ID: 615403
Sample Name:
SecuriteInfo.com.W32.AIDetectNet.01.19723.25833
Cookbook: default.jbs
Time: 07:00:27
Date: 26/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

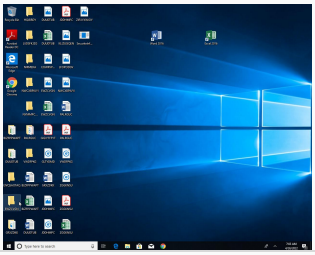
Windows Analysis Report

SecuriteInfo.com.W32.AIDetectNet.01.19723.25833

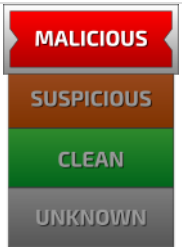
Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetectNet.01.19723.25833 (renamed file extension from 25833 to exe)
Analysis ID:	615403
MD5:	a27c8ee8b37605..
SHA1:	6a8b97217d52a7.
SHA256:	910a6e4138cb42..
Tags:	AgentTesla exe
Infos:	



Detection



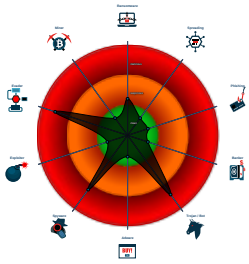
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains very larg…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Queries sensitive BIOS Information…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.W32.AIDetectNet.01.19723.exe (PID: 5840 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19723.exe" MD5: A27C8EE8B37605F3C05E4EB4D614F359)
  - SecuriteInfo.com.W32.AIDetectNet.01.19723.exe (PID: 2508 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19723.exe MD5: A27C8EE8B37605F3C05E4EB4D614F359)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "FTP",
  "FTP Host": "ftp://ftp.unitelha.com/",
  "Username": "kilop@unitelha.com",
  "Password": "Wljp?jjgQwC?"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.371685383.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000000.371685383.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.376573034.0000000003BA5000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.376573034.0000000003BA5000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.378112998.0000000003DD6000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.3dd6c40.9.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.3dd6c40.9.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.3dd6c40.9.raw.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x327e8:$s10: logins • 0x66a08:$s10: logins • 0x3224f:$s11: credential • 0x6646f:$s11: credential • 0x2e82e:$g1: get_Clipboard • 0x62a4e:$g1: get_Clipboard • 0x2e83c:$g2: get_Keyboard • 0x62a5c:$g2: get_Keyboard • 0x2e849:$g3: get_Password • 0x62a69:$g3: get_Password • 0x2fb58:$g4: get_CtrlKeyDown • 0x63d78:$g4: get_CtrlKeyDown • 0x2fb68:$g5: get_ShiftKeyDown • 0x63d88:$g5: get_ShiftKeyDown • 0x2fb79:$g6: get_AltKeyDown • 0x63d99:$g6: get_AltKeyDown
2.0.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.0.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 30 entries				

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

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)
Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Stealing of Sensitive Information

Yara detected AgentTesla
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal browser information (history, passwords, etc)

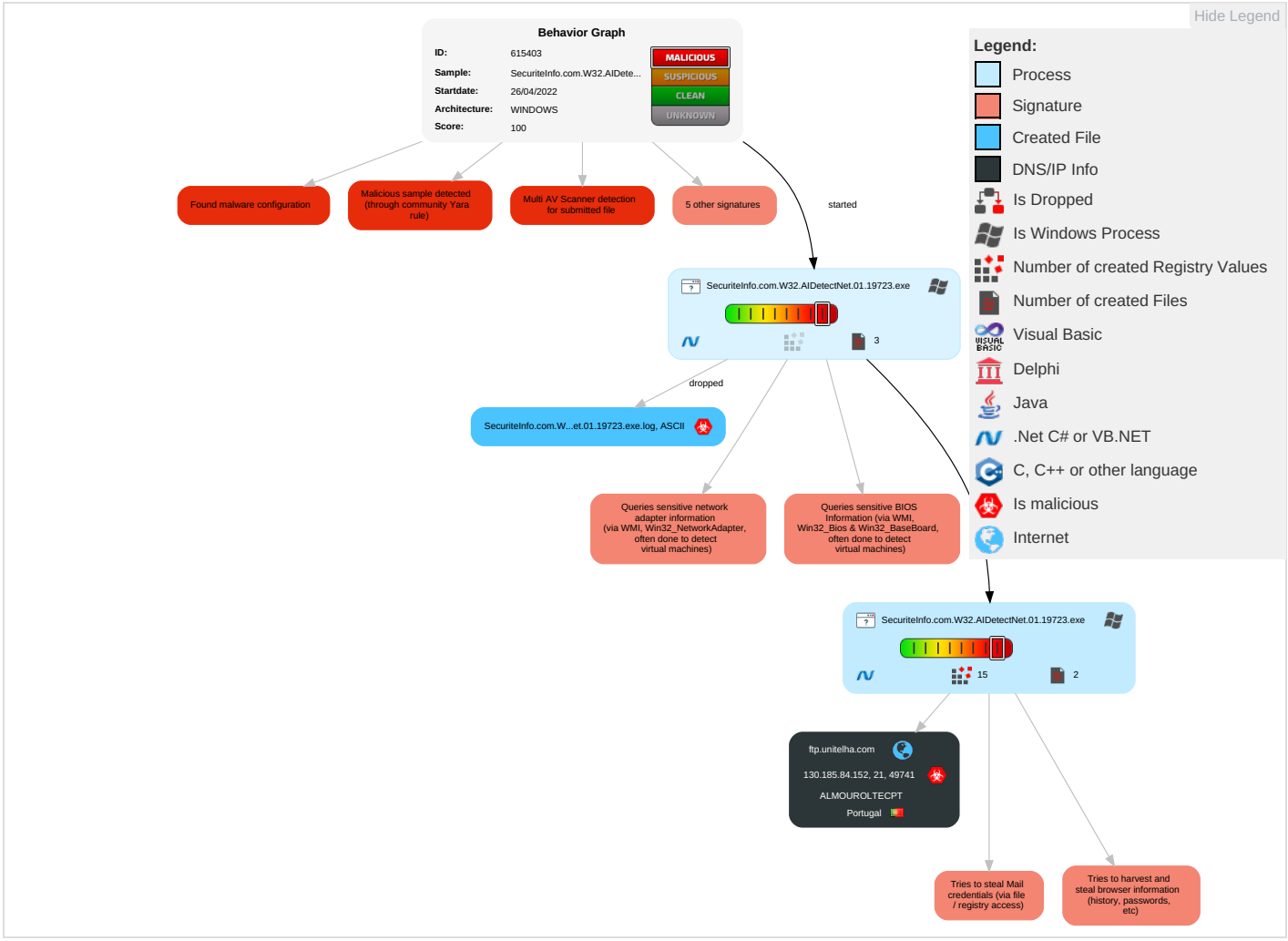
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	1 Exfiltration Over Alternative Protocol	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	1 Process Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	1 Data from Local System	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 Remote System 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	2 Obfuscated Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

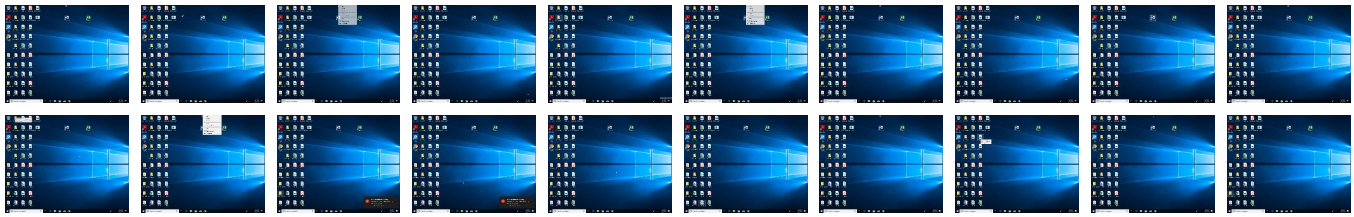
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.W32.AIDetectNet.01.19723.exe	28%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetectNet.01.19723.exe	21%	ReversingLabs	Win32.Trojan.AgentTesla	
SecuriteInfo.com.W32.AIDetectNet.01.19723.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://MaQvjL.com	0%	Avira URL Cloud	safe	
http://ftp.unitelha.com	0%	Avira URL Cloud	safe	
http://ftp://ftp.unitelha.com/kilop	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ftp.unitelha.com	130.185.84.152	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.W32.AIDetectNet.01.19723.exe, 00000002.00000002.633680403.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://MaQvjL.com	SecuriteInfo.com.W32.AIDetectNet.01.19723.exe, 00000002.00000002.633680403.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ftp.unitelha.com	SecuriteInfo.com.W32.AIDetectNet.01.19723.exe, 00000002.00000002.634279983.0000000003338000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.W32.AIDetectNet.01.19723.exe, 00000002.00000002.634267246.000000000332C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ftp://ftp.unitelha.com/kilop	SecuriteInfo.com.W32.AIDetectNet.01.19723.exe, 00000002.00000002.633680403.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	SecuriteInfo.com.W32.AIDetectNet.01.19723.exe, 00000002.00000002.633680403.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	SecuriteInfo.com.W32.AIDetectNet.01.19723.exe, 00000002.00000002.633680403.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
130.185.84.152	ftp.unitelha.com	Portugal		24768	ALMOUROLTECPT	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	615403
Start date and time: 26/04/202207:00:27	2022-04-26 07:00:27 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetectNet.01.19723.25833 (renamed file extension from 25833 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:	18
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@3/1@1/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 48% • Quality standard deviation: 33%

HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target SecuriteInfo.com.W32.AIDetectNet.01.19723.exe, PID 5840 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:01:38	API Interceptor	797x Sleep call for process: SecuriteInfo.com.W32.AIDetectNet.01.19723.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19723.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2271
Entropy (8bit):	5.364115343032043
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvmHKiQHKx1qHxvAHj:iqXeqm00YqhQnouRqjntIxHeqz+qBqxz

MD5:	2AC349459A771367D95FB2E5271E538F
SHA1:	FC9D5F6DDFC0D588E344C98EBC48E37C5E587E77
SHA-256:	0F36341CBF0410D1ACE0A351ABCA5343D2073F92ABC2B54C1E92767B9FCF0074
SHA-512:	9DF1CAC11964291805C7914E319A1C6F73FFCF458EBD32BD615ECD65FB94BC6880461FF60F6589CAB2A165A6C4DCDA83F50E18D965413A0D48A59A1E51B7EAC6
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.856549843950473
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SecuriteInfo.com.W32.AIDetectNet.01.19723.exe
File size:	650240
MD5:	a27c8ee8b37605f3c05e4eb4d614f359
SHA1:	6a8b97217d52a752075b08207bad7d7c867a8854
SHA256:	910a6e4138cb422bf570130f05cdb463d726c0eddb2882bdc6e42fb1daace384
SHA512:	769fe817c1616f80672a63ad8a8464c26aa4374e569343df04feab22a3a1193eac5f7eee5fb3afaa94ed28792da492659c2b02220f0197c1b89641a0d7f9f536
SSDEEP:	12288:STId9kv1FSJqWFQGPHIn0M8h/1JlK4IIIIQqJqi+p:rd9gSqHGPa0L/1JUiIIci0
TLSH:	C8D4122BF354B212CEB507B644567C9199FBBE272137DB8F548C7A29E6333E08A53061
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Ogb.....0.....J.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49fb4a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x62674F11 [Tue Apr 26 01:46:57 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
and byte ptr [eax], al
or al, byte ptr [eax]
or eax, 2D000900h
add byte ptr [eax], dh
add byte ptr [ecx], dh
add byte ptr [edx], dh
add byte ptr [ebx], dh
add byte ptr [eax+eax], dh
xor eax, 37003600h
add byte ptr [eax], bh
add byte ptr [ecx], bh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9faf8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa0000	0x5b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9db70	0x9dc00	False	0.908947541105	data	7.87323976123	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa0000	0x5b0	0x800	False	0.318359375	data	3.30301138268	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa2000	0xc	0x400	False	0.025390625	data	0.0558553080537	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa0090	0x320	data		
RT_MANIFEST	0xa03c0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

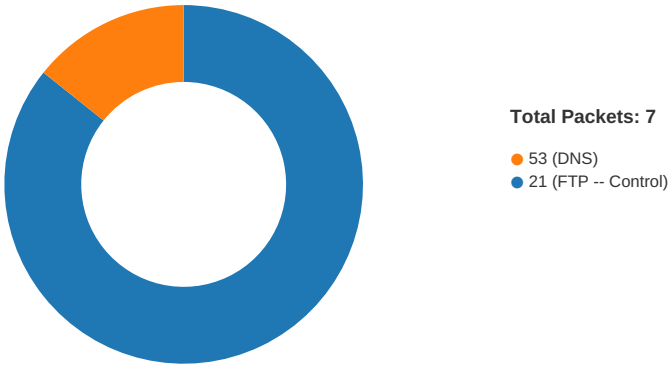
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Soltys 2010
Assembly Version	1.0.0.0
InternalName	CALLC.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	dotXMLTools
ProductVersion	1.0.0.0
FileDescription	dotXMLTools
OriginalFilename	CALLC.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2022 07:01:56.847805023 CEST	49741	21	192.168.2.6	130.185.84.152

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2022 07:01:56.895060062 CEST	21	49741	130.185.84.152	192.168.2.6
Apr 26, 2022 07:01:56.895224094 CEST	49741	21	192.168.2.6	130.185.84.152
Apr 26, 2022 07:01:56.915653944 CEST	49741	21	192.168.2.6	130.185.84.152
Apr 26, 2022 07:01:56.945121050 CEST	21	49741	130.185.84.152	192.168.2.6
Apr 26, 2022 07:01:56.945218086 CEST	49741	21	192.168.2.6	130.185.84.152
Apr 26, 2022 07:01:56.963036060 CEST	21	49741	130.185.84.152	192.168.2.6
Apr 26, 2022 07:01:56.963162899 CEST	49741	21	192.168.2.6	130.185.84.152
Apr 26, 2022 07:01:56.963299990 CEST	21	49741	130.185.84.152	192.168.2.6
Apr 26, 2022 07:01:56.963385105 CEST	49741	21	192.168.2.6	130.185.84.152

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2022 07:01:56.730844975 CEST	50958	53	192.168.2.6	8.8.8.8
Apr 26, 2022 07:01:56.757020950 CEST	53	50958	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 26, 2022 07:01:56.730844975 CEST	192.168.2.6	8.8.8.8	0xcc6c	Standard query (0)	ftp.unitelha.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 26, 2022 07:01:56.757020950 CEST	8.8.8.8	192.168.2.6	0xcc6c	No error (0)	ftp.unitelha.com		130.185.84.152	A (IP address)	IN (0x0001)

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 26, 2022 07:01:56.945121050 CEST	21	49741	130.185.84.152	192.168.2.6	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 23 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 23 of 50 allowed.220-Local time is now 06:01. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 23 of 50 allowed.220-Local time is now 06:01. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 23 of 50 allowed.220-Local time is now 06:01. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 23 of 50 allowed.220-Local time is now 06:01. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Apr 26, 2022 07:01:56.963036060 CEST	21	49741	130.185.84.152	192.168.2.6	220 Logout.

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.19723.exe PID: **5840**, Parent PID: **5336**

General

Target ID:	1
Start time:	07:01:36
Start date:	26/04/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19723.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19723.exe"
Imagebase:	0x720000
File size:	650240 bytes
MD5 hash:	A27C8EE8B37605F3C05E4EB4D614F359
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.376573034.0000000003BA5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.376573034.0000000003BA5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.378112998.0000000003DD6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.378112998.0000000003DD6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.375601643.0000000002BFE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.375072023.0000000002AB1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA5CF06	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	6DA5CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD6C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.19723.exe.log	0	2271	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	6DD6C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml.Linq\f54e3a73bfefb71eb6e1de09129af7f0\System.Xml.Linq.ni.dll.aux	unknown	872	success or wait	1	6D9903DE	ReadFile

Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.19723.exe PID: 2508, Parent PID: 5840

General

Target ID:	2
Start time:	07:01:39
Start date:	26/04/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19723.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.19723.exe
Imagebase:	0xbf0000
File size:	650240 bytes
MD5 hash:	A27C8EE8B37605F3C05E4EB4D614F359
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.371685383.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.371685383.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.371337269.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.371337269.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.372498524.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.372498524.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.372086381.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.372086381.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.632505310.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.632505310.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.633680403.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.633680403.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA5CF06	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	6DA5CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	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	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C0B1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\98bd75d2-ce84-459a-aada-2da99aef3201	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C0B1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C0B1B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly