ID: 404243
Sample Name:
20210504_20210405.exe
Cookbook: default.jbs
Time: 20:39:29
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

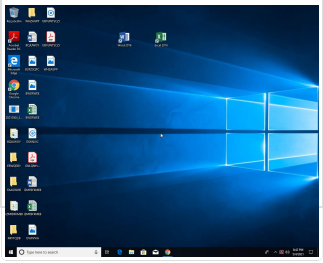
Analysis Report 20210504_20210405.exe

Overview

General Information

Sample Name:	20210504_20210405.exe
Analysis ID:	404243
MD5:	f40f9b893ced71c..
SHA1:	0d109db09fc59e2.
SHA256:	97eba4e44b5a77..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

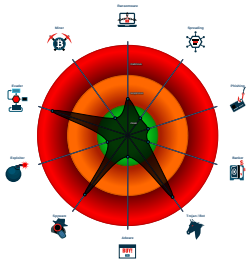
AgentTesla Telegram RAT

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Yara detected Telegram RAT
- .NET source code contains very larg…
- .NET source code references suspic…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- 20210504_20210405.exe (PID: 7000 cmdline: 'C:\Users\user\Desktop\20210504_20210405.exe' MD5: F40F9B893CED71CB1CA32422CCD18D75)
  - 20210504_20210405.exe (PID: 7076 cmdline: C:\Users\user\Desktop\20210504_20210405.exe MD5: F40F9B893CED71CB1CA32422CCD18D75)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1354205151",
  "Chat URL": "https://api.telegram.org/bot1437981864:AAFmXsejy8kUC_pj3BwrEvAeb2cv12XMVZI/sendDocument"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.912316096.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.657827131.0000000003BE9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.913920147.000000000323000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.913920147.000000000323000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.656827071.0000000002C35000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 5 entries

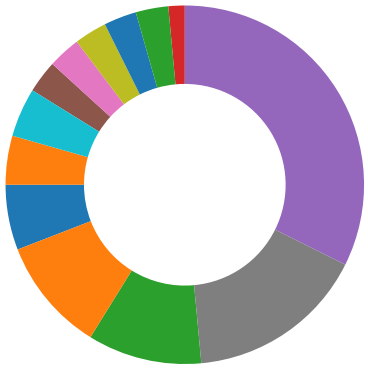
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.20210504_20210405.exe.3dd7748.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.20210504_20210405.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.20210504_20210405.exe.3c88898.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.20210504_20210405.exe.3dd7748.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- 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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Uses the Telegram API (likely for C&C communication)

System Summary:

.NET source code contains very large array initializations

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:

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected Telegram RAT

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:

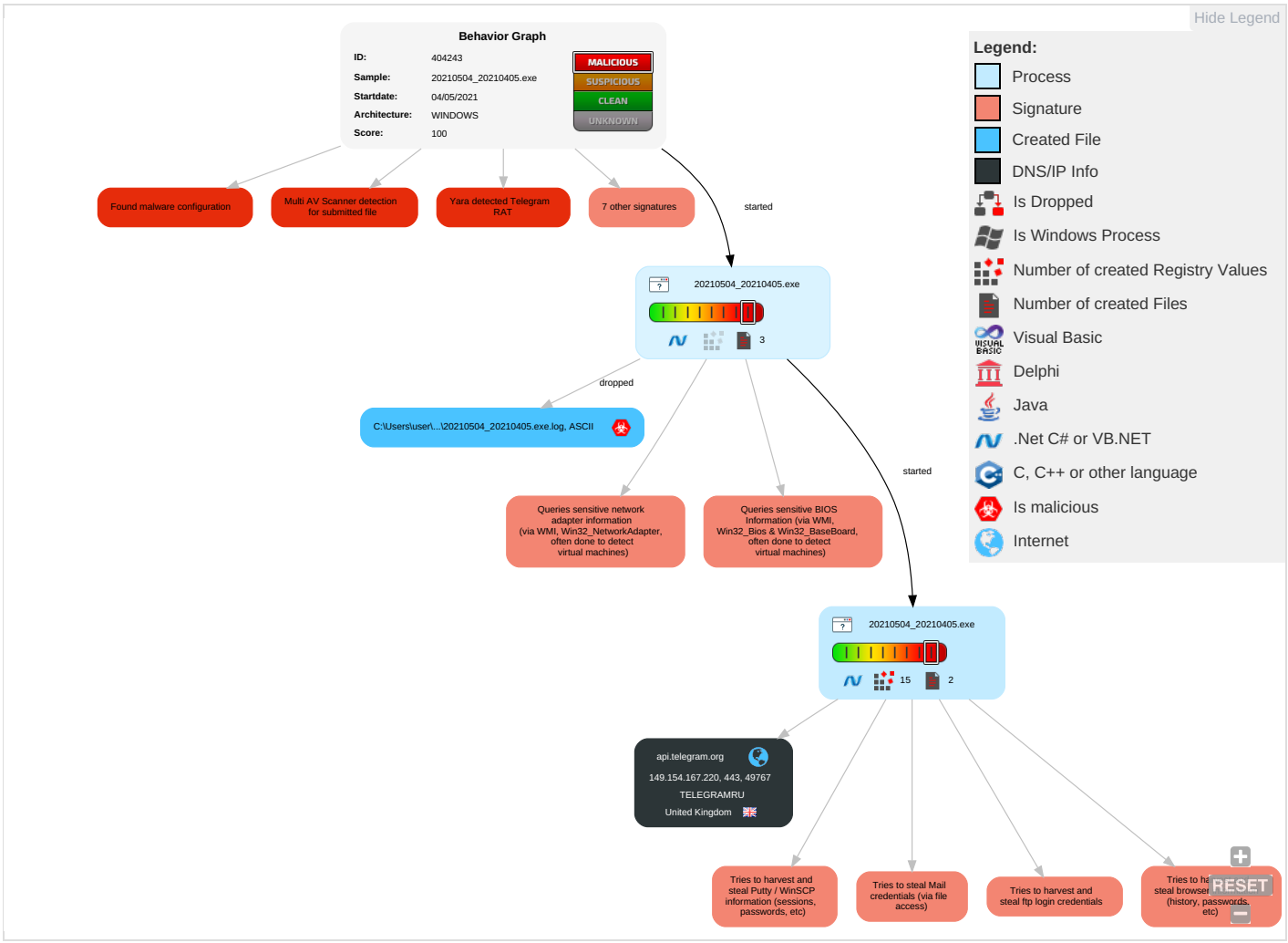
Yara detected AgentTesla

Yara detected Telegram RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Input Capture 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Credentials in Registry 1	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer 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
20210504_20210405.exe	14%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
20210504_20210405.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.20210504_20210405.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	

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://DynDns.comDynDNS	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://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://api.telegram.org41k	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://LKsSWf.com	0%	Avira URL Cloud	safe	
http://https://ZjkYYZZsvgTe1lRecEb.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

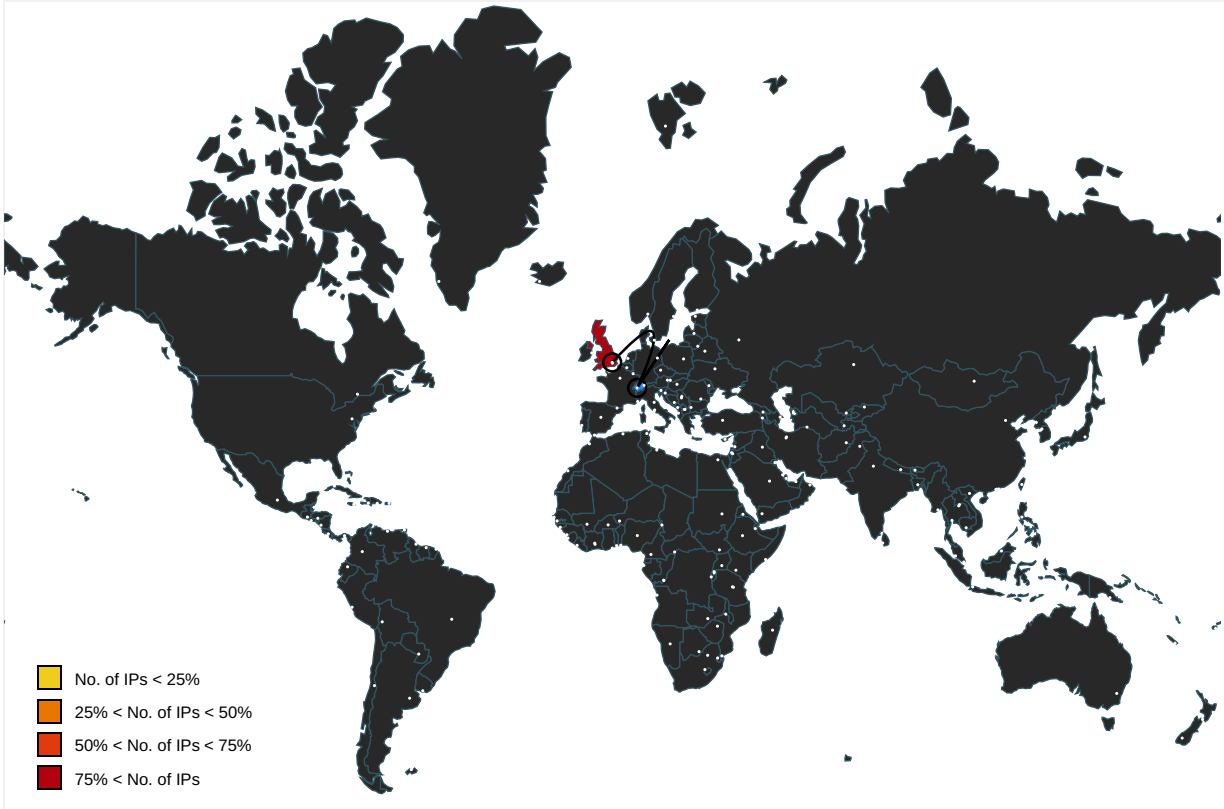
Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.godaddy.com/gdroot-g2.crl0F	20210504_20210405.exe, 00000001.00000002.914611347.00000000035A7000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	20210504_20210405.exe, 00000001.00000002.913920147.0000000003231000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	20210504_20210405.exe, 00000001.00000002.913920147.0000000003231000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://vbcity.com/forums/t/51894.aspx	20210504_20210405.exe	false		high
http://https://api.telegram.org	20210504_20210405.exe, 00000001.00000002.914571014.0000000003592000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	20210504_20210405.exe, 00000001.00000002.913920147.0000000003231000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.godaddy.com/repository/0	20210504_20210405.exe, 00000001.00000002.913117138.0000000001583000.00000004.00000020.sdmp	false		high
http://certs.godaddy.com/repository/1301	20210504_20210405.exe, 00000001.00000002.913117138.0000000001583000.00000004.00000020.sdmp	false		high
http://crl.godaddy.com/gdroot.crl0F	20210504_20210405.exe, 00000001.00000002.914611347.00000000035A7000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot1437981864:AAFmXsejy8kUC_pj3BwrEvAeb2cv12XMVZI/sendDocument	20210504_20210405.exe, 00000001.00000002.913247711.0000000001614000.00000004.00000020.sdmp, 20210504_20210405.exe, 00000001.00000002.914571014.0000000003592000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot1437981864:AAFmXsejy8kUC_pj3BwrEvAeb2cv12XMVZI/	20210504_20210405.exe, 00000000.00000002.657827131.0000000003BE9000.00000004.00000001.sdmp, 20210504_20210405.exe, 00000001.00000002.912316096.0000000000402000.00000040.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.godaddy.com/gdig2s1-1823.crl0	20210504_20210405.exe, 00000001.00000002.913117138.000000001583000.00000004.00000020.sdmp	false		high
http://https://certs.godaddy.com/repository/0	20210504_20210405.exe, 00000001.00000002.914611347.00000000035A7000.00000004.00000001.sdmp	false		high
http://api.telegram.org	20210504_20210405.exe, 00000001.00000002.914611347.00000000035A7000.00000004.00000001.sdmp	false		high
http://certificates.godaddy.com/repository/gdig2.crt0	20210504_20210405.exe, 00000001.00000002.913117138.000000001583000.00000004.00000020.sdmp	false		high
http://https://api.telegram.org41k	20210504_20210405.exe, 00000001.00000002.914571014.000000003592000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	20210504_20210405.exe, 00000000.00000002.656756518.0000000002BE1000.00000004.00000001.sdmp, 20210504_20210405.exe, 00000001.00000002.914571014.0000000003592000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	20210504_20210405.exe, 00000000.00000002.657827131.0000000003BE9000.00000004.00000001.sdmp, 20210504_20210405.exe, 00000001.00000002.912316096.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://LKsSWf.com	20210504_20210405.exe, 00000001.00000002.913920147.000000003231000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ZjkYYZZsvgTe1lRecEb.org	20210504_20210405.exe, 00000001.00000002.913920147.000000003231000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	20210504_20210405.exe, 00000000.00000002.656827071.0000000002C35000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot1437981864:AAFmXsejy8kUC_pj3BwrEvAeb2cv12XMVZI/sendDocumentdocument-----	20210504_20210405.exe, 00000001.00000002.913920147.000000003231000.00000004.00000001.sdmp	false		high
http://https://github.com/MrCylops	20210504_20210405.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404243
Start date:	04.05.2021
Start time:	20:39:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	20210504_20210405.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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.3%) • Quality average: 54.3% • Quality standard deviation: 33%
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): 20.82.210.154, 131.253.33.200, 13.107.22.200, 104.43.193.48, 104.43.139.144, 104.42.151.234, 2.20.157.220, 40.88.32.150, 20.50.102.62, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.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
20:40:18	API Interceptor	791x Sleep call for process: 20210504_20210405.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.154.167.220	PO5421-allignright.doc	Get hash	malicious	Browse	
	Pending DHL Shipment Notification REF 04521.xlsx	Get hash	malicious	Browse	
	04052021paymentscancopy.doc	Get hash	malicious	Browse	
	85a3f6aa_by_Libranalysis.rtf	Get hash	malicious	Browse	
	BID6200306761.exe	Get hash	malicious	Browse	
	OverdueInvoice-PDF.exe	Get hash	malicious	Browse	
	SLIP.exe	Get hash	malicious	Browse	
	NeworderMay20212021-pdf.exe	Get hash	malicious	Browse	
	1hbYGZf6BQ.exe	Get hash	malicious	Browse	
	from-iso_RFQ___PU.EXE1__.exe	Get hash	malicious	Browse	
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	menXxRXr64.exe	Get hash	malicious	Browse	
	pN0fSLX8vx.exe	Get hash	malicious	Browse	
	Order Of Items Listed.xlsx	Get hash	malicious	Browse	
	l6qQa2fQ97.exe	Get hash	malicious	Browse	
	PO 300174.xlsx	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	WdWqhSMRsdKJxkl.exe	Get hash	malicious	Browse	
	Quotation 90809.exe	Get hash	malicious	Browse	
	nrEs3n7XCQ.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.telegram.org	PO5421-allignright.doc	Get hash	malicious	Browse	• 149.154.167.220
	Pending DHL Shipment Notification REF 04521.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	04052021paymentscancopy.doc	Get hash	malicious	Browse	• 149.154.167.220
	85a3f6aa_by_Libranalysis.rtf	Get hash	malicious	Browse	• 149.154.167.220
	BID6200306761.exe	Get hash	malicious	Browse	• 149.154.167.220
	OverdueInvoice-PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	SLIP.exe	Get hash	malicious	Browse	• 149.154.167.220
	NeworderMay20212021-pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	1hbYGZf6BQ.exe	Get hash	malicious	Browse	• 149.154.167.220
	from-iso_RFQ___PU.EXE1__.exe	Get hash	malicious	Browse	• 149.154.167.220
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	• 149.154.167.220
	menXxRXr64.exe	Get hash	malicious	Browse	• 149.154.167.220
	pN0fSLX8vx.exe	Get hash	malicious	Browse	• 149.154.167.220
	Order Of Items Listed.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	l6qQa2fQ97.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 300174.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Quotation.exe	Get hash	malicious	Browse	• 149.154.167.220
	WdWqhSMRsdKJxkl.exe	Get hash	malicious	Browse	• 149.154.167.220
	Quotation 90809.exe	Get hash	malicious	Browse	• 149.154.167.220
	nrEs3n7XCQ.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEGRAMRU	PO5421-allignright.doc	Get hash	malicious	Browse	• 149.154.167.220
	Pending DHL Shipment Notification REF 04521.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	04052021paymentscancopy.doc	Get hash	malicious	Browse	• 149.154.167.220
	85a3f6aa_by_Libranalysis.rtf	Get hash	malicious	Browse	• 149.154.167.220
	TT1eJMw4qZ.exe	Get hash	malicious	Browse	• 95.161.76.100
	BID6200306761.exe	Get hash	malicious	Browse	• 149.154.167.220
	OverdueInvoice-PDF.exe	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SLIP.exe	Get hash	malicious	Browse	• 149.154.167.220
	NeworderMay20212021-pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	1hbYGZf6BQ.exe	Get hash	malicious	Browse	• 149.154.167.220
	from-iso_RFQ___PU.EXE1__.exe	Get hash	malicious	Browse	• 149.154.167.220
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	• 149.154.167.220
	menXxRXr64.exe	Get hash	malicious	Browse	• 149.154.167.220
	pN0fSLX8vx.exe	Get hash	malicious	Browse	• 149.154.167.220
	Order Of Items Listed.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	l6qQa2fQ97.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 300174.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Quotation.exe	Get hash	malicious	Browse	• 149.154.167.220
	WdWqhSMRsdKJxkl.exe	Get hash	malicious	Browse	• 149.154.167.220
	Quotation 90809.exe	Get hash	malicious	Browse	• 149.154.167.220

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	Sample Order.exe	Get hash	malicious	Browse	• 149.154.167.220
	d.exe	Get hash	malicious	Browse	• 149.154.167.220
	d.exe	Get hash	malicious	Browse	• 149.154.167.220
	d.exe	Get hash	malicious	Browse	• 149.154.167.220
	d.exe	Get hash	malicious	Browse	• 149.154.167.220
	2bb0000.exe	Get hash	malicious	Browse	• 149.154.167.220
	2f50000.exe	Get hash	malicious	Browse	• 149.154.167.220
	oiY37pLlj7.exe	Get hash	malicious	Browse	• 149.154.167.220
	3ZtdRsbjxo.exe	Get hash	malicious	Browse	• 149.154.167.220
	Oej1asjUTO.exe	Get hash	malicious	Browse	• 149.154.167.220
	OK0n4zMIIm.exe	Get hash	malicious	Browse	• 149.154.167.220
	BID6200306761.exe	Get hash	malicious	Browse	• 149.154.167.220
	OverdueInvoice-PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	SLIP.exe	Get hash	malicious	Browse	• 149.154.167.220
	NeworderMay20212021-pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	1hbYGZf6BQ.exe	Get hash	malicious	Browse	• 149.154.167.220
	c89928a29ebf0c8c2acd7d9a457236e15d1a604d5c892.exe	Get hash	malicious	Browse	• 149.154.167.220
	from-iso_RFQ___PU.EXE1__.exe	Get hash	malicious	Browse	• 149.154.167.220
	80896e11_by_Libranalysis.exe	Get hash	malicious	Browse	• 149.154.167.220
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	• 149.154.167.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\20210504_20210405.exe.log

Process:	C:\Users\user\Desktop\20210504_20210405.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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.65793626017001
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	20210504_20210405.exe
File size:	915968
MD5:	f40f9b893ced71cb1ca32422ccd18d75
SHA1:	0d109db09fc59e2c15b17f401919be62ff061742
SHA256:	97eba4e44b5a777231316e709cb9eda7bd9670034fdac573724347196acfcf57
SHA512:	1d04a60818df9501ecf5dbf27a0a294959395f3c65eb6e7dab211867a402de3811b143b41697e680ba9493b93bdb0be8069502ca552c429173c0b9345fb5035
SSDEEP:	24576:yKqYxyKgykKnC2wtUQazELj4UlqERz1i/JF4O0h:qe9kD1KQtFRz4/b4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o.....P.....j.... ... .@.. .....` .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4e0e6a
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:	0xF2EE6F15 [Wed Feb 25 14:17:57 2099 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

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
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	0xe0e18	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe2000	0x5cc	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xe0dfc	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	0xdee70	0xdf000	False	0.847543485496	data	7.66441131733	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe2000	0x5cc	0x600	False	0.426432291667	data	4.12925062436	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe4000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe2090	0x33c	data		
RT_MANIFEST	0xe23dc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

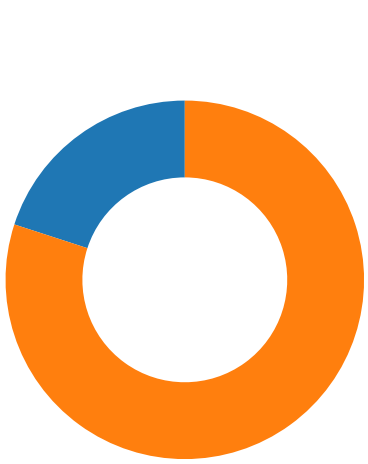
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	StubHelpers.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	StarEggControl
ProductVersion	1.0.0.0
FileDescription	StarEggControl
OriginalFilename	StubHelpers.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:42:04.192122936 CEST	49767	443	192.168.2.4	149.154.167.220
May 4, 2021 20:42:04.242762089 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.242861032 CEST	49767	443	192.168.2.4	149.154.167.220
May 4, 2021 20:42:04.329534054 CEST	49767	443	192.168.2.4	149.154.167.220
May 4, 2021 20:42:04.381201029 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.381259918 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.381315947 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.381349087 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.381376982 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.382545948 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.382587910 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.383671999 CEST	49767	443	192.168.2.4	149.154.167.220
May 4, 2021 20:42:04.383724928 CEST	49767	443	192.168.2.4	149.154.167.220
May 4, 2021 20:42:04.395021915 CEST	49767	443	192.168.2.4	149.154.167.220
May 4, 2021 20:42:04.446156025 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.495764971 CEST	49767	443	192.168.2.4	149.154.167.220
May 4, 2021 20:42:04.734357119 CEST	49767	443	192.168.2.4	149.154.167.220
May 4, 2021 20:42:04.785861015 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.788855076 CEST	49767	443	192.168.2.4	149.154.167.220
May 4, 2021 20:42:04.880815029 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.907237053 CEST	443	49767	149.154.167.220	192.168.2.4
May 4, 2021 20:42:04.948878050 CEST	49767	443	192.168.2.4	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:40:09.771846056 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:09.825483084 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 20:40:09.927006960 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:09.999141932 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 20:40:10.146344900 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:10.195960045 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 20:40:11.089144945 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:11.138391018 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 20:40:11.990179062 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:12.051601887 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 20:40:12.441615105 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:12.510978937 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 20:40:13.720036983 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:13.768572092 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 20:40:14.748639107 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:14.801845074 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 20:40:15.975275040 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:16.026875019 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 20:40:17.210853100 CEST	64549	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:40:17.262057066 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 20:40:18.297317982 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:18.346009970 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 20:40:19.221184969 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:19.272701025 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 20:40:20.427603006 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:20.479773998 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 20:40:21.606590033 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:21.658119917 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 20:40:22.734302998 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:22.791281939 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 20:40:24.029783964 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:24.078418970 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 20:40:26.073687077 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:26.125221968 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 20:40:26.980449915 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:27.029561043 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 20:40:28.074004889 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:28.123935938 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 20:40:29.028944969 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:29.079714060 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 20:40:30.155356884 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:30.216062069 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 20:40:31.149739027 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:31.206571102 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 20:40:44.069988012 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:44.125586033 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 20:40:48.048274994 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 20:40:48.112409115 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 20:41:04.183442116 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:04.249094009 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 20:41:04.518188000 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:04.647422075 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 20:41:05.233036995 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:05.290298939 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 20:41:05.852013111 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:05.912156105 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 20:41:06.350812912 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:06.454221964 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:06.470460892 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 20:41:06.530004025 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 20:41:07.031008005 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:07.146509886 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 20:41:07.688594103 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:07.843024969 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 20:41:08.461589098 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:08.518961906 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 20:41:09.718070030 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:09.775479078 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 20:41:11.311207056 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:11.372390032 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 20:41:11.860690117 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:11.918756962 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 20:41:21.453840017 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:21.518172979 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 20:41:52.597062111 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:52.647588015 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 20:41:54.362317085 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 20:41:54.420639038 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 20:42:04.037260056 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 20:42:04.087466955 CEST	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:42:04.037260056 CEST	192.168.2.4	8.8.8.8	0x4f9f	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:42:04.087466955 CEST	8.8.8.8	192.168.2.4	0x4f9f	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 20:42:04.382545948 CEST	149.154.167.220	443	192.168.2.4	49767	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior

● 20210504_20210405.exe
● 20210504_20210405.exe

Click to jump to process

System Behavior

Analysis Process: 20210504_20210405.exe PID: 7000 Parent PID: 5900

General

Start time:	20:40:16
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\20210504_20210405.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\20210504_20210405.exe'
Imagebase:	0x850000
File size:	915968 bytes
MD5 hash:	F40F9B893CED71CB1CA32422CCD18D75
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: 00000000.00000002.657827131.0000000003BE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.656827071.0000000002C35000.00000004.00000001.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	6D17CF06	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	6D17CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\20210504_20210405.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\20210504_20210405.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	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: 20210504_20210405.exe PID: 7076 Parent PID: 7000

General

Start time:	20:40:20
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\20210504_20210405.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\20210504_20210405.exe
Imagebase:	0xdd0000
File size:	915968 bytes
MD5 hash:	F40F9B893CED71CB1CA32422CCD18D75
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: 00000001.00000002.912316096.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.913920147.0000000003231000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.913920147.0000000003231000.00000004.00000001.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	6D17CF06	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	6D17CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\738fae7c-24da-4f44-b2de-8e1b738b27d2	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6BFC1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis