ID: 662065
Sample Name:
SecuriteInfo.com.Variant.Jaik.84784.3654.exe
Cookbook: default.jbs
Time: 17:52:39
Date: 12/07/2022
Version: 35.0.0 Citrine

Table of Contents

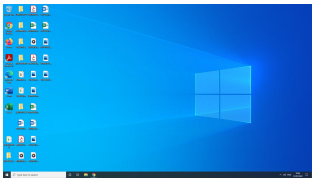
Windows Analysis Report

SecuriteInfo.com.Variant.Jaik.84784.3654.exe

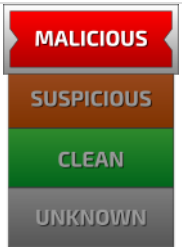
Overview

General Information

Sample Name:	SecuriteInfo.com.Variant.Jaik.84784.3654.exe
Analysis ID:	662065
MD5:	74cd3c3d32dcf5…
SHA1:	d7ec9719a6e5ea..
SHA256:	cb943da125fde1..
Infos:	



Detection



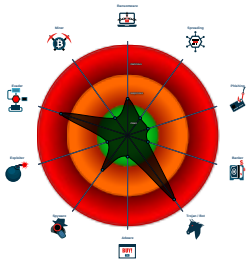
AsyncRAT, DcRat

Score:	62
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected DcRat
- Yara detected AsyncRAT
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Self deletion via cmd or bat file
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Uses ping.exe to check the status o…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.Variant.Jaik.84784.3654.exe (PID: 7424 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe" MD5: 74CD3C3D32DCF5029D1BC66347F44AF7)
  - schtasks.exe (PID: 2612 cmdline: C:\Windows\system32\schtasks.exe" /create /tn COMSurrogate /f /sc onlogon /rl highest /tr "C:\Users\user\AppVerif\DllHelper.exe MD5: 478BEAEC1C3A9417272BC8964ADD1CEE)
    - conhost.exe (PID: 740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - DllHelper.exe (PID: 7412 cmdline: "C:\Users\user\AppVerif\DllHelper.exe" MD5: BFEF1ABAB0ACACB7DC9D8828B32CFDE4)
    - InstallUtil.exe (PID: 8700 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: 5D4073B2EB6D217C19F2B22F21BF8D57)
  - cmd.exe (PID: 8812 cmdline: C:\Windows\System32\cmd.exe" /c chcp 65001 && ping 127.0.0.1 && DEL /F /S /Q /A "C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 7752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - chcp.com (PID: 7520 cmdline: chcp 65001 MD5: 41146159AA3D41A92B53ED311EE15693)
    - PING.EXE (PID: 572 cmdline: ping 127.0.0.1 MD5: B3624DD758CCECF93A1226CEF252CA12)
- DllHelper.exe (PID: 7420 cmdline: C:\Users\user\AppVerif\DllHelper.exe MD5: BFEF1ABAB0ACACB7DC9D8828B32CFDE4)
  - InstallUtil.exe (PID: 9100 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: 5D4073B2EB6D217C19F2B22F21BF8D57)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT

```
{
  "Server": "137.74.157.86",
  "Ports": "4449",
  "Version": " 5.0.5",
  "Autorun": "false",
  "Install_Folder": "%AppData%",
  "Install_File": "",
  "AES_key": "AdlbMZFl5HbWg0iu5lqX0wSXQQa8QOLS",
  "Mutex": "ads3",
  "AntiDetection": "null",
  "External_config_on_Pastebin": "false",
  "BDOS": "1",
  "Startup_Delay": "zP7fPronnwucEY5Dp6OPgBbQxf8tJiPByXJ04rcWlJToRK/Y32OI2MU20Hq4rMVqVG/uL5FysKz/0xBrbRqJJA==",
  "HWID": "null",
  "Certificate":
"MIICMzCCAZygAwIBAgIVALgbuadTIXCBGx92qk2Pt658vf8pMA0GCSqGSIb3DQEBDQUAMGcxGDAWBgNVBAMMD1Zlbm9tUkFUIFNlcnZlcjETMBEGA1UECwwKcXdxZGFuY2h1bjEcMBoGA1UECgwTRGNSYXQgQnkgcXdxZGFuY2h1bjELMAkGA1UEBwwCU0gxCzAJBgNVBAYTAkNOMB4XDTIxMDExMjE3MzIzNloXDTMxMTAyMjE3MzIzNlowEDEOMAwGA1UEAwwFRGNSYXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAPLknDSnzkq9SuHSkPVyOxBFVoX/n/Y/SNOD2TO9vxmiaLG1rfOcnt7KPbQA3CJxOmVjCVDvtURayayaErAu6R280hq1HgF3iL7u8+5R9XY6JvXkaiKj2rYiEVKKWU55xGCztKNQAfUY7prw8li8QJk+J8vzitqKS1zz7G2UcGx1AgMBAAGjMjAwMB0GA1UdDgQWBBSyJslOSHG/21uHIrLBFtFJb3nJHzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBDQUAA4GBAG/y6mnqPy3k1abtSAqAnm79siuBJ99b4uxdaTRVNIjATBtYUb3stSpQGefhnzNh4YS6w3SvTZk/BwuWyC0MKvHEbQhbk4JyoIcF4s2wzd5/mcTYK/kwPzAGUp+b93Fp38f3TRgFz+fWVZGheqUlWxzMzV1boXz2JX4pGQTypJBM",
  "ServerSignature":
"eKZENGspnXkrDqiaf/g9a4bTxFDTrVNeU3cFp9wRLJ8NWVUlptiRl8ToeqRS9jPunWKEhdxjsDe0H4qXg9I+nnzookw2XZ89OySClh7WkoBOgKjFz5TA3lLa1ua13At2m1fLiobd36+By2SM4DBQNM+wHUj39Fa7aIAF+t1ovLo=",
  "Group": "false"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000019.00000003.2279210253.000000000F110000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
00000019.00000003.2279210253.000000000F110000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000019.00000003.2279210253.000000000F110000.00000004.00000800.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_WMI_EnumerateVideoDevice	Detects executables attemping to enumerate video devices using WMI	ditekSHen	• 0xd0cc:$q1: Select * from Win32_CacheMemory • 0xd10c:$d1: {860BB310-5D01-11d0-BD3B-00A0C911CE86} • 0xd15a:$d2: {62BE5D10-60EB-11d0-BD3B-00A0C911CE86} • 0xd1a8:$d3: {55272A00-42CB-11CE-8135-00AA004BB851}
00000018.00000003.2241216338.000000000DB30000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
00000018.00000003.2241216338.000000000DB30000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Click to see the 21 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
24.2.DllHelper.exe.1551530.1.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
24.2.DllHelper.exe.1551530.1.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
24.2.DllHelper.exe.1551530.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_WMI_EnumerateVideoDevice	Detects executables attemping to enumerate video devices using WMI	ditekSHen	• 0xd0cc:$q1: Select * from Win32_CacheMemory • 0xd10c:$d1: {860BB310-5D01-11d0-BD3B-00A0C911CE86} • 0xd15a:$d2: {62BE5D10-60EB-11d0-BD3B-00A0C911CE86} • 0xd1a8:$d3: {55272A00-42CB-11CE-8135-00AA004BB851}
25.3.DllHelper.exe.f110000.0.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
25.3.DllHelper.exe.f110000.0.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Click to see the 51 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Observed Malicious SSL Cert (AsyncRAT Variant) - Source IP: 137.74.157.86 - Destination IP: 192.168.11.20

Timestamp:	137.74.157.86192.168.11.204449497602848152 07/12/22-17:58:43.541738
SID:	2848152
Source Port:	4449
Destination Port:	49760
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed Malicious SSL Cert (AsyncRAT) - Source IP: 137.74.157.86 - Destination IP: 192.168.11.20

Timestamp:	137.74.157.86192.168.11.204449497602850454 07/12/22-17:58:43.541738
SID:	2850454
Source Port:	4449
Destination Port:	49760
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Uses ping.exe to check the status of other devices and networks

Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected AsyncRAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Yara detected AsyncRAT

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd or bat file

Malware Analysis System Evasion

Yara detected AsyncRAT

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Yara detected AsyncRAT

Stealing of Sensitive Information

Yara detected DcRat

Remote Access Functionality

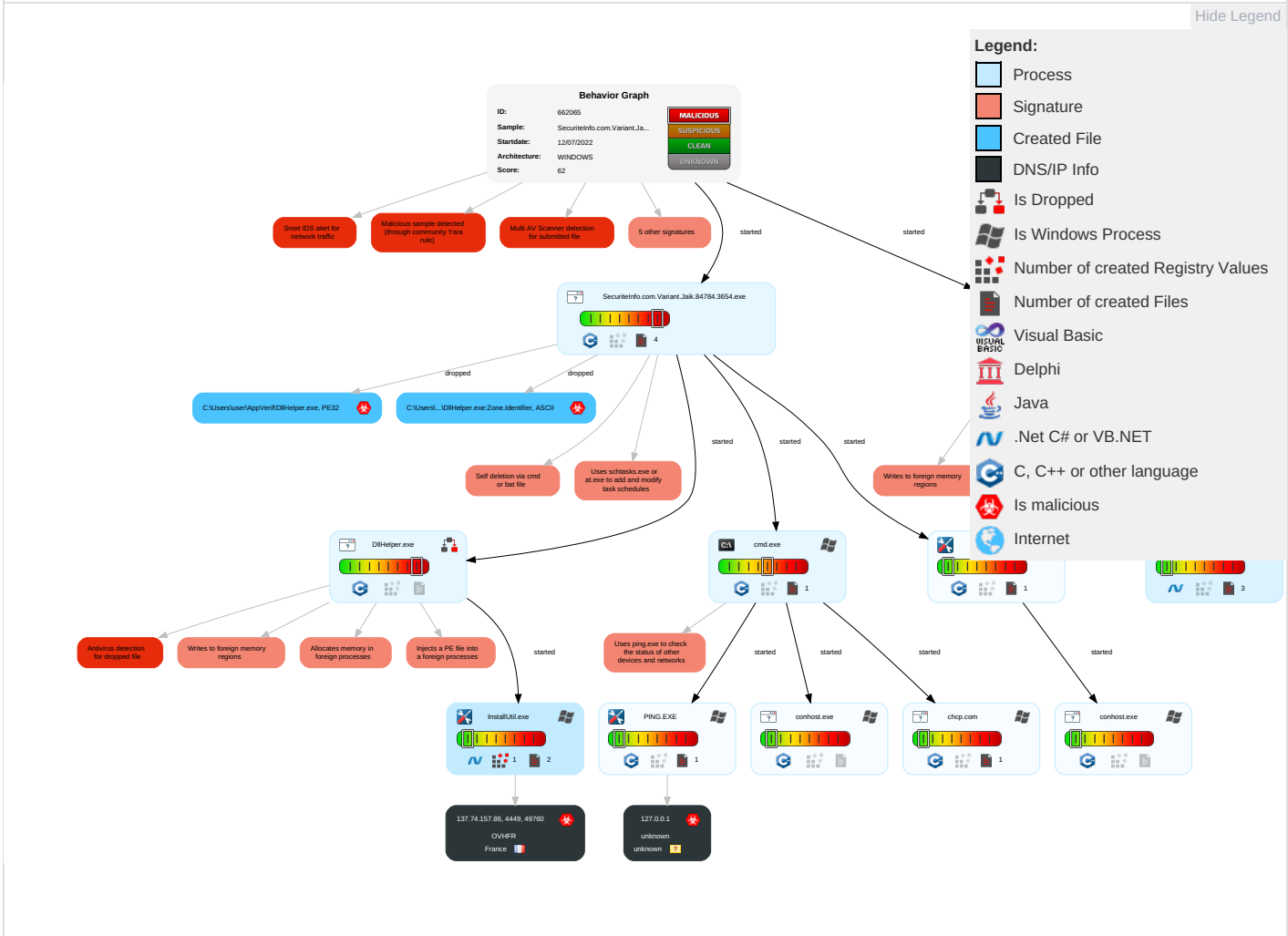
Yara detected DcRat

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 Windows Management Instrumentation	2 Scheduled Task/Job	3 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Scheduled Task/Job	1 DLL Side-Loading	2 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	6 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	Logon Script (Windows)	1 DLL Side-Loading	3 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 2 Process Injection	NTDS	3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 Software Packing	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	2 File and Directory Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	3 4 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

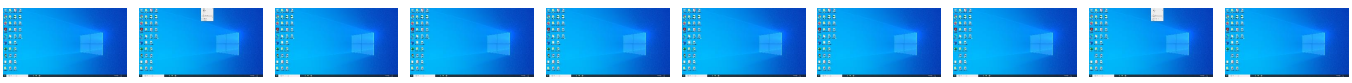
Behavior Graph

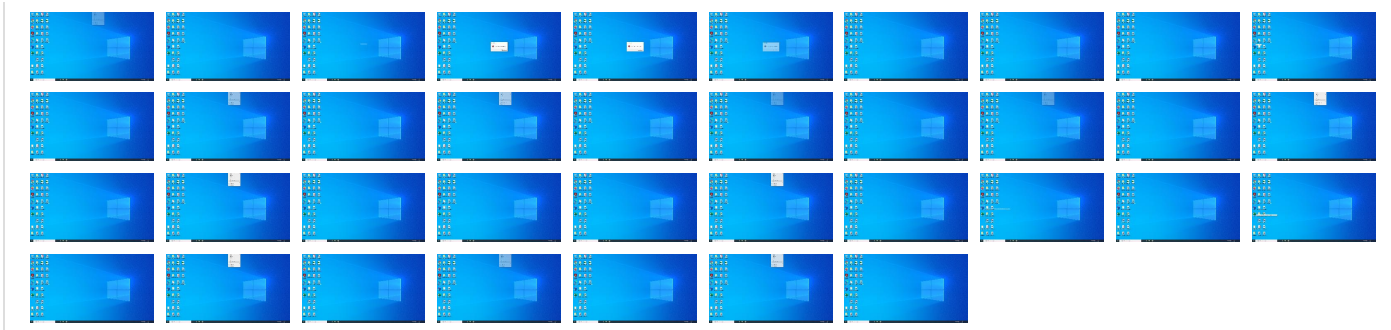


Screenshots

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.Variant.Jaik.84784.3654.exe	59%	Virustotal		Browse
SecuriteInfo.com.Variant.Jaik.84784.3654.exe	69%	ReversingLabs	Win32.Trojan.Jaik	
SecuriteInfo.com.Variant.Jaik.84784.3654.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppVerifi\DllHelper.exe	100%	Avira	TR/Dropper.Gen7	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.3.DllHelper.exe.db30000.0.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
31.2.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1202861		Download File

Source	Detection	Scanner	Label	Link	Download
25.3.DllHelper.exe.f110000.0.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
31.0.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
24.3.DllHelper.exe.db30000.1.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
30.2.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
25.3.DllHelper.exe.f110000.1.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
31.0.InstallUtil.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
30.0.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
30.0.InstallUtil.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1202861		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

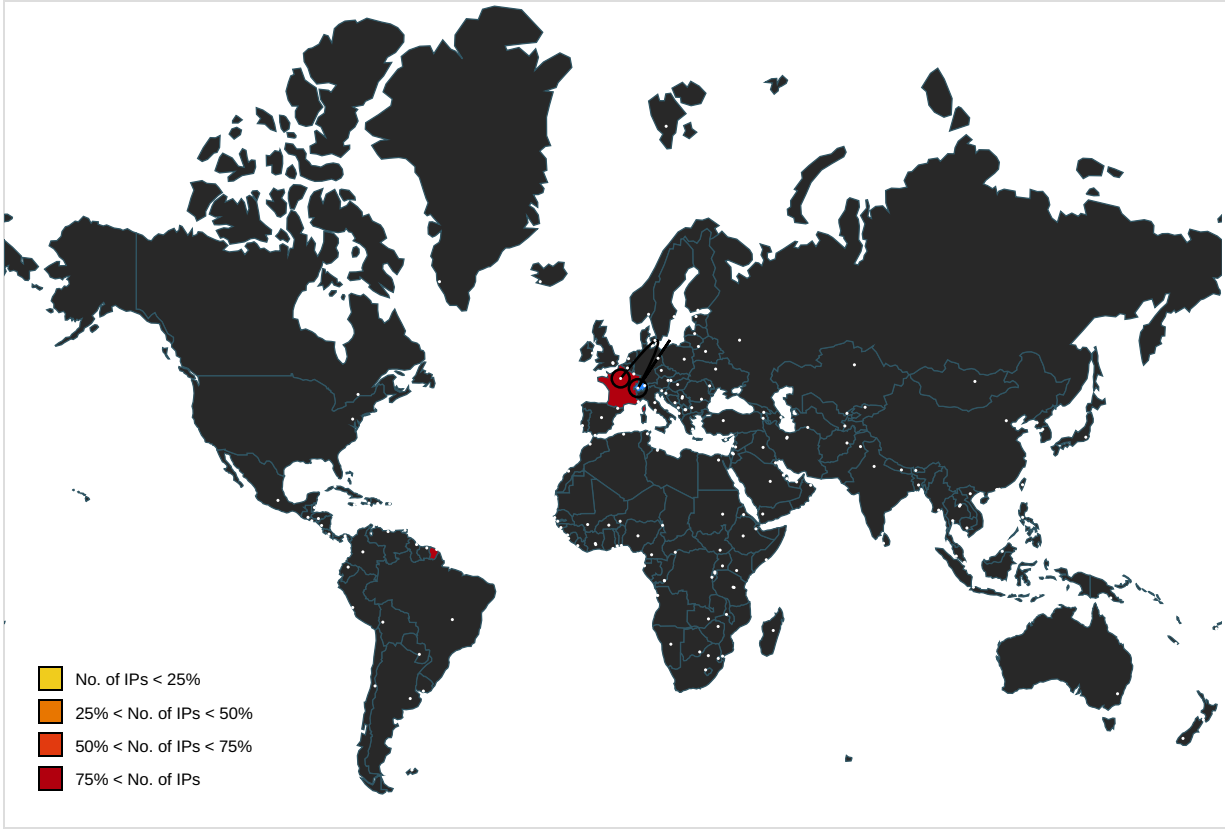
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	InstallUtil.exe, 0000001E.00000002.5754333031.00000000030D0000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000001E.00000002.5747812323.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
137.74.157.86	unknown	France		16276	OVHFR	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	662065
Start date and time: 12/07/202217:52:39	2022-07-12 17:52:39 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 19m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Jaik.84784.3654.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	39
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:	mal62.troj.evad.winEXE@18/4@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 28.6% (good quality ratio 27.1%) • Quality average: 74% • Quality standard deviation: 29.1%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MusNotification.exe, dllhost.exe, RuntimeBroker.exe, SIHClient.exe, backgroundTaskHost.exe, MoUsoCoreWorker.exe, UsoClient.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.82.19.171, 93.184.221.240, 209.197.3.8
- Excluded domains from analysis (whitelisted): fs.microsoft.com, slscr.update.microsoft.com, wu.ec.azureedge.net, settings-win.data.microsoft.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wdcp.microsoft.com, arc.msn.com, wd-prod-cp.trafficmanager.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net, fe3cr.delivery.mp.microsoft.com, ris.api.iris.microsoft.com, wdcpalt.microsoft.com, login.live.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, wd-prod-cp-eu-west-2-fe.westeurope.cloudapp.azure.com, img-prod-cms-rt-microsoft-com.akamaized.net, nexusrules.officeapps.live.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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
17:57:39	Task Scheduler	Run new task: COMSurrogate path: C:\Users\user\AppVerif\DllHelper.exe
17:58:44	API Interceptor	1x Sleep call for process: InstallUtil.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\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.402941568099142
Encrypted:	false
SSDEEP:	6:kKdSQ8Yb+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:gQPNkPlE99SNxAhUeE1
MD5:	C2DBA9ABC6BF0908291C545046D98A63
SHA1:	F5EF21F117B4F19470C243DF5747753B44905B32
SHA-256:	E604D978C3CA33ECFCF47FE2BD012842B71CA3F5E7A21B886F03171DF4DB15F1
SHA-512:	E6CF8576FEB74856F23C6767B4E4CA429C8EE6C0F20775C4C3C4A869710F77182B7BCEAEBF241404FD0E5D4D2EBEE1EDCD98345EDE1786C277ACACC0FD92A5CE
Malicious:	false
Preview:	p..... .....(.....QF.... .....L.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.35152097590267
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPuuOKbbDLI4MWuPJKy2Khav:ML9E4KGbKDE4KhKzKhk
MD5:	8C7889BDE41724CE3DB7C67E730677F6
SHA1:	485891CC9120CB2203A2483754DBD5E6EA24F28E
SHA-256:	83C70BFCB1B41892C9C50CABE9BC2D96B2F7420B28545AFABD32F682AC62D0AD
SHA-512:	B7C3AAB27FC924DCAEF78987B492931E164B9E30B813C532FE87E1D40001ED1861C4B5DDBDD85CD2278681A22E32EEE816877F4F63CECAA9972976D87E38F5CC
Malicious:	false
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\68e52ded8d0e73920808d8880ed14efd\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\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll",0..

C:\Users\user\AppVerif\DllHelper.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	831294376
Entropy (8bit):	0.039372401793613315
Encrypted:	false
SSDEEP:	
MD5:	BFEF1ABAB0ACACB7DC9D8828B32CFDE4
SHA1:	77E8DB7D353194E119A2988D851E98069BD44CAD
SHA-256:	CAE28D2DB2FC7CDFD80CA57DB3A9704AED9685421F194C52A2BEF94D7510A843
SHA-512:	73ABDE477518AC06DCA49303A7B93A5477BBB30BD8056262A15831D748082F4CAFD7163B8D98D3CB4120ACBC178A7557F67B3E4F48F6B4C76B3EA4209AA4B98
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...h..h..h..v...y..v...T..v.....O..k..h.....v...j..v...i..h...i..v...i..Richh.....PE..L....{J.....@.....@.....l...(...`.....x.....@.....text...`..... ..`.data...h1.....@....tenio.....P.....@....rsrc.....`.....@..@.reloc..rG.....H...0.....@..B.....

C:\Users\user\AppVerif\DllHelper.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.789455480828862
TrID:	• Win32 Executable (generic) a (10002005/4) 99.53% • InstallShield setup (43055/19) 0.43% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Variant.Jaik.84784.3654.exe
File size:	1870760
MD5:	74cd3c3d32dcf5029d1bc66347f44af7
SHA1:	d7ec9719a6e5ea0b386ef590b1b74c317e597ff8
SHA256:	cb943da125fde19e41c965a9f260caf79a6fca98c89b83bde609b843be0da377
SHA512:	6b1340641f1f7820755ccc9e78b083ab32444d560274103e21a3ccaf4dee93b62340a6445960dc5a8f09a0de87c138e182a2c1012fdaf4f4d6d39e88922451fe
SSDEEP:	49152:yCu54sLM0OEl6bINMreuk8i09pEkJz5lAcs5PVS7fhl:yCu5OGpQefZ0vfTsfSj
TLSH:	9D851208EA509426F4F7863451F98AADA63C94D71F4845C387E4A3FA866C3D0FE3257B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...h...h...h...v...y...v...T...v.....O...k...h.....v...j...v...i...h...i...v...i...Richh.....PE..L..

File Icon

Icon Hash:	e0ccbcccc2f2e4cc

Static PE Info

General

Entrypoint:	0x40cdb0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x5D280B2C [Fri Jul 12 04:23:08 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	7f1ef45f5deb563bbecd8473c31a66d3

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=R3, O=Let's Encrypt, C=US
Signature Validation Error:	**A certificate chain could not be built to a trusted root authority**
Error Number:	-2146762486
Not Before, Not After	• 23/05/2022 10:32:40 21/08/2022 10:32:39
Subject Chain	• CN=www.artweaver.de
Version:	3
Thumbprint MD5:	BC879E2879685CBEB888E5D32DD8189D
Thumbprint SHA-1:	01B29404E8E3D0019404677B8E9699DF9750B294
Thumbprint SHA-256:	0FA3497022A3B9B10A0B786533C315048B785CDFE262198828BDCAB722017FC9
Serial:	03BB38E009072B417BF8459D28B7B3D18D33

Entrypoint Preview
Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007F1F90B3D85Bh
call 00007F1F90B34EA6h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 0059F440h
push 004112B0h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF94h
push ebx
push esi
push edi
mov eax, dword ptr [005A1338h]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-70h], 00000000h
mov dword ptr [ebp-04h], 00000000h
lea eax, dword ptr [ebp-60h]

Instruction
push eax
call dword ptr [004010C4h]
mov dword ptr [ebp-04h], FFFFFFFEh
jmp 00007F1F90B34EB8h
mov eax, 00000001h
ret
mov esp, dword ptr [ebp-18h]
mov dword ptr [ebp-78h], 000000FFh
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, dword ptr [ebp-78h]
jmp 00007F1F90B34FE7h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007F1F90B35024h
mov dword ptr [ebp-6Ch], eax
push 00000001h
call 00007F1F90B3ED9Ah
add esp, 04h
test eax, eax
jne 00007F1F90B34E9Ch
push 0000001Ch
call 00007F1F90B34FDCh
add esp, 04h
call 00007F1F90B3CAE4h
test eax, eax
jne 00007F1F90B34E9Ch
push 00000010h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C++] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x19fc6c	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a6000	0x21cc8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1c7800	0x13a8	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1c8000	0x19c0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1200	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x82a8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1bc	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19f660	0x19f800	False	0.8492162821525271	data	7.816031131002002	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x1a1000	0x3168	0x1400	False	0.3314453125	data	3.4095039121071826	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tenio	0x1a5000	0x4	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x1a6000	0x21cc8	0x21e00	False	0.8149792435424354	data	7.4602970996808775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1c8000	0x4772	0x4800	False	0.3001844618055556	data	3.257312610228726	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1a6360	0x1608e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x1bc3f0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1c0618	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 16777216, next used block 0		
RT_ICON	0x1c2bc0	0xea8	data		
RT_ICON	0x1c3a68	0x668	data		
RT_ICON	0x1c40d0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1c5178	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 12707524, next used block 13232843		
RT_ICON	0x1c5a20	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2866470365, next used block 64682		
RT_ICON	0x1c5d08	0x988	data		
RT_ICON	0x1c6690	0x6c8	data		
RT_ICON	0x1c6d58	0x1e8	data		
RT_ICON	0x1c6f40	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1c73a8	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1c7910	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1c7a38	0xca	data		
RT_VERSION	0x1c7b08	0x1bc	data		

Imports

DLL	Import
KERNEL32.dll	ExitProcess, GetCommandLineW, SearchPathW, FindVolumeClose, CreateFiber, FreeResource, CreateFileTransactedW, LoadResource, InitializeSListHead, HeapFree, MoveFileWithProgressA, GetModuleHandleW, GetCommConfig, GenerateConsoleCtrlEvent, GetProcessHeap, ClearCommBreak, SetCommTimeouts, LoadLibraryW, SwitchToFiber, GetCalendarInfoW, SetConsoleCursorPosition, GetACP, SetThreadPriority, VerifyVersionInfoW, DeleteFiber, GetLastError, SetLastError, GetProcAddress, GetProcessHeaps, SetConsoleCtrlHandler, SetFileApisToANSI, FoldStringA, GetThreadPriority, DebugSetProcessKillOnExit, WaitCommEvent, EnumSystemGeoID, CloseHandle, MoveFileTransactedW, FindActCtxSectionStringW, ResetWriteWatch, CreateThread, InterlockedIncrement, InterlockedDecrement, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetFullPathNameA, GetStartupInfoW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetModuleFileNameW, HeapValidate, IsBadReadPtr, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, IsDebuggerPresent, GetDriveTypeA, GetOEMCP, GetCPInfo, IsValidCodePage, TlsGetValue, TlsAlloc, TlsSetValue, GetCurrentThreadId, TlsFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, HeapDestroy, HeapCreate, VirtualFree, GetModuleFileNameA, WriteFile, FlushFileBuffers, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, DebugBreak, OutputDebugStringA, WriteConsoleW, OutputDebugStringW, HeapAlloc, HeapSize, HeapReAlloc, VirtualAlloc, InitializeCriticalSectionAndSpinCount, GetCurrentDirectoryA, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, LoadLibraryA, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, SetFilePointer, CreateFileA

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
137.74.157.86192.168.11.204449497602848152 07/12/22-17:58:43.541738	TCP	2848152	ETPRO TROJAN Observed Malicious SSL Cert (AsyncRAT Variant)	4449	49760	137.74.157.86	192.168.11.20
137.74.157.86192.168.11.204449497602850454 07/12/22-17:58:43.541738	TCP	2850454	ETPRO TROJAN Observed Malicious SSL Cert (AsyncRAT)	4449	49760	137.74.157.86	192.168.11.20

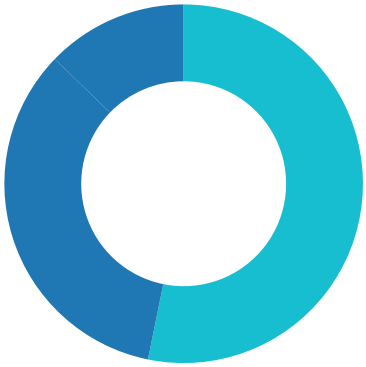
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 12, 2022 17:58:43.468368053 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:43.487335920 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:58:43.487631083 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:43.520340919 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:43.541738033 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:58:43.547988892 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:43.569195032 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:58:43.612924099 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:45.455966949 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:45.519243002 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:58:45.519464016 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:45.581790924 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:58:57.445862055 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:57.519129038 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:58:57.519452095 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:57.540577888 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:58:57.594261885 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:57.613362074 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:58:57.656783104 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:57.795804024 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:57.863199949 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:58:57.863424063 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:58:57.925687075 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:09.396325111 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:09.457000017 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:09.457176924 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:09.477658033 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:09.529151917 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:09.548430920 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:09.591762066 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:09.667908907 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:09.738001108 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:09.738202095 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:09.800726891 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:15.210663080 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:15.262234926 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:15.281449080 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:15.324704885 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:21.586010933 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:21.659635067 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:21.659771919 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:21.680174112 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:21.729585886 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:21.748480082 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:21.792139053 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:21.797532082 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:21.863042116 CEST	4449	49760	137.74.157.86	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 12, 2022 17:59:21.863226891 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:21.925453901 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:33.302330971 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:33.362873077 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:33.363187075 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:33.389679909 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:33.430144072 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:33.449682951 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:33.492542982 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:33.498559952 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:33.581856966 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:33.582079887 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:33.644290924 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:45.210776091 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:45.255635023 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:45.274761915 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:45.318262100 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:45.400360107 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:45.472410917 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:45.472580910 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:45.492846966 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:45.536858082 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:45.556005001 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:45.599385977 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:45.619894028 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:45.691129923 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:45.691438913 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:45.753420115 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:57.191132069 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:57.253688097 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:57.254262924 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:57.275015116 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:57.315433979 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:57.334304094 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:57.377983093 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:57.380475998 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:57.441272020 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 17:59:57.441450119 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 17:59:57.503982067 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 18:00:09.147196054 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 18:00:09.206793070 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 18:00:09.207063913 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 18:00:09.228027105 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 18:00:09.281673908 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 18:00:09.301120043 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 18:00:09.344209909 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 18:00:09.346262932 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 18:00:09.409477949 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 18:00:09.409713984 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 18:00:09.472460032 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 18:00:15.211327076 CEST	4449	49760	137.74.157.86	192.168.11.20
Jul 12, 2022 18:00:15.264772892 CEST	49760	4449	192.168.11.20	137.74.157.86
Jul 12, 2022 18:00:15.284172058 CEST	4449	49760	137.74.157.86	192.168.11.20

Statistics

Behavior



- SecuriteInfo.com.Variant.Jaik.8478…
- schtasks.exe
- conhost.exe
- DllHelper.exe
- DllHelper.exe
- cmd.exe
- conhost.exe
- chcp.com
- PING.EXE
- InstallUtil.exe
- InstallUtil.exe

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Variant.Jaik.84784.3654.exe PID: **7424**, Parent PID: **7300**

General

Target ID:	0
Start time:	17:56:03
Start date:	12/07/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe"
Imagebase:	0xc90000
File size:	1870760 bytes
MD5 hash:	74CD3C3D32DCF5029D1BC66347F44AF7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: schtasks.exe PID: **2612**, Parent PID: **7424**

General

Target ID:	22
Start time:	17:57:36
Start date:	12/07/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\schtasks.exe" /create /tn COMSurrogate /f /sc onlogon /rl highest /tr "C:\Users\user\AppVerif\DllHelper.exe
Imagebase:	0x120000
File size:	187904 bytes
MD5 hash:	478BEAEC1C3A9417272BC8964ADD1CEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Analysis Process: conhost.exe PID: **740**, Parent PID: **2612**

General

Target ID:	23
Start time:	17:57:37
Start date:	12/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ee140000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: DllHelper.exe PID: **7412**, Parent PID: **7424**

General

Target ID:	24
Start time:	17:57:44
Start date:	12/07/2022
Path:	C:\Users\user\AppVerif\DllHelper.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppVerif\DllHelper.exe"
Imagebase:	0xfb0000
File size:	831294376 bytes
MD5 hash:	BFEF1ABAB0ACACB7DC9D8828B32CFDE4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000018.00000003.2241216338.000000000DB30000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000018.00000003.2241216338.000000000DB30000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_WMI_EnumerateVideoDevice, Description: Detects executables attemping to enumerate video devices using WMI, Source: 00000018.00000003.2241216338.000000000DB30000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000018.00000003.2256208402.000000000DB32000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000018.00000003.2265536971.0000000001540000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000018.00000002.2270243732.0000000001540000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: DllHelper.exe PID: **7420**, Parent PID: **1376**

General

Target ID:	25
Start time:	17:57:45
Start date:	12/07/2022
Path:	C:\Users\user\AppVerif\DllHelper.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppVerif\DllHelper.exe
Imagebase:	0xfb0000
File size:	831294376 bytes
MD5 hash:	BFEF1ABAB0ACACB7DC9D8828B32CFDE4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000019.00000003.2279210253.000000000F110000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000019.00000003.2279210253.000000000F110000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_WMI_EnumerateVideoDevice, Description: Detects executables attemping to enumerate video devices using WMI, Source: 00000019.00000003.2279210253.000000000F110000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000019.00000003.2304950340.0000000000AB2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000019.00000002.2306850553.0000000000AB2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000019.00000003.2293118725.000000000F112000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **8812**, Parent PID: **7424**

General

Target ID:	26
Start time:	17:57:46
Start date:	12/07/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe" /c chcp 65001 && ping 127.0.0.1 && DEL /F /S /Q /A "C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe
Imagebase:	0x9b0000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Analysis Process: conhost.exe PID: **7752**, Parent PID: **8812**

General

Target ID:	27
Start time:	17:57:46
Start date:	12/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ee140000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: chcp.com PID: 7520, Parent PID: 8812

General

Target ID:	28
Start time:	17:57:46
Start date:	12/07/2022
Path:	C:\Windows\SysWOW64\chcp.com
Wow64 process (32bit):	true
Commandline:	chcp 65001
Imagebase:	0x790000
File size:	12800 bytes
MD5 hash:	41146159AA3D41A92B53ED311EE15693
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Analysis Process: PING.EXE PID: 572, Parent PID: 8812

General

Target ID:	29
Start time:	17:57:46
Start date:	12/07/2022
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1
Imagebase:	0xe80000
File size:	18944 bytes
MD5 hash:	B3624DD758CCECF93A1226CEF252CA12
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

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

Analysis Process: InstallUtil.exe PID: **8700**, Parent PID: **7412**

General

Target ID:	30
Start time:	17:58:40
Start date:	12/07/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0xa80000
File size:	42064 bytes
MD5 hash:	5D4073B2EB6D217C19F2B22F21BF8D57
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001E.00000002.5733215574.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001E.00000000.2255355229.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001E.00000000.2255974959.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DcRat_2, Description: Yara detected DcRat, Source: 0000001E.00000002.5755782102.0000000003119000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DcRat_2, Description: Yara detected DcRat, Source: 0000001E.00000002.5747812323.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

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	6DDA3263	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	6DDA3263	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6DDA099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6DDA099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DDA099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCF62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6DDAD97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6DDAD97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDAD97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6DCF62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA099B	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DDA099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCF62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCF62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCF62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6CD09B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6CD09B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DCF62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6DDA099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6DDA099B	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\ActiveMovie\devenum	success or wait	1	6DDE44F6	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\ActiveMovie\devenum	Version	dword	7	success or wait	1	6DDE44F6	unknown

Analysis Process: InstallUtil.exe PID: **9100**, Parent PID: **7420**

General

Target ID:	31
Start time:	17:58:44
Start date:	12/07/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x7ff6733e0000
File size:	42064 bytes
MD5 hash:	5D4073B2EB6D217C19F2B22F21BF8D57
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001F.00000000.2292908991.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001F.00000000.2292384259.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001F.00000002.2324411113.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

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	6DDA3263	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DDA3263	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InstallUtil.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E19A037	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\InstallUtil.exe.log	0	425	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 36 38 65 35 32 64 65 64 38 64 30 65 37 33 39 32 30 38 30 38 64 38 38 38 38 30 65 64 31 34 65 66 64 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\68e52ded8d0e73920808d8880ed14efd\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6E19A0C7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6DDA099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6DDA099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DDA099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCF62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6DDAD97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6DDAD97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDAD97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6DCF62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DDA099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCF62DE	ReadFile

Disassembly

No disassembly