ID: 412365
Sample Name: 6Rn5G1VWPB
Cookbook: default.jbs
Time: 16:39:38
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

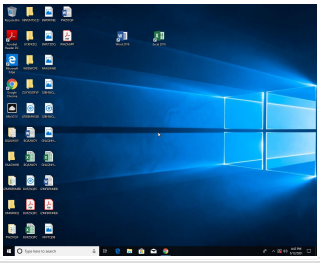
Analysis Report 6Rn5G1VWPB

Overview

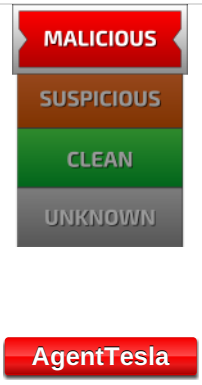
General Information

Sample Name:	6Rn5G1VWPB (renamed file extension from none to exe)
Analysis ID:	412365
MD5:	c12fea2da39e517.
SHA1:	ef3754b85ecd9f7..
SHA256:	19f2d4a6fe01ce9..
Infos:	

Most interesting Screenshot:



Detection

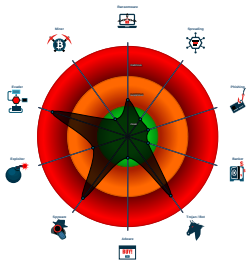


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- 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…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- 6Rn5G1VWPB.exe (PID: 6004 cmdline: 'C:\Users\user\Desktop\6Rn5G1VWPB.exe' MD5: C12FEA2DA39E5173FA674AB5E22A928F)
  - 6Rn5G1VWPB.exe (PID: 6488 cmdline: C:\Users\user\Desktop\6Rn5G1VWPB.exe MD5: C12FEA2DA39E5173FA674AB5E22A928F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "info@garciadelacruz.comsc9v6b2nmail.garciadelacruz.comwilliamslucy570@gmail.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.912960268.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.912960268.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.657613935.0000000003A71000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.657613935.0000000003A71000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.657207704.0000000002ABF000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 6 entries

Copyright Joe Security LLC 2021

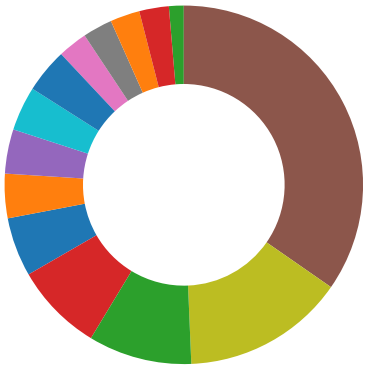
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.6Rn5G1VWPB.exe.3b28798.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.6Rn5G1VWPB.exe.3b28798.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.2.6Rn5G1VWPB.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.6Rn5G1VWPB.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.6Rn5G1VWPB.exe.3b28798.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted 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:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Copyright Joe Security LLC 2021

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)

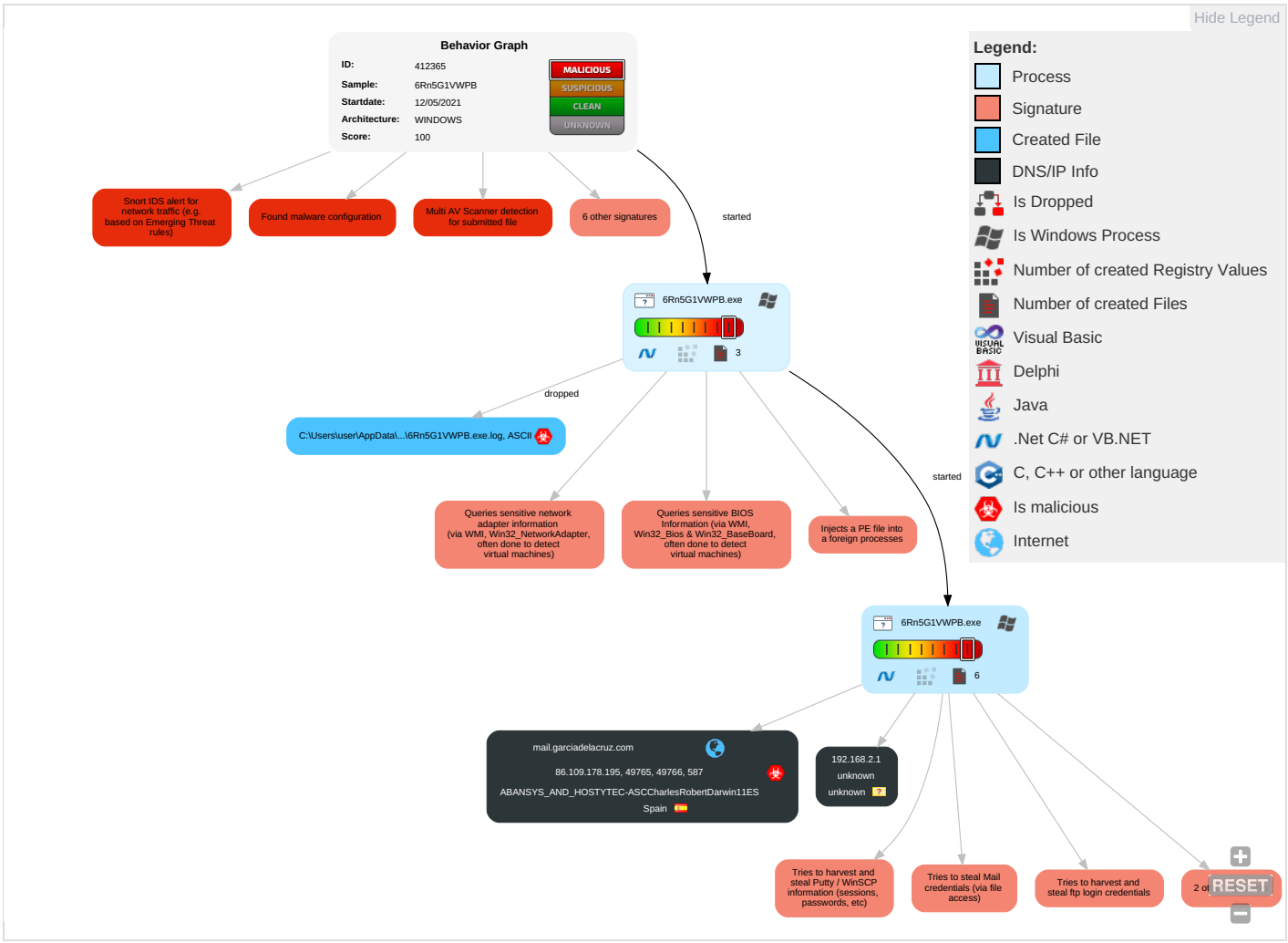
Remote Access Functionality:

- 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	Comm and C
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encry Chan
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1 1 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth	Non-S Port
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Credentials in Registry 1	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Appli Layer Proto
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Appli Layer Proto
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallba Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multit Comr
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comr Used

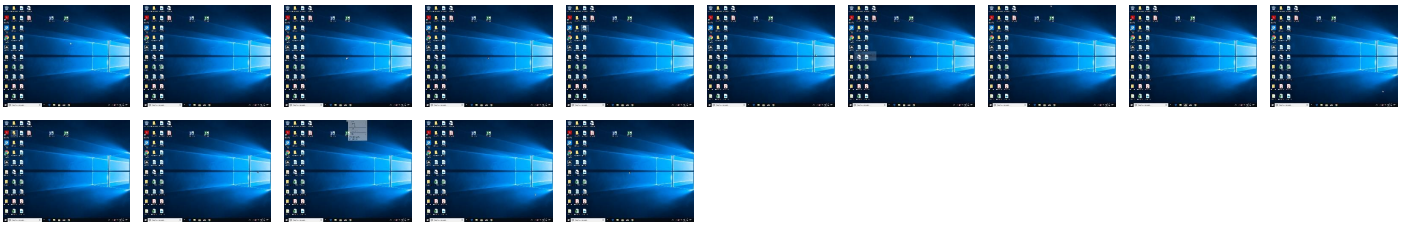
Behavior Graph



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
6Rn5G1VWPB.exe	27%	Virustotal		Browse
6Rn5G1VWPB.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.6Rn5G1VWPB.exe.400000.0.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://DynDns.comDynDNS	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
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%	Virustotal		Browse
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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://EPtbzE.com	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://mail.garciadelacruz.com	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/report/reporter_index.php?name=	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://servermanager.miixit.org/	0%	Avira URL Cloud	safe	
http://ThqqlGVRjff9puHH.com	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	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

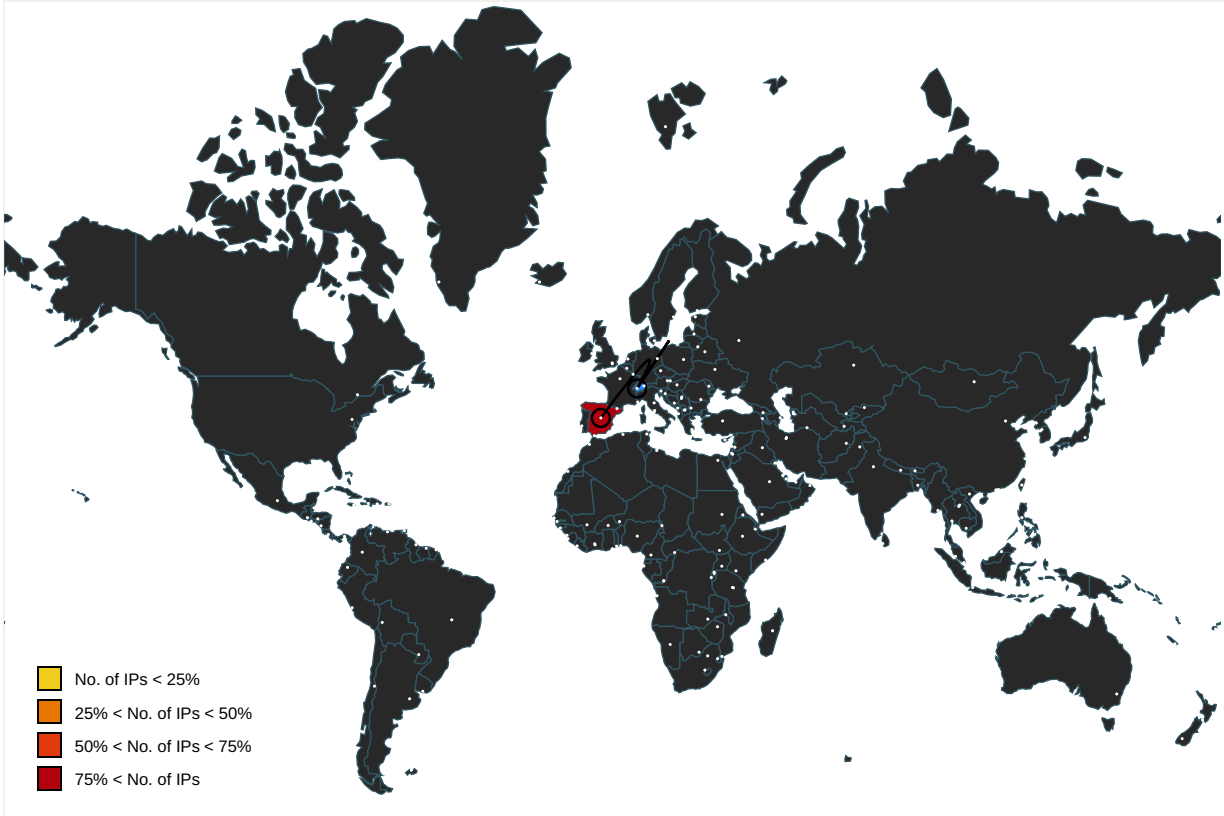
Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.garciadelacruz.com	86.109.178.195	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	6Rn5G1VWPB.exe, 00000002.00000002.915088523.0000000002CF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	6Rn5G1VWPB.exe, 00000002.00000002.915088523.0000000002CF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org/	6Rn5G1VWPB.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	6Rn5G1VWPB.exe, 00000002.00000002.915088523.0000000002CF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://EPtbzE.com	6Rn5G1VWPB.exe, 00000002.00000002.915088523.0000000002CF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=1	6Rn5G1VWPB.exe	false	• Avira URL Cloud: safe	unknown
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC	6Rn5G1VWPB.exe	false		high
http://servermanager.miixit.org/E	6Rn5G1VWPB.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/index_ru.html	6Rn5G1VWPB.exe	false	• Avira URL Cloud: safe	unknown
http://mail.garciadelacruz.com	6Rn5G1VWPB.exe, 00000002.00000002.915860392.000000000305E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://servermanager.miixit.org/report/reporter_index.php?name=	6Rn5G1VWPB.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	6Rn5G1VWPB.exe, 00000002.00000002.915088523.0000000002CF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://servermanager.miixit.org/	6Rn5G1VWPB.exe	false	• Avira URL Cloud: safe	unknown
http://ThqqlGVRjff9puHH.com	6Rn5G1VWPB.exe, 00000002.00000002.915088523.0000000002CF1000.00000004.00000001.sdmp, 6Rn5G1VWPB.exe, 00000002.00000002.915918195.000000000306D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	6Rn5G1VWPB.exe, 00000000.00000002.657132516.0000000002A71000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/index_ru.htmlk	6Rn5G1VWPB.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	6Rn5G1VWPB.exe, 00000000.00000002.657613935.0000000003A71000.00000004.00000001.sdmp, 6Rn5G1VWPB.exe, 00000002.00000002.912960268.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	6Rn5G1VWPB.exe, 00000000.00000002.657207704.0000000002ABF000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/downloads/	6Rn5G1VWPB.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=	6Rn5G1VWPB.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%$	6Rn5G1VWPB.exe, 00000002.00000002.915088523.0000000002CF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
86.109.178.195	mail.garciadelacruz.com	Spain		196713	ABANSYS_AND_HOSTYTEC-ASCCharlesRobertDarwin11ES	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412365
Start date:	12.05.2021
Start time:	16:39:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6Rn5G1VWPB (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/2@2/2
EGA Information:	• Successful, ratio: 100%
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

Copyright Joe Security LLC 2021

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.147.198.201, 20.50.102.62, 52.155.217.156, 20.54.26.129, 2.20.143.16, 2.20.142.209, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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
16:40:28	API Interceptor	709x Sleep call for process: 6Rn5G1VWPB.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
86.109.178.195	Facturas_DHL.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.garciadelacruz.com	Facturas_DHL.exe	Get hash	malicious	Browse	• 86.109.178.195

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ABANSYS_AND_HOSTYTEC-ASCCharlesRobertDarwin11ES	Facturas_DHL.exe	Get hash	malicious	Browse	• 86.109.178.195
	Documentation__UC8G8HI9.doc	Get hash	malicious	Browse	• 86.109.178.160
	Documentation__UC8G8HI9.doc	Get hash	malicious	Browse	• 86.109.178.160
	rzx0Vt5BFs.doc	Get hash	malicious	Browse	• 86.109.178.160
	764829483582_2019_04_12.doc	Get hash	malicious	Browse	• 86.109.170.198
	764829483582_2019_04_12.doc	Get hash	malicious	Browse	• 86.109.170.198
	http://mavitec.es/TINxe-Od_FYMO-c5/ZS91/invoicing/En_us/Companies-Invoice-1220317	Get hash	malicious	Browse	• 86.109.167.210

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fee-docs.doc	Get hash	malicious	Browse	• 86.109.170.194
	fee-docs.doc	Get hash	malicious	Browse	• 86.109.170.194
	fee-docs.doc	Get hash	malicious	Browse	• 86.109.170.194
	fee-docs.doc	Get hash	malicious	Browse	• 86.109.170.194
	FILE-679339.pdf	Get hash	malicious	Browse	• 86.109.167.76
	DHL number - Mittwoch, 15_00-18_00 Uhr.doc	Get hash	malicious	Browse	• 86.109.170.57
	DHL number - Mittwoch, 15_00-18_00 Uhr.doc	Get hash	malicious	Browse	• 86.109.170.57
	emotet_36.doc	Get hash	malicious	Browse	• 86.109.170.12
	emotet_36.doc	Get hash	malicious	Browse	• 86.109.170.12
	http://l.e.lastlap.com/rts/go2.aspx?h=700033&tp=i-H43-Q4x-J7o-GuCmL-5V-A14-1c-GuWPV-FWem8	Get hash	malicious	Browse	• 86.109.162.135
	http://l.e.lastlap.com/rts/go2.aspx?h=700033&tp=i-H43-Q4x-J7o-GuJdM-5V-Vn2-1c-GuWPV-3WGdU	Get hash	malicious	Browse	• 86.109.162.135
	Scan1782384.doc	Get hash	malicious	Browse	• 86.109.161.249
	Scan1782384.doc	Get hash	malicious	Browse	• 86.109.161.249

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6Rn5G1VWPB.exe.log	
Process:	C:\Users\user\Desktop\6Rn5G1VWPB.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
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\Roaming\ikffln5u.f20\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\6Rn5G1VWPB.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Roaming\ikffln5u.f20\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):	7.694119021117804
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	6Rn5G1VWPB.exe
File size:	1162752
MD5:	c12fea2da39e5173fa674ab5e22a928f
SHA1:	ef3754b85ecd9f789bc9bbf8a8c6b36be41cc996
SHA256:	19f2d4a6fe01ce9e0bc8362933e41f0d707df28bf9ab662db7dc7504aef3845a
SHA512:	26bd4ff8262c9b5bb684889ab89b373a10f33b9fe61b88ee0ec7bea69390e1c461b62c17280f3e2e68ef48cce67be523559647552d6fdae1fd9b166e82f9ff0e
SSDEEP:	24576:N6bI6jw9IkyU4BbYDW/X/4W7TPds2fSc8SfhJAwIdvLe6:0ESkkEkl7DdsDc5+VdvL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...w..`.....P..0.....N... ...`....@.. ....@.....

File Icon

Icon Hash:	d28ab3b0e0ab96c4

Static PE Info

General

Entrypoint:	0x4f4eb2
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:	0x609BC077 [Wed May 12 11:48:07 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

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
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

Copyright Joe Security LLC 2021

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf4e60	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf6000	0x288f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x120000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xf4d28	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
.text	0x2000	0xf2eb8	0xf3000	False	0.913331082819	data	7.89681221538	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xf6000	0x288f8	0x28a00	False	0.348028846154	data	5.39732699522	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x120000	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	0xf62b0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x106ad8	0x94a8	data		
RT_ICON	0x10ff80	0x5488	data		
RT_ICON	0x115408	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0x119630	0x25a8	data		
RT_ICON	0x11bbd8	0x10a8	data		
RT_ICON	0x11cc80	0x988	data		
RT_ICON	0x11d608	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x11da70	0x76	data		
RT_GROUP_ICON	0x11dae8	0x14	data		
RT_VERSION	0x11dafc	0x394	data		
RT_MANIFEST	0x11de90	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	Macroeconomist
Assembly Version	4.1.2.1
InternalName	NullableMarshaler.exe
FileVersion	4.1.2.1
CompanyName	Macroeconomist 2021
LegalTrademarks	
Comments	
ProductName	GlobalizationExtensions
ProductVersion	4.1.2.1
FileDescription	GlobalizationExtensions
OriginalFilename	NullableMarshaler.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-16:42:13.863185	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49765	587	192.168.2.4	86.109.178.195
05/12/21-16:42:16.929135	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49766	587	192.168.2.4	86.109.178.195

Network Port Distribution

Total Packets: 71

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:42:13.134754896 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.211566925 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:13.211824894 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.377419949 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:13.378144026 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.454828024 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:13.455018044 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:13.456748009 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.535165071 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:13.535989046 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.617292881 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:13.619561911 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.697374105 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:13.697834969 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.781431913 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:13.781960964 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.860829115 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:13.863184929 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.863420963 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.864106894 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.864223957 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:13.940037012 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:13.940723896 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:14.269522905 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:14.318522930 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:15.774117947 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:15.851397991 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:15.852571011 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:15.853324890 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:15.853451967 CEST	49765	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:15.933919907 CEST	587	49765	86.109.178.195	192.168.2.4
May 12, 2021 16:42:16.297874928 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.374768019 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:16.374926090 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.454835892 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:16.455365896 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.532181978 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:16.532442093 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:16.535346985 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.612245083 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:16.612946033 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.690330029 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:16.690743923 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.767704010 CEST	587	49766	86.109.178.195	192.168.2.4

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:42:16.768399000 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.846424103 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:16.846874952 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.926548004 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:16.928909063 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.929135084 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.929260969 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.929411888 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.929640055 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.929826021 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.929915905 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:16.930042982 CEST	49766	587	192.168.2.4	86.109.178.195
May 12, 2021 16:42:17.007592916 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:17.008039951 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:17.008965969 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:17.008979082 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:17.420620918 CEST	587	49766	86.109.178.195	192.168.2.4
May 12, 2021 16:42:17.475102901 CEST	49766	587	192.168.2.4	86.109.178.195

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:40:18.445195913 CEST	58028	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:18.495414019 CEST	53	58028	8.8.8.8	192.168.2.4
May 12, 2021 16:40:19.896186113 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:19.944896936 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 16:40:20.977637053 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:21.030966997 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 16:40:22.337939978 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:22.389678001 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 16:40:23.664412022 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:23.717228889 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 16:40:24.927752018 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:24.980926037 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 16:40:26.547545910 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:26.599379063 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 16:40:27.727233887 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:27.775940895 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 16:40:30.397442102 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:30.446260929 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 16:40:31.586272001 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:31.635117054 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 16:40:32.475155115 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:32.532696962 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 16:40:33.587733984 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:33.647283077 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 16:40:34.448817015 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:34.500467062 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 16:40:35.432074070 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:35.480787992 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 16:40:37.240926027 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:37.289674044 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 16:40:38.215845108 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:38.276186943 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 16:40:39.350717068 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:39.400345087 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 16:40:42.640199900 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:42.689085960 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 16:40:47.615437031 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 16:40:47.675681114 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 16:41:03.036144018 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:03.250905037 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 16:41:03.817640066 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:03.877968073 CEST	53	61522	8.8.8.8	192.168.2.4

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:41:04.456588984 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:04.546590090 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 16:41:04.760132074 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:04.817827940 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 16:41:04.977973938 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:05.036331892 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 16:41:05.634725094 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:05.683474064 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 16:41:06.247292995 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:06.304621935 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 16:41:06.758164883 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:06.820440054 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 16:41:07.621284008 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:07.680427074 CEST	53	56448	8.8.8.8	192.168.2.4
May 12, 2021 16:41:08.857274055 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:08.914813042 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 16:41:09.355947018 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:09.413249016 CEST	53	62420	8.8.8.8	192.168.2.4
May 12, 2021 16:41:12.174837112 CEST	60579	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:12.236542940 CEST	53	60579	8.8.8.8	192.168.2.4
May 12, 2021 16:41:22.057522058 CEST	50183	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:22.117943048 CEST	53	50183	8.8.8.8	192.168.2.4
May 12, 2021 16:41:22.240628958 CEST	61531	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:22.299323082 CEST	53	61531	8.8.8.8	192.168.2.4
May 12, 2021 16:41:24.312402964 CEST	49228	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:24.371192932 CEST	53	49228	8.8.8.8	192.168.2.4
May 12, 2021 16:41:58.178168058 CEST	59794	53	192.168.2.4	8.8.8.8
May 12, 2021 16:41:58.235702991 CEST	53	59794	8.8.8.8	192.168.2.4
May 12, 2021 16:42:00.238121033 CEST	55916	53	192.168.2.4	8.8.8.8
May 12, 2021 16:42:00.304614067 CEST	53	55916	8.8.8.8	192.168.2.4
May 12, 2021 16:42:12.913924932 CEST	52752	53	192.168.2.4	8.8.8.8
May 12, 2021 16:42:13.008151054 CEST	53	52752	8.8.8.8	192.168.2.4
May 12, 2021 16:42:16.233340979 CEST	60542	53	192.168.2.4	8.8.8.8
May 12, 2021 16:42:16.293699980 CEST	53	60542	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 16:42:12.913924932 CEST	192.168.2.4	8.8.8.8	0xf629	Standard query (0)	mail.garci adelacruz.com	A (IP address)	IN (0x0001)
May 12, 2021 16:42:16.233340979 CEST	192.168.2.4	8.8.8.8	0xe06	Standard query (0)	mail.garci adelacruz.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 16:42:13.008151054 CEST	8.8.8.8	192.168.2.4	0xf629	No error (0)	mail.garci adelacruz.com		86.109.178.195	A (IP address)	IN (0x0001)
May 12, 2021 16:42:16.293699980 CEST	8.8.8.8	192.168.2.4	0xe06	No error (0)	mail.garci adelacruz.com		86.109.178.195	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 16:42:13.377419949 CEST	587	49765	86.109.178.195	192.168.2.4	220 h0226.hostytec.com ESMTP Postfix
May 12, 2021 16:42:13.378144026 CEST	49765	587	192.168.2.4	86.109.178.195	EHLO 813848
May 12, 2021 16:42:13.455018044 CEST	587	49765	86.109.178.195	192.168.2.4	250-h0226.hostytec.com 250-PIPELINING 250-SIZE 20480000 250-ETRN 250-STARTTLS 250-AUTH DIGEST-MD5 CRAM-MD5 PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 CHUNKING
May 12, 2021 16:42:13.456748009 CEST	49765	587	192.168.2.4	86.109.178.195	AUTH login aW5mb0BnYXJjaWFkZWxhY3J1ei5jb20=

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 16:42:13.535165071 CEST	587	49765	86.109.178.195	192.168.2.4	334 UGFzc3dvcmQ6
May 12, 2021 16:42:13.617292881 CEST	587	49765	86.109.178.195	192.168.2.4	235 2.7.0 Authentication successful
May 12, 2021 16:42:13.619561911 CEST	49765	587	192.168.2.4	86.109.178.195	MAIL FROM:<info@garciadelacruz.com>
May 12, 2021 16:42:13.697374105 CEST	587	49765	86.109.178.195	192.168.2.4	250 2.1.0 Ok
May 12, 2021 16:42:13.697834969 CEST	49765	587	192.168.2.4	86.109.178.195	RCPT TO:<williamslucy570@gmail.com>
May 12, 2021 16:42:13.781431913 CEST	587	49765	86.109.178.195	192.168.2.4	250 2.1.5 Ok
May 12, 2021 16:42:13.781960964 CEST	49765	587	192.168.2.4	86.109.178.195	DATA
May 12, 2021 16:42:13.860829115 CEST	587	49765	86.109.178.195	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
May 12, 2021 16:42:13.864223957 CEST	49765	587	192.168.2.4	86.109.178.195	.
May 12, 2021 16:42:14.269522905 CEST	587	49765	86.109.178.195	192.168.2.4	250 2.0.0 Ok: queued as B83851082C54E
May 12, 2021 16:42:15.774117947 CEST	49765	587	192.168.2.4	86.109.178.195	QUIT
May 12, 2021 16:42:15.851397991 CEST	587	49765	86.109.178.195	192.168.2.4	221 2.0.0 Bye
May 12, 2021 16:42:16.454835892 CEST	587	49766	86.109.178.195	192.168.2.4	220 h0226.hostytec.com ESMTP Postfix
May 12, 2021 16:42:16.455365896 CEST	49766	587	192.168.2.4	86.109.178.195	EHLO 813848
May 12, 2021 16:42:16.532442093 CEST	587	49766	86.109.178.195	192.168.2.4	250-h0226.hostytec.com 250-PIPELINING 250-SIZE 20480000 250-ETRN 250-STARTTLS 250-AUTH DIGEST-MD5 CRAM-MD5 PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 CHUNKING
May 12, 2021 16:42:16.535346985 CEST	49766	587	192.168.2.4	86.109.178.195	AUTH login aW5mb0BnYXJjaWFkZWxhY3J1ei5jb20=
May 12, 2021 16:42:16.612245083 CEST	587	49766	86.109.178.195	192.168.2.4	334 UGFzc3dvcmQ6
May 12, 2021 16:42:16.690330029 CEST	587	49766	86.109.178.195	192.168.2.4	235 2.7.0 Authentication successful
May 12, 2021 16:42:16.690743923 CEST	49766	587	192.168.2.4	86.109.178.195	MAIL FROM:<info@garciadelacruz.com>
May 12, 2021 16:42:16.767704010 CEST	587	49766	86.109.178.195	192.168.2.4	250 2.1.0 Ok
May 12, 2021 16:42:16.768399000 CEST	49766	587	192.168.2.4	86.109.178.195	RCPT TO:<williamslucy570@gmail.com>
May 12, 2021 16:42:16.846424103 CEST	587	49766	86.109.178.195	192.168.2.4	250 2.1.5 Ok
May 12, 2021 16:42:16.846874952 CEST	49766	587	192.168.2.4	86.109.178.195	DATA
May 12, 2021 16:42:16.926548004 CEST	587	49766	86.109.178.195	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
May 12, 2021 16:42:16.930042982 CEST	49766	587	192.168.2.4	86.109.178.195	.
May 12, 2021 16:42:17.420620918 CEST	587	49766	86.109.178.195	192.168.2.4	250 2.0.0 Ok: queued as C80EF108681F7

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: 6Rn5G1VWPB.exe PID: 6004 Parent PID: 5956

General

Start time:	16:40:26
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\6Rn5G1VWPB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\6Rn5G1VWPB.exe'
Imagebase:	0x620000
File size:	1162752 bytes
MD5 hash:	C12FEA2DA39E5173FA674AB5E22A928F
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: 00000000.00000002.657613935.0000000003A71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.657613935.0000000003A71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.657207704.0000000002ABF000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6Rn5G1VWPB.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6Rn5G1VWPB.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	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile

Analysis Process: 6Rn5G1VWPB.exe PID: 6488 Parent PID: 6004

General

Start time:	16:40:30
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\6Rn5G1VWPB.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\6Rn5G1VWPB.exe
Imagebase:	0x7d0000
File size:	1162752 bytes

MD5 hash:	C12FEA2DA39E5173FA674AB5E22A928F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.912960268.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.912960268.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.915088523.0000000002CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.915088523.0000000002CF1000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Roaming\ikffln5u.f20	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ikffln5u.f20\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ikffln5u.f20\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ikffln5u.f20\Chrome\Default\Cookies	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	6C1DDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ikffln5u.f20\Chrome\Default\Cookies	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ikffln5u.f20\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 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 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 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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C1DDD66	CopyFileW

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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\1aac658a-5083-459b-8a3c-c1d0bbd9a968	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\ikffln5u.f20\Chrome\Default\Cookies	unknown	16384	success or wait	1	6C1D1B4F	ReadFile

Disassembly

Code Analysis

Copyright Joe Security LLC 2021

Code Analysis