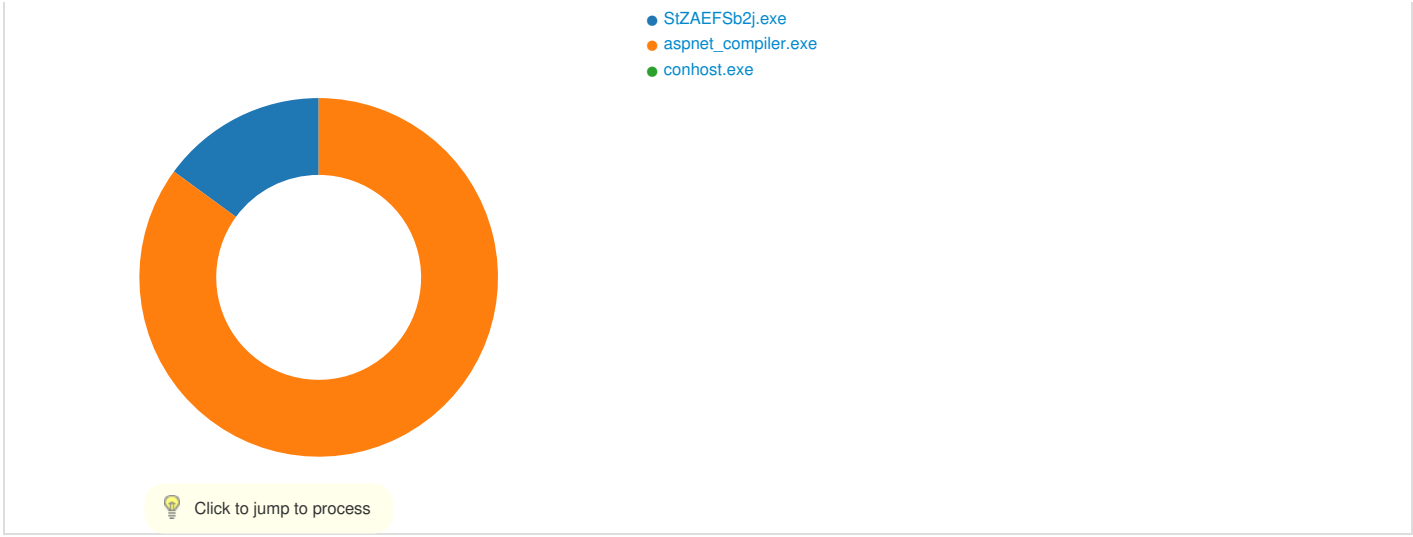
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:44:38.365986109 CET	8.8.8.8	192.168.2.4	0x53e5	No error (0)	tgc8x.tk		50.115.174.192	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:45:07.974468946 CET	8.8.8.8	192.168.2.4	0x5f34	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:45:08.007771969 CET	8.8.8.8	192.168.2.4	0x3a	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- tgc8x.tk
- 194.55.186.201:6008

Statistics

Behavior



System Behavior

Analysis Process: StZAEFSb2j.exe PID: 780, Parent PID: 3528

General

Target ID:	0
Start time:	12:44:36
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\StZAEFSb2j.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\StZAEFSb2j.exe
Imagebase:	0x5d0000
File size:	43520 bytes
MD5 hash:	C71616E2B7CEDF9FC8E2CA6F6929ABDF
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: 00000000.00000002.321721404.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.321721404.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000000.00000002.321721404.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D61CF06	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	6D61CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\StZAEFSb2j.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D92C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\StZAEFSb2j.exe.log	0	847	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6D92C907	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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	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

Analysis Process: aspnet_compiler.exe PID: **1592**, Parent PID: **780**

General

Target ID:	1
Start time:	12:44:40
Start date:	03/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe

Imagebase:	0xc10000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
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: 00000001.00000000.316565039.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.316565039.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000001.00000000.316565039.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.415555604.0000000002FAF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

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	6D61CF06	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	6D61CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpA487.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpA4F5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpCF62.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpE3B6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpE3D6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpE406.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpF80C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpB95.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpBF4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpC33.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpC92.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpCC2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpD30.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpD60.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDBF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpE2D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpE8C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpEBC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp1881.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp18B1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp18B2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp1920.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp1921.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp1951.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C46BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C46BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\aspnet_compiler.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D92C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA4F5.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA487.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE3B6.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpCF62.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE406.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE3D6.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpB95.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpF80C.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpC33.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpBF4.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpCC2.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpC92.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpD60.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpD30.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE2D.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpDBF.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpEBC.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE8C.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp1881.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp18B1.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp18B2.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp1920.tmp	success or wait	1	6C466A95	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1921.tmp	success or wait	1	6C466A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp1951.tmp	success or wait	1	6C466A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\aspnet_compiler.exe.log	0	2412	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 53 65 72 76 69 63 65 4d 6f 64 65 6c 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 30	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30	success or wait	1	6D92C907	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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\86d45445dab867207240160512711f5f9\System.Net.Http.ni.dll.aux	unknown	536	success or wait	1	6D5503DE	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	3	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	42	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	273	end of file	3	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	3	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA4F5.tmp	unknown	49152	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE3B6.tmp	unknown	49152	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE406.tmp	unknown	49152	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	3	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	273	end of file	3	6C461B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB95.tmp	unknown	94208	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC33.tmp	unknown	94208	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCC2.tmp	unknown	94208	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	3	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	273	end of file	3	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD60.tmp	unknown	94208	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE2D.tmp	unknown	94208	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpEBC.tmp	unknown	94208	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1881.tmp	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp18B1.tmp	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp18B2.tmp	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1920.tmp	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1921.tmp	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1951.tmp	unknown	4096	success or wait	1	6C461B4F	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

Analysis Process: conhost.exe PID: **6120**, Parent PID: **1592**

General

Target ID:	2
Start time:	12:44:40
Start date:	03/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly