ID: 682146
Sample Name:
SecuriteInfo.com.W32.AIDetectNet.01.18072.21111
Cookbook: default.jbs
Time: 06:30:06
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

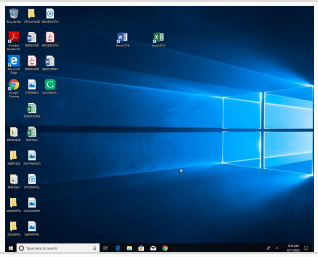
Windows Analysis Report

SecuriteInfo.com.W32.AIDetectNet.01.18072.21111

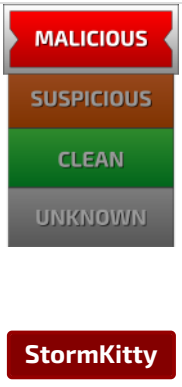
Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetectNet.01.18072.21111 (renamed file extension from 21111 to exe)
Analysis ID:	682146
MD5:	62d82f1dfb55dde.
SHA1:	01e84f81780700..
SHA256:	7b968e65480e57.
Tags:	exe
Infos:	



Detection



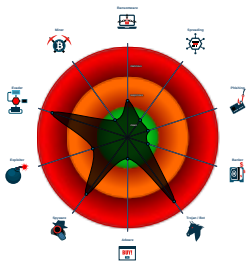
StormKitty

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AntiVM3
- Yara detected StormKitty Stealer
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- May check the online IP address of…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.W32.AIDetectNet.01.18072.exe (PID: 4288 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.18072.exe" MD5: 62D82F1DFB55DDE5554C8B278A819AC9)
  - MSBuild.exe (PID: 4144 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
  - MSBuild.exe (PID: 5640 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
    - AppLaunch.exe (PID: 60 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.278305735.00000000074F3000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000006.00000000.267975304.00000000012B2000.00000040.00000400.00020000.00000000.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x327c:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x316c:$op2: 00 17 03 1F 20 17 19 15 28 • 0x3c02:$op3: 00 04 03 69 91 1B 40 • 0x4452:$op3: 00 04 03 69 91 1B 40
00000006.00000000.267975304.00000000012B2000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000006.00000000.267975304.00000000012B2000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_StormKitty	Yara detected StormKitty Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000000.267975304.00000000012B2000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.W32.AIDetectNet.01.18072.exe.3775250.2.raw.unpack	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	• 0x17ef0:$s1: Temporary Directory * for • 0x17f4c:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0x17904:$s6: Content-Disposition: form-data; name="document"; filename=" • 0x17e7c:$s7: CopyHere • 0x17e44:$s9: shell.application • 0x17e9c:$s9: Shell.Application • 0x17a64:$s10: SetRequestHeader • 0x17ffc:$s12: @TITLE Removing • 0x18034:$s13: @RD /S /Q "
0.2.SecuriteInfo.com.W32.AIDetectNet.01.18072.exe.3775250.2.unpack	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	• 0x17ef0:$s1: Temporary Directory * for • 0x17f4c:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0x17904:$s6: Content-Disposition: form-data; name="document"; filename=" • 0x17e7c:$s7: CopyHere • 0x17e44:$s9: shell.application • 0x17e9c:$s9: Shell.Application • 0x17a64:$s10: SetRequestHeader • 0x17ffc:$s12: @TITLE Removing • 0x18034:$s13: @RD /S /Q "
5.0.MSBuild.exe.400000.0.unpack	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	• 0x17ef0:$s1: Temporary Directory * for • 0x17f4c:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0x17904:$s6: Content-Disposition: form-data; name="document"; filename=" • 0x17e7c:$s7: CopyHere • 0x17e44:$s9: shell.application • 0x17e9c:$s9: Shell.Application • 0x17a64:$s10: SetRequestHeader • 0x17ffc:$s12: @TITLE Removing • 0x18034:$s13: @RD /S /Q "
6.0.AppLaunch.exe.12b0000.0.unpack	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x347c:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x336c:$op2: 00 17 03 1F 20 17 19 15 28 • 0x3e02:$op3: 00 04 03 69 91 1B 40 • 0x4652:$op3: 00 04 03 69 91 1B 40
6.0.AppLaunch.exe.12b0000.0.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
Click to see the 5 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

Machine Learning detection for sample

Networking

May check the online IP address of the machine

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation

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

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Telegram RAT

Yara detected StormKitty 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 Telegram RAT

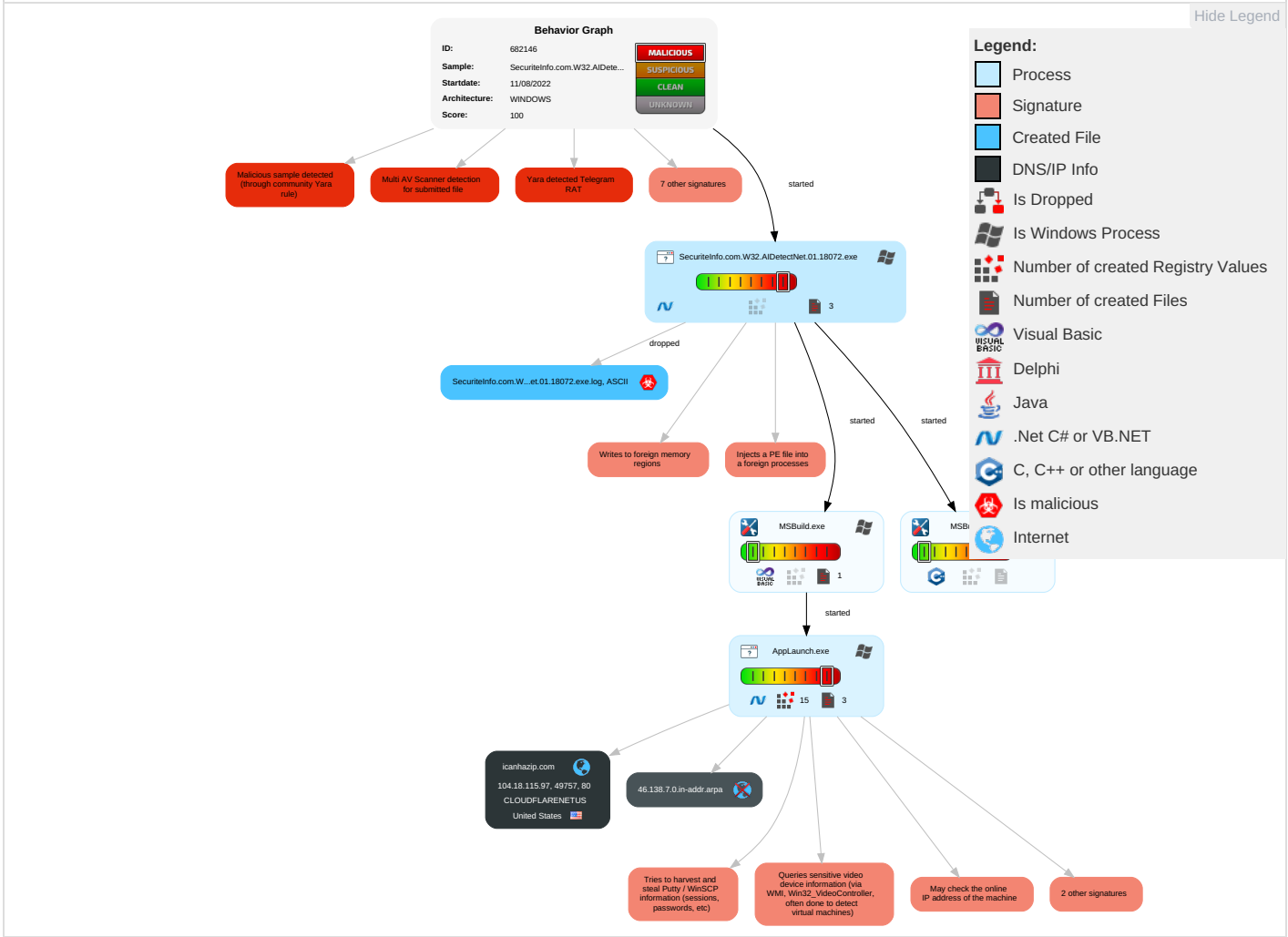
Yara detected StormKitty Stealer

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	1 3 1 Windows Management Instrumentation	Path Interception	2 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	2 3 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
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 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 4 1 Virtualization/Sandbox Evasion	Security Account Manager	1 4 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 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	1 System Network Configuration 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	3 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory 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	1 3 Software Packing	DCSync	3 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

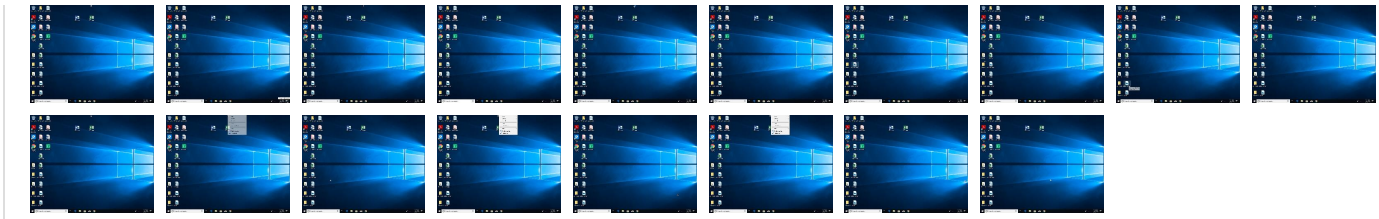
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.W32.AIDetectNet.01.18072.exe	38%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetectNet.01.18072.exe	22%	ReversingLabs	ByteCode-MSIL.Infostealer.Generic	
SecuriteInfo.com.W32.AIDetectNet.01.18072.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.SecuriteInfo.com.W32.AIDetectNet.01.18072.exe.3775250.2.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
46.138.7.0.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://icanhazip.com4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/=2	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comcom9	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//s	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fontbureau.como&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/s2Lo	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y02	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//2(o$	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.fontbureau.comlvfet	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/22	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/=2	0%	Avira URL Cloud	safe	
http://www.fonts.comn75	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
icanhazip.com	104.18.115.97	true	false		high
46.138.7.0.in-addr.arpa	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://icanhazip.com/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.270617234.000000000377400 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.270730941.000000000379 7000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 00000005.00000000.262112216.0000000000401000.00000040.00000400.00020000.00000000.sdmp, AppLaunch.exe, 00000006.00000000.267975304.00000000012B2000.00000040.00000400.00020000.00000000.sdmp	false		high
http://icanhazip.com4	AppLaunch.exe, 00000006.00000002.278289378.00000000074EE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/=2	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.236731661.000000000575700 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.236769351.000000000574 3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcom9	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.239067222.000000000575500 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp//s	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.236731661.000000000575700 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.236769351.000000000574 3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.265577466.000000000987000 0.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695 2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

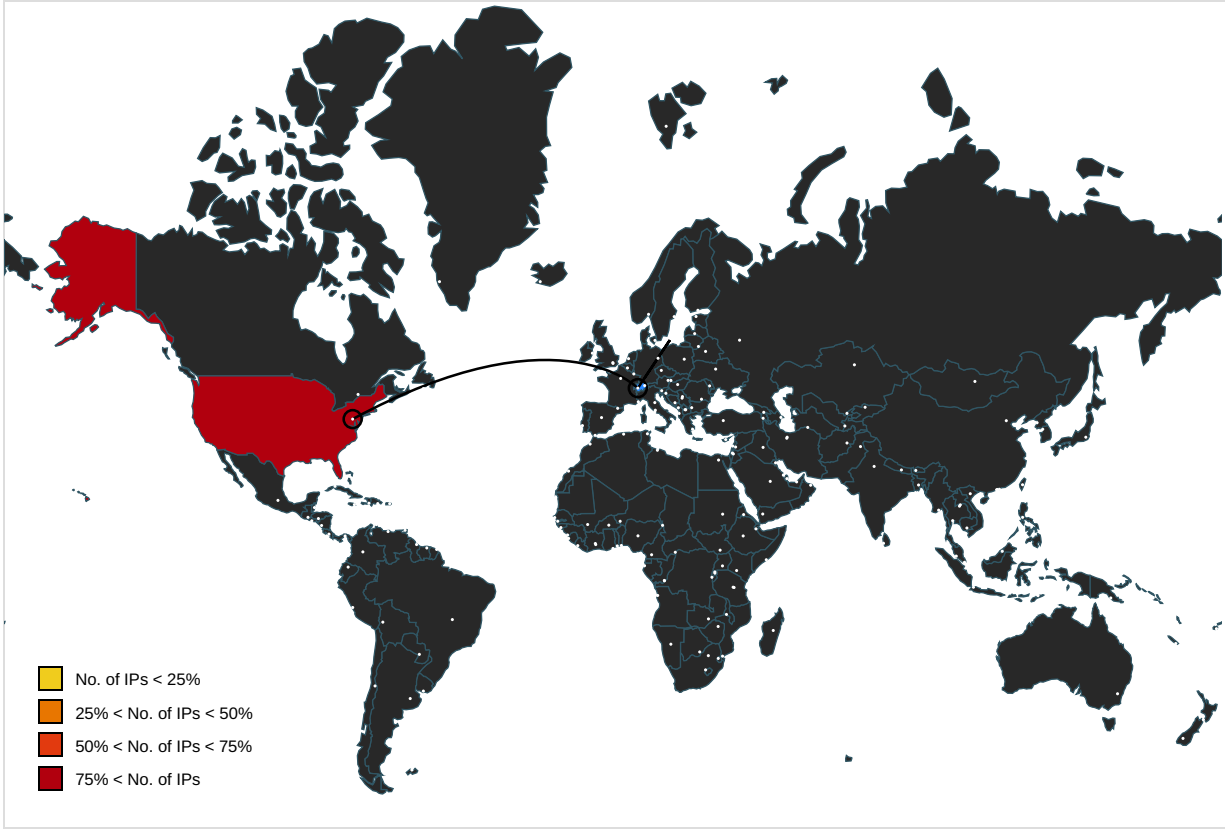
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.comic	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.232090615.000000000575B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/LimerBoy/StormKitty	AppLaunch.exe, 00000006.00000002.277763256.0000000007421000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000006.00000000.267975304.00000000012B2000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://icanhazip.com	AppLaunch.exe, 00000006.00000002.277763256.0000000007421000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000006.00000002.278255663.00000000074E5000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000006.00000002.278305735.00000000074F3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.urwpp.deDPlease	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000006.00000002.278255663.00000000074E5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.242460534.000000000575700.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.241663603.0000000005757000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.0000000006952000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.comc	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.232034414.000000000575B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como&	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.239067222.000000000575500.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/s2Lo	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237559788.000000000575500.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237693783.00000000574C000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237887447.0000000005757000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237478456.000000000574C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y02	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237416278.000000000575500.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237224324.000000000575500 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237416278.00000000057 55000.00000004.00000800.00020000.0000000 0.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072. exe, 00000000.00000003.237559788.0000000 005755000.00000004.00000800.00020000.000 00000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18 072.exe, 00000000.00000003.237693783.000 000000574C000.00000004.00000800.00020000 .00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.0 1.18072.exe, 00000000.00000003.238153037 .0000000005755000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.W32 .AIDetectNet.01.18072.exe, 00000000.0000 0003.237887447.0000000005757000.00000004 .00000800.00020000.00000000.sdmp, Securi teInfo.com.W32.AIDetectNet.01.18072.exe, 00000000. 00000003.237133726.0000000005755000.0000 0004.00000800.00020000.00000000.sdmp, Se curiteInfo.com.W32.AIDetectNet.01.18072.exe, 00000 000.00000003.237478456.000000000574C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//2(o$	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237416278.000000000575500 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237559788.00000000057 55000.00000004.00000800.00020000.0000000 0.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072. exe, 00000000.00000003.237693783.0000000 00574C000.00000004.00000800.00020000.000 00000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18 072.exe, 00000000.00000003.237887447.000 0000005757000.00000004.00000800.00020000 .00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.0 1.18072.exe, 00000000.00000003.237478456 .000000000574C000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.234226531.000000000574E00 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.00000000069 52000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/o	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.236731661.000000000575700 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.236769351.00000000057 43000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comlvfet	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.242460534.000000000575700 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.241663603.00000000057 57000.00000004.00000800.00020000.0000000 0.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072. exe, 00000000.00000003.242609831.0000000 005758000.00000004.00000800.00020000.000 00000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18 072.exe, 00000000.00000003.242565843.000 0000005757000.00000004.00000800.00020000 .00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.0 1.18072.exe, 00000000.00000003.264148491 .0000000005753000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comm	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.239067222.000000000575500 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237224324.000000000575500 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237416278.00000000057 55000.00000004.00000800.00020000.0000000 0.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072. exe, 00000000.00000003.237559788.0000000 005755000.00000004.00000800.00020000.000 00000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18 072.exe, 00000000.00000003.237693783.000 000000574C000.00000004.00000800.00020000 .00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.0 1.18072.exe, 00000000.00000003.238153037 .0000000005755000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.W32 .AIDetectNet.01.18072.exe, 00000000.0000 0003.236731661.0000000005757000.00000004 .00000800.00020000.00000000.sdmp, Securi teInfo.com.W32.AIDetectNet.01.18072.exe, 00000000. 00000003.237887447.0000000005757000.0000 0004.00000800.00020000.00000000.sdmp, Se curiteInfo.com.W32.AIDetectNet.01.18072.exe, 00000 000.00000003.237133726.0000000005755000. 00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 0 0000000.00000003.237478456.000000000574C 000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000 6952000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.1807 2.exe, 00000000.00000003.236769351.00000 00005743000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000002.273219672.000000000695200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/e	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237224324.000000000575500 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237416278.00000000057 55000.00000004.00000800.00020000.0000000 0.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072. exe, 00000000.00000003.237559788.0000000 005755000.00000004.00000800.00020000.000 00000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18 072.exe, 00000000.00000003.237693783.000 000000574C000.00000004.00000800.00020000 .00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.0 1.18072.exe, 00000000.00000003.237133726 .0000000005755000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.W32 .AIDetectNet.01.18072.exe, 00000000.0000 0003.237478456.000000000574C000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalic	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.239067222.000000000575500 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/22	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237224324.000000000575500 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237416278.00000000057 55000.00000004.00000800.00020000.0000000 0.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072. exe, 00000000.00000003.237559788.0000000 005755000.00000004.00000800.00020000.000 00000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18 072.exe, 00000000.00000003.237693783.000 000000574C000.00000004.00000800.00020000 .00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.0 1.18072.exe, 00000000.00000003.236731661 .0000000005757000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.W32 .AIDetectNet.01.18072.exe, 00000000.0000 0003.237887447.0000000005757000.00000004 .00000800.00020000.00000000.sdmp, Securi teInfo.com.W32.AIDetectNet.01.18072.exe, 00000000. 00000003.237133726.0000000005755000.0000 0004.00000800.00020000.00000000.sdmp, Se curiteInfo.com.W32.AIDetectNet.01.18072.exe, 00000 000.00000003.237478456.000000000574C000. 00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 0 0000000.00000003.236769351.0000000005743 000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/=2	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237224324.000000000575500 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.237416278.00000000057 55000.00000004.00000800.00020000.0000000 0.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18072. exe, 00000000.00000003.237559788.0000000 005755000.00000004.00000800.00020000.000 00000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.18 072.exe, 00000000.00000003.237693783.000 000000574C000.00000004.00000800.00020000 .00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.0 1.18072.exe, 00000000.00000003.237887447 .0000000005757000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.W32 .AIDetectNet.01.18072.exe, 00000000.0000 0003.237133726.0000000005755000.00000004 .00000800.00020000.00000000.sdmp, Securi teInfo.com.W32.AIDetectNet.01.18072.exe, 00000000. 00000003.237478456.000000000574C000.0000 0004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn75	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe, 00000000.00000003.232053595.000000000575B00 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.115.97	icanhazip.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682146
Start date and time:	2022-08-11 06:30:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetectNet.01.18072.21111 (renamed file extension from 21111 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:	29
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@2/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target MSBuild.exe, PID 5640 because there are no executed function
- 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
06:31:16	API Interceptor	1x Sleep call for process: SecuriteInfo.com.W32.AIDetectNet.01.18072.exe modified
06:31:23	API Interceptor	903x Sleep call for process: MSBuild.exe modified
06:31:29	API Interceptor	1x Sleep call for process: AppLaunch.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):	1036
Entropy (8bit):	5.356180291633412
Encrypted:	false
SSDEEP:	24:MLasXE4qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7K84j:MNH2HKXwYHKhQnoPtHoxHhAHKzvKvj

MD5:	7F8E631F679DF67A018544E516CF841E
SHA1:	02F03B1AB3CF33821236F743139693A61906A72B
SHA-256:	1FB2E1F28E4A338CD7E04A147E290E1DD880E83054BB2BA48EF6038EBA0BFACD
SHA-512:	4F7FD1AC6D22F8891F77BD3359EB0A536AB8E8A3D064BBAAB6620826F6B9FC8FC18DAB73474DB4806ED9CD1F5652549D7122E1DE8E5741010E7B3BE3F79EBB B7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni. dll",0..3,"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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8 e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral,

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.18072.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.18072.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=neutral, PublicKeyToken=b03f5f7f11d50a3a",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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.559415867177912
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SecuriteInfo.com.W32.AIDetectNet.01.18072.exe
File size:	581632
MD5:	62d82f1dfb55dde5554c8b278a819ac9
SHA1:	01e84f817807005f8d557d5320ddf9c366486620
SHA256:	7b968e65480e574dbf93ace25a28a30ca1f7b77fa98aabe980435484c365efbc
SHA512:	e1e629f928a1596325af166a50248794d0a4c8129442b25dd514a5ec6e9eef39c1d8867db6f85a72ffd3f0aa349c28af7ff70dd58027f8a04e15a8cb491a1d54
SSDEEP:	12288:M3Ih6jMEb6Qyxao8Fhyq+rqSAl4zXh2J3Fi7mX/IkQkk36EZd/gnS9ZvIl:W9Jb6Q28Fu9AvPI2k71fB
TLSH:	2BC4D02125A97229E0397BB51DD770A107F5F622DE06F57F3CB931860251E838BAE732
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Qi.b.....P.....4..... .....@.. .....@.....@.....

File Icon

Icon Hash:	d4eaccb4e4c8bac4

Static PE Info

General

Entrypoint:	0x48c90e
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:	0x62F46951 [Thu Aug 11 02:28:33 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]
inc edx
add byte ptr [eax+eax+41h], al
add byte ptr [ecx+00h], al
inc ebx
add byte ptr [ecx+00h], al
inc edx
add byte ptr [ecx+00h], al
inc ebx
add byte ptr [eax+eax+42h], al
add byte ptr [ebx+00h], al
inc esp
add byte ptr [ecx+00h], al
inc esp
add byte ptr [ebx+00h], al
inc ebx
add byte ptr [edx+00h], al
inc esp
add byte ptr [ecx+00h], 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8c8bc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8e000	0x30a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x92000	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	0x8a93c	0x8aa00	False	0.8138402417718665	data	7.562192679273532	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x8e000	0x30a4	0x3200	False	0.91921875	data	7.63895625946023	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x92000	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	0x8e0c8	0x2c63	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x90d3c	0x14	data		
RT_VERSION	0x90d60	0x340	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution

Total Packets: 7

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:31:28.024966955 CEST	49757	80	192.168.2.4	104.18.115.97
Aug 11, 2022 06:31:28.042078972 CEST	80	49757	104.18.115.97	192.168.2.4
Aug 11, 2022 06:31:28.042203903 CEST	49757	80	192.168.2.4	104.18.115.97
Aug 11, 2022 06:31:28.043061018 CEST	49757	80	192.168.2.4	104.18.115.97
Aug 11, 2022 06:31:28.059881926 CEST	80	49757	104.18.115.97	192.168.2.4
Aug 11, 2022 06:31:28.067483902 CEST	80	49757	104.18.115.97	192.168.2.4
Aug 11, 2022 06:31:28.160531998 CEST	49757	80	192.168.2.4	104.18.115.97
Aug 11, 2022 06:31:29.704567909 CEST	49757	80	192.168.2.4	104.18.115.97

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:31:27.635854006 CEST	62099	53	192.168.2.4	8.8.8.8
Aug 11, 2022 06:31:27.653176069 CEST	53	62099	8.8.8.8	192.168.2.4
Aug 11, 2022 06:31:27.965552092 CEST	53775	53	192.168.2.4	8.8.8.8
Aug 11, 2022 06:31:27.987278938 CEST	53	53775	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 11, 2022 06:31:27.635854006 CEST	192.168.2.4	8.8.8.8	0x74b5	Standard query (0)	46.138.7.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 11, 2022 06:31:27.965552092 CEST	192.168.2.4	8.8.8.8	0xb375	Standard query (0)	icanhazip.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:31:27.653176069 CEST	8.8.8.8	192.168.2.4	0x74b5	Name error (3)	46.138.7.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Aug 11, 2022 06:31:27.987278938 CEST	8.8.8.8	192.168.2.4	0xb375	No error (0)	icanhazip.com		104.18.115.97	A (IP address)	IN (0x0001)
Aug 11, 2022 06:31:27.987278938 CEST	8.8.8.8	192.168.2.4	0xb375	No error (0)	icanhazip.com		104.18.114.97	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- icanhazip.com

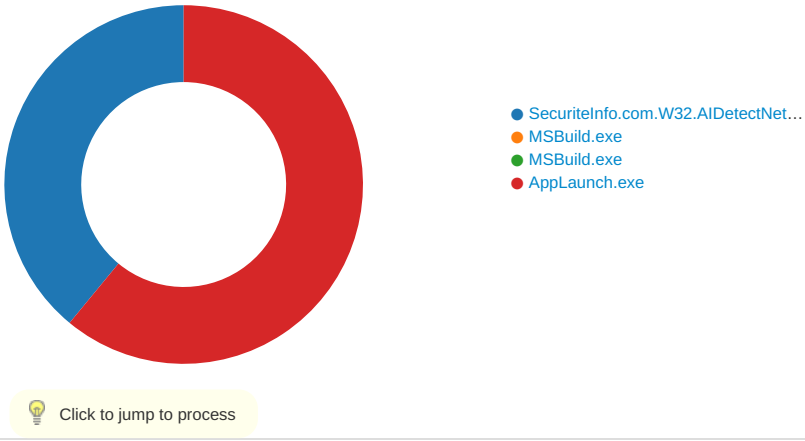
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49757	104.18.115.97	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:31:28.043061018 CEST	1022	OUT	GET / HTTP/1.1 Host: icanhazip.com Connection: Keep-Alive
Aug 11, 2022 06:31:28.067483902 CEST	1023	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 04:31:28 GMT Content-Type: text/plain Content-Length: 14 Connection: keep-alive Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET Set-Cookie: __cf_bm=Ey9b06GkUs3RvYus4mW9JMaXcGtQPk1nY.hCZFDJvks-1660192288-0-ATd2/GorYZ33ONvLo9CvyJg1+WCE9p13NRWeYbFnhablhqkRPrYfYCNh6YHAX3XQFFLxJFgRV8le0MmrRGHHRkc=; path=/; expires=Thu, 11-Aug-22 05:01:28 GMT; domain=.icanhazip.com; HttpOnly Server: cloudflare CF-RAY: 738e3de84d1768f2-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 30 32 2e 31 32 39 2e 31 34 33 2e 33 0a Data Ascii: 102.129.143.3

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.18072.exe PID: 4288, Parent PID: 3572

General

Target ID:	0
Start time:	06:31:05
Start date:	11/08/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.18072.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.18072.exe"
Imagebase:	0x340000
File size:	581632 bytes
MD5 hash:	62D82F1DFB55DDE5554C8B278A819AC9
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.270730941.0000000003797000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth
Reputation:	low

File Activities

Analysis Process: MSBuild.exe PID: **4144**, Parent PID: **4288**

General

Target ID:	4
Start time:	06:31:19
Start date:	11/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x420000
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: **5640**, Parent PID: **4288**

General

Target ID:	5
Start time:	06:31:21
Start date:	11/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe90000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000005.00000003.271797122.00000000013AA000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000003.271797122.00000000013AA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_StormKitty, Description: Yara detected StormKitty Stealer, Source: 00000005.00000003.271797122.00000000013AA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000003.271797122.00000000013AA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: AppLaunch.exe PID: **60**, Parent PID: **5640**

General

Target ID:	6
Start time:	06:31:24
Start date:	11/08/2022
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:	0x1310000
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: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.278305735.00000000074F3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000006.00000000.267975304.00000000012B2000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000000.267975304.00000000012B2000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_StormKitty, Description: Yara detected StormKitty Stealer, Source: 00000006.00000000.267975304.00000000012B2000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000000.267975304.00000000012B2000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.278474507.000000000753B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CF2CF06	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	6CF2CF06	unknown
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	6D23C78D	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	1036	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 4d 61 6e 61 67 65 6d 65 6e 74 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 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 33 31	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3031	success or wait	1	6D23C907	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	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6CF0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6CF0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6CF05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6BD71B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BD71B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly