ID: 339373
Sample Name: Request For Quotation_pdf.scr
Cookbook: default.jbs
Time: 21:51:41
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

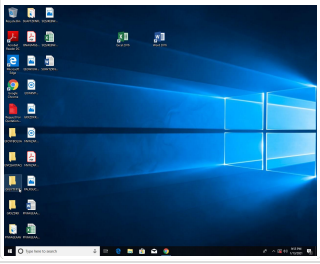
Analysis Report Request For Quotation_pdf.scr

Overview

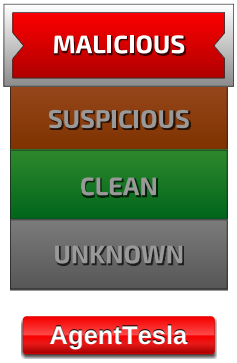
General Information

Sample Name:	Request For Quotation_pdf.scr (renamed file extension from scr to exe)
Analysis ID:	339373
MD5:	a9125d57b0d416..
SHA1:	56bcb534abe3e5..
SHA256:	4f84f23b927e4a2..
Tags:	AgentTesla scr

Most interesting Screenshot:



Detection

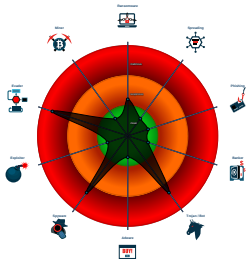


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…
- 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**
- Request For Quotation_pdf.exe (PID: 6644 cmdline: 'C:\Users\user\Desktop\Request For Quotation_pdf.exe' MD5: A9125D57B0D4162E7DA34D6B8C10836F)
  - schtasks.exe (PID: 6852 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\FLahHLuGzK' /XML 'C:\Users\user\AppData\Local\Temp\tmp91A5.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "kBDUWu4tdzmw4m",
  "URL: ": "https://70m3WJPOC5dv7ww.org",
  "To: ": "diamondraylog@yandex.ru",
  "ByHost: ": "smtp.yandex.ru:587",
  "Password: ": "RQslMXh",
  "From: ": "diamondraylog@yandex.ru"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.608313718.0000000003D76000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.604230367.0000000002A21000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.604230367.0000000002A2 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000000.00000002.610458939.00000000064C 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: Request For Quotation_pdf.exe PID: 6644	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

Unpacked PEs

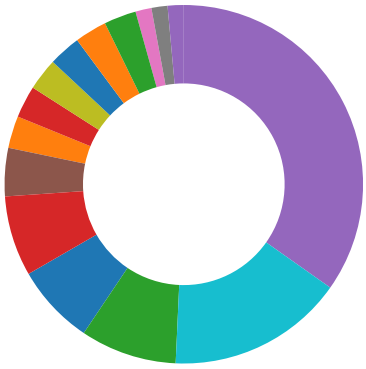
Source	Rule	Description	Author	Strings
0.2.Request For Quotation_pdf.exe.64c0000.7.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Request For Quotation_pdf.exe.64c0000.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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)

Stealing of Sensitive Information:

Yara detected AgentTesla

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)

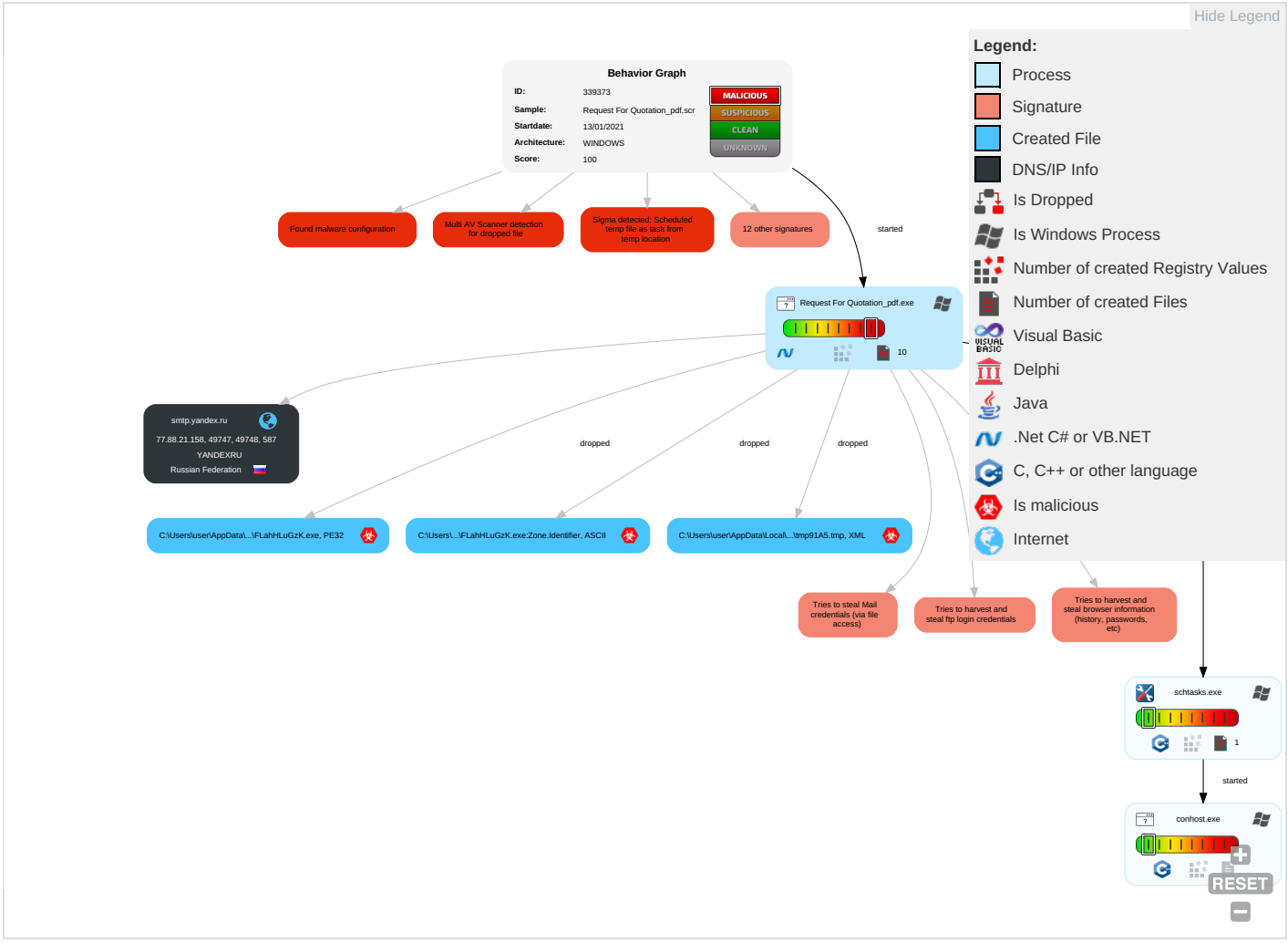
Remote Access Functionality:

Yara detected AgentTesla

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	Scheduled Task/Job 1	Process Injection 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Obfuscated Files or Information 2	Input Capture 1	System Information Discovery 1 1 3	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Laye Protocol 1 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 4	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 2	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Laye 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
Request For Quotation_pdf.exe	26%	ReversingLabs	Win32.Trojan.Pwsx	
Request For Quotation_pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\FLahHLuGzK.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\FLahHLuGzK.exe	26%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://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://70m3WJPOC5dv7ww.org	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://mPTCSt.com	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://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high

Contacted URLs

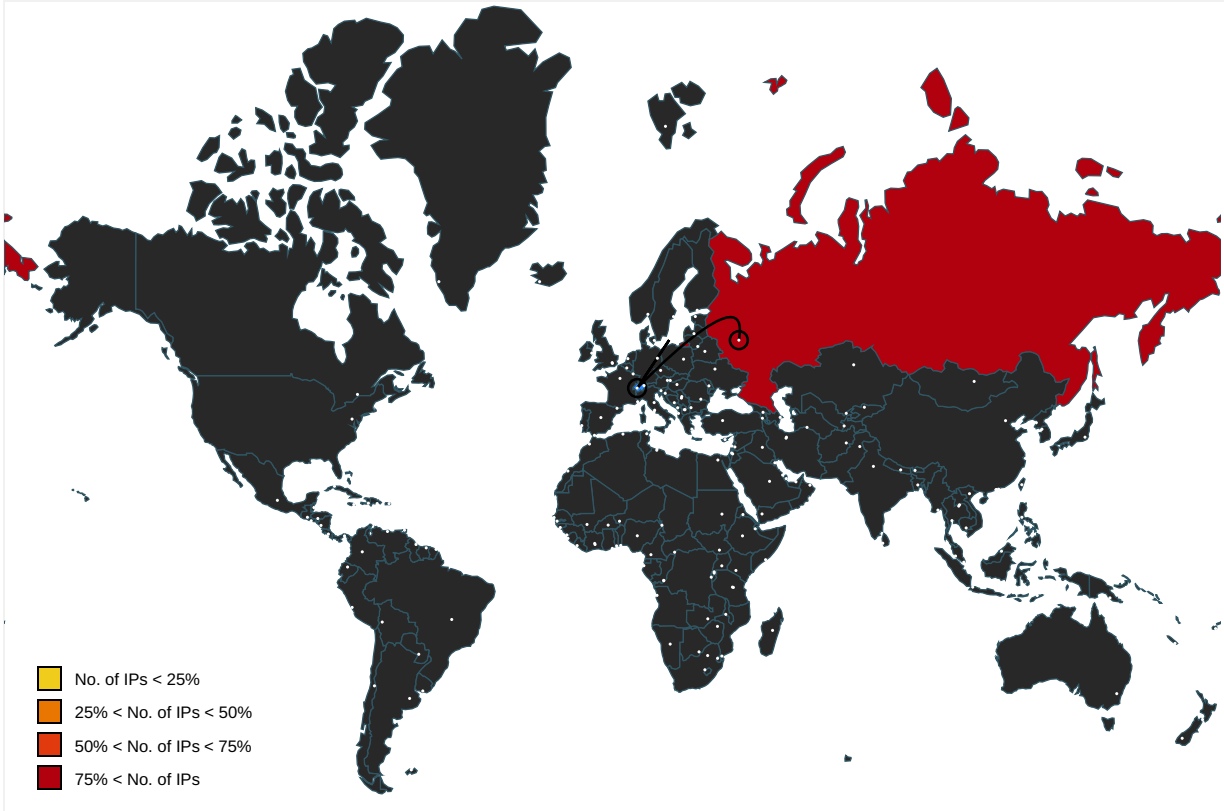
Name	Malicious	Antivirus Detection	Reputation
http://https://70m3WJPOC5dv7ww.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://subca.ocsp-certum.com0.	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ca.cer09	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	Request For Quotation_pdf.exe, 00000000.00000002.604230367.000000002A21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	Request For Quotation_pdf.exe, 00000000.00000002.604230367.000000002A21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ctnca.cer09	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false		high
http://crls.yandex.net/certum/ycasha2.crl0-	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Request For Quotation_pdf.exe, 00000000.00000002.604230367.000000002A21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.certum.pl/ctnca.crl0k	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false		high
http://subca.ocsp-certum.com01	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://yandex.crl.certum.pl/ycasha2.crl0q	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false		high
http://crl.certum.pl/ca.crl0h	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false		high
http://https://www.certum.pl/CPS0	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false		high
http://mPTCSt.com	Request For Quotation_pdf.exe, 00000000.00000002.604230367.000000002A21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Request For Quotation_pdf.exe, 00000000.00000002.604230367.000000002A21000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Request For Quotation_pdf.exe, 00000000.00000002.608313718.000000003D76000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certum.pl/CPS0	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false		high
http://yandex.ocsp-responder.com03	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ycasha2.cer0	Request For Quotation_pdf.exe, 00000000.00000002.606262254.000000002D18000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	unknown	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339373
Start date:	13.01.2021
Start time:	21:51:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Request For Quotation_pdf.scr (renamed file extension from scr 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:	31
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@4/4@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 52.255.188.83, 13.64.90.137, 168.61.161.212, 23.210.248.85, 51.104.139.180, 92.122.213.247, 92.122.213.194, 8.248.149.254, 8.253.95.249, 8.253.204.121, 67.26.75.254, 67.26.137.254, 20.54.26.129, 84.53.167.113, 51.103.5.186, 51.132.208.181, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, wildcard.weather.microsoft.com.edgekey.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/339373/sample/Request For Quotation_pdf.exe

Simulations

Behavior and APIs

Time	Type	Description
21:52:41	API Interceptor	1084x Sleep call for process: Request For Quotation_pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.88.21.158	SWIFT HKEB0C01725410-T02.zip.exe	Get hash	malicious	Browse	
	RFQ#675568PL_pdf.exe	Get hash	malicious	Browse	
	Quote ROE-127488-MU.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase order.exe	Get hash	malicious	Browse	
	Request For Quotation GH67511_pdf.exe	Get hash	malicious	Browse	
	swiftcopy001#pdf.exe	Get hash	malicious	Browse	
	Payment Receipt.exe	Get hash	malicious	Browse	
	TT Copy_pdf.exe	Get hash	malicious	Browse	
	PO-98766.exe	Get hash	malicious	Browse	
	Original_Copies.exe	Get hash	malicious	Browse	
	Purchase order001#pdf.exe	Get hash	malicious	Browse	
	Product Catalogue List. docs.exe	Get hash	malicious	Browse	
	Payment Receipt.exe	Get hash	malicious	Browse	
	Product Catalogue.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.35832395.5304.exe	Get hash	malicious	Browse	
	iuu4DJ67MC.exe	Get hash	malicious	Browse	
	Order 539.exe	Get hash	malicious	Browse	
	3yoE6lNVNy.exe	Get hash	malicious	Browse	
	SWIFT COPY AMOUNT OF US 49.676,30 FOR SMX022-10-20 DATED 23122020.xlsx	Get hash	malicious	Browse	
	yuag0m1Xh7.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.yandex.ru	SWIFT HKEB0C01725410-T02.zip.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#675568PL_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	Quote ROE-127488-MU.exe	Get hash	malicious	Browse	• 77.88.21.158
	Purchase order.exe	Get hash	malicious	Browse	• 77.88.21.158
	Request For Quotation GH67511_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	swiftcopy001#pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment Receipt.exe	Get hash	malicious	Browse	• 77.88.21.158
	TT Copy_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO-98766.exe	Get hash	malicious	Browse	• 77.88.21.158
	Original_Copies.exe	Get hash	malicious	Browse	• 77.88.21.158
	Purchase order001#pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	Product Catalogue List. docs.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment Receipt.exe	Get hash	malicious	Browse	• 77.88.21.158
	Product Catalogue.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.GenericKD.35832395.5304.exe	Get hash	malicious	Browse	• 77.88.21.158
	iuu4DJ67MC.exe	Get hash	malicious	Browse	• 77.88.21.158
	Order 539.exe	Get hash	malicious	Browse	• 77.88.21.158
	3yoE6lNVNy.exe	Get hash	malicious	Browse	• 77.88.21.158
	SWIFT COPY AMOUNT OF US 49.676,30 FOR SMX022-10-20 DATED 23122020.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	yuag0m1Xh7.exe	Get hash	malicious	Browse	• 77.88.21.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YANDEXRU	SWIFT HKEB0C01725410-T02.zip.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#675568PL_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	Quote ROE-127488-MU.exe	Get hash	malicious	Browse	• 77.88.21.158
	Purchase order.exe	Get hash	malicious	Browse	• 77.88.21.158
	Request For Quotation GH67511_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	swiftcopy001#pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment Receipt.exe	Get hash	malicious	Browse	• 77.88.21.158
	TT Copy_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO-98766.exe	Get hash	malicious	Browse	• 77.88.21.158
	Original_Copies.exe	Get hash	malicious	Browse	• 77.88.21.158
	http://ovd.ru/forum/register.php?a=act&u=84666&i=25545989	Get hash	malicious	Browse	• 87.250.250.36
	http://mainfreight-6452496282.eritro.ir/retailer.php?ikpah=Z2lvdmFuYS50YWJhcmluaUBtYWluZnJlaWdodC5jb20=	Get hash	malicious	Browse	• 87.250.250.119
	Purchase order001#pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	Product Catalogue List. docs.exe	Get hash	malicious	Browse	• 77.88.21.158
	http://iaaoaot.angelx97.xyz/OCFAheVlOOWYzT2RoWDEvaFE	Get hash	malicious	Browse	• 87.250.251.119

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	lZVNh1BPxm.exe	Get hash	malicious	Browse	• 87.250.250.22
	qG5E4q8Cv5.exe	Get hash	malicious	Browse	• 87.250.250.22
	http://browsermine.com	Get hash	malicious	Browse	• 77.88.21.119
	Payment Receipt.exe	Get hash	malicious	Browse	• 77.88.21.158
	Product Catalogue.exe	Get hash	malicious	Browse	• 77.88.21.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\tmp91A5.tmp

Process:	C:\Users\user\Desktop\Request For Quotation_pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.193980191585194
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBntn:cbh47TlNQ//rydbz9l3YODOLNdq3n
MD5:	C27284C9952E79A82CEE03B348A03192
SHA1:	96E60BEA3998F19646082C48AB3FB0AAAAB4AEB6
SHA-256:	621CC8F055B4E0294DB250611782A694C2EA00AED46F3BD23CABE04A8231EB12
SHA-512:	13F16F1AEF62D2ECFD3C15EEB167875351FC30CA35C503839998444E37CDBE767FFD2A2C5814EAF06F52F7C4E48377517E2BB4DAFEE11C389B81040EF283ED5 1
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\FLahHLuGzK.exe

Process:	C:\Users\user\Desktop\Request For Quotation_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1206272
Entropy (8bit):	6.475210120171716
Encrypted:	false
SSDEEP:	12288:Tk3i7spOXX0muTKVzRaLrXOa/lcCgTZX8naDUf+h6a9Env:p+OeSaH+atcCKZIzP
MD5:	A9125D57B0D4162E7DA34D6B8C10836F
SHA1:	56BCB534ABE3E5111B07B4F502B647FB5584B905
SHA-256:	4F84F23B927E4A2F6F64D0C824777C1E0EDB05F8F83A662EF59617793582CFB6
SHA-512:	430731A8792D27FAC18BE517BB200A514CC8B7D72E90D0BDFCD630BA85600C46633F13B3499EEA0993573122C07DD5015FC2318B7E13DBED9495222822D6930I
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P..... .....@.. ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....f.....@..B.....H.....<X.....$.....(....*&..(.....*.s .....s!.....s".....s#.....s$.....*...0.....~....o%....+..*.0.....~....o &....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0.....~....o)....+..*&..(*....*...0..<.....~.....(+.....!r...p.....(....o-...s.....~.....+..*.0.....~.....+..*".....*.0.....(....r=. .p~....o/....+..*...0..<.....~.....(+.....!rG..p.....(,

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

Process:	C:\Users\user\Desktop\Request For Quotation_pdf.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Roaming\FLahHLuGzK.exe:Zone.Identifier	
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\qxsok1rs.4ec\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Request For Quotation_pdf.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
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):	6.475210120171716
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:	Request For Quotation_pdf.exe
File size:	1206272
MD5:	a9125d57b0d4162e7da34d6b8c10836f
SHA1:	56bcb534abe3e5111b07b4f502b647fb5584b905
SHA256:	4f84f23b927e4a2f6f64d0c824777c1e0edb05f8f83a662ef59617793582cfb6
SHA512:	430731a8792d27fac18be517bb200a514cc8b7d72e90d0bdfcd630ba85600c46633f13b3499eea0993573122c07dc5015fc2318b7e13dbed9495222822d6930d
SSDEEP:	12288:Tk3i7spOXX0muTKVzRaLrXOa/lcCgTZX8naDUf+h6a9Env:p+OeSaH+atcCKZlzP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ._.....P..... .....@.. .....@.....

File Icon

	
Icon Hash:	3cfcc4dcfcdcf4c4

Static PE Info

General

Entrypoint:	0x4cd5f6
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:	0x5FFEC78E [Wed Jan 13 10:12:30 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

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
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	0xcd5a4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0x5ad04	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x12a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcb5fc	0xcb600	False	0.694828720421	data	7.29828241423	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x5ad04	0x5ae00	False	0.031467610901	data	2.76557267543	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x12a000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xce220	0x42028	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x110248	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1106b0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x112c58	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x113d00	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x124528	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x128750	0x5a	data		
RT_VERSION	0x1287ac	0x36c	data		
RT_MANIFEST	0x128b18	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

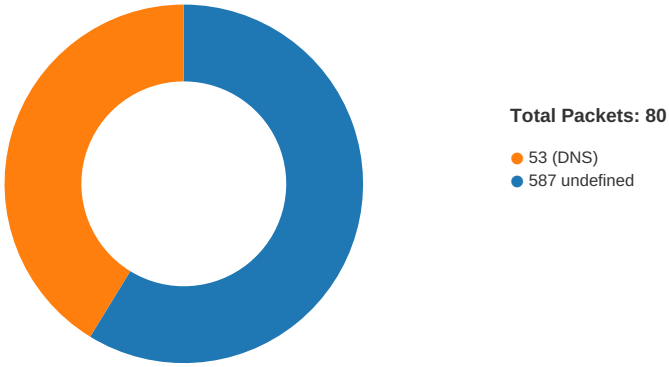
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2011
Assembly Version	1.0.0.0
InternalName	CompletionActionInvoker.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	FileReplacement
ProductVersion	1.0.0.0
FileDescription	FileReplacement

Description	Data
OriginalFilename	CompletionActionInvoker.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:54:16.140419960 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:16.234174013 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:16.234333992 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:16.429976940 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:16.430802107 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:16.524565935 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:16.524590015 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:16.525309086 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:16.618880033 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:16.666510105 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:16.681868076 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:16.776935101 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:16.776972055 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:16.776998043 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:16.777019024 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:16.777072906 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:16.777156115 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:16.825010061 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:16.918986082 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:16.963412046 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:16.980113029 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:17.074919939 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:17.077862978 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:17.171621084 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:17.173211098 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:17.283544064 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:17.285033941 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:17.386183977 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:17.386729002 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:17.488045931 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:17.489068985 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:17.582864046 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:17.586572886 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:17.587012053 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:17.587766886 CET	49747	587	192.168.2.3	77.88.21.158

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:54:17.588051081 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:17.680660963 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:17.681606054 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:18.115304947 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:18.166568041 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:18.556735039 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:18.650461912 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:18.650487900 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:18.650566101 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:18.663522005 CET	49747	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:18.664649963 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:18.757010937 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:18.757086992 CET	587	49747	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:18.757102966 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:18.922470093 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:18.922744036 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.015113115 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.015132904 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.015640020 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.108129978 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.108654976 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.202399015 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.202441931 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.202467918 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.202488899 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.202560902 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.202694893 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.206944942 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.299706936 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.303919077 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.397281885 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.397789955 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.491343975 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.492532015 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.603725910 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.604460955 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.704807997 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.705328941 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.805012941 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.809865952 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.903364897 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.904927969 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.905071974 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.905189991 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.905313969 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.905492067 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.905590057 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.905677080 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.905762911 CET	49748	587	192.168.2.3	77.88.21.158
Jan 13, 2021 21:54:19.998595953 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:19.999022961 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:20.039907932 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:20.391532898 CET	587	49748	77.88.21.158	192.168.2.3
Jan 13, 2021 21:54:20.432727098 CET	49748	587	192.168.2.3	77.88.21.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:52:30.341128111 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:30.391957998 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 21:52:31.117417097 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:31.165441036 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 21:52:31.888267994 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:31.947860003 CET	53	50141	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:52:33.057636976 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:33.121685028 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 21:52:33.902951002 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:33.950781107 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 21:52:34.803869009 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:34.851890087 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 21:52:35.712589025 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:35.760587931 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 21:52:36.822915077 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:36.870805025 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 21:52:37.964888096 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:38.012837887 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 21:52:39.130528927 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:39.178371906 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 21:52:40.316240072 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:40.367026091 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 21:52:58.632570028 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:52:58.690195084 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 21:53:00.592031002 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:53:00.639974117 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 21:53:05.732527971 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:53:05.790543079 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 21:53:19.036228895 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:53:19.094764948 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 21:53:20.094482899 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:53:20.161669970 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 21:53:20.266303062 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:53:20.278212070 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:53:20.326759100 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 21:53:20.344448090 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 21:53:23.654299974 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:53:23.710993052 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 21:54:03.916651964 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:54:03.964550018 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 21:54:04.368026972 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:54:04.432178974 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 21:54:16.062416077 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:54:16.118700027 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 21:54:24.146873951 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:54:24.194705963 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 21:55:17.542475939 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:55:17.601933002 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 21:55:18.298346043 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:55:18.354852915 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 21:55:19.150937080 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:55:19.201879025 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 21:55:20.081162930 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:55:20.145354033 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 21:55:23.096648932 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:55:23.156980991 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 21:55:26.835577965 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:55:26.891942024 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 21:55:27.761446953 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:55:27.817890882 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 21:55:28.943160057 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:55:28.999450922 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 21:55:30.158791065 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:55:30.209395885 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 21:55:30.678241968 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:55:30.734525919 CET	53	55708	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:54:16.062416077 CET	192.168.2.3	8.8.8.8	0xc0c8	Standard query (0)	smtp.yandex.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:54:16.118700027 CET	8.8.8.8	192.168.2.3	0xc0c8	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

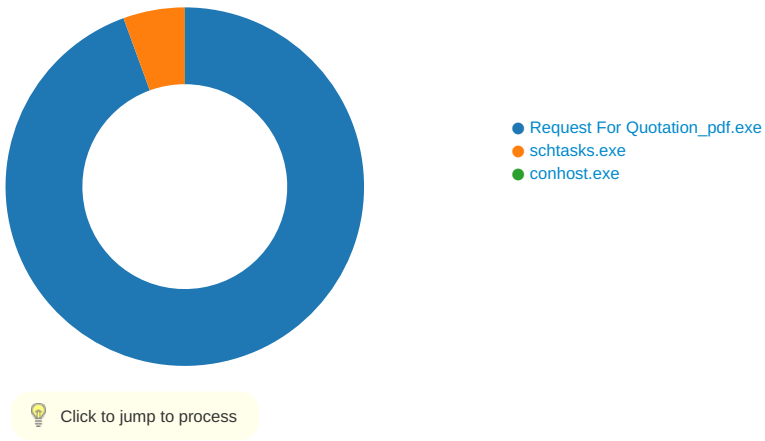
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 21:54:16.429976940 CET	587	49747	77.88.21.158	192.168.2.3	220 vla1-0125c0e65a03.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Jan 13, 2021 21:54:16.430802107 CET	49747	587	192.168.2.3	77.88.21.158	EHLO 571345
Jan 13, 2021 21:54:16.524590015 CET	587	49747	77.88.21.158	192.168.2.3	250-vla1-0125c0e65a03.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Jan 13, 2021 21:54:16.525309086 CET	49747	587	192.168.2.3	77.88.21.158	STARTTLS
Jan 13, 2021 21:54:16.618880033 CET	587	49747	77.88.21.158	192.168.2.3	220 Go ahead
Jan 13, 2021 21:54:18.922470093 CET	587	49748	77.88.21.158	192.168.2.3	220 vla3-3dd1bd6927b2.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Jan 13, 2021 21:54:18.922744036 CET	49748	587	192.168.2.3	77.88.21.158	EHLO 571345
Jan 13, 2021 21:54:19.015132904 CET	587	49748	77.88.21.158	192.168.2.3	250-vla3-3dd1bd6927b2.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Jan 13, 2021 21:54:19.015640020 CET	49748	587	192.168.2.3	77.88.21.158	STARTTLS
Jan 13, 2021 21:54:19.108129978 CET	587	49748	77.88.21.158	192.168.2.3	220 Go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Request For Quotation_pdf.exe PID: 6644 Parent PID: 5624

General

Start time:	21:52:35
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Request For Quotation_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Request For Quotation_pdf.exe'
Imagebase:	0x540000
File size:	1206272 bytes
MD5 hash:	A9125D57B0D4162E7DA34D6B8C10836F
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: 00000000.00000002.608313718.0000000003D76000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.604230367.0000000002A21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.604230367.0000000002A21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.610458939.00000000064C0000.00000004.00000001.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	6E07CF06	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	6E07CF06	unknown
C:\Users\user\AppData\Roaming\FLahHLuGzK.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CECDD66	CopyFileW
C:\Users\user\AppData\Roaming\FLahHLuGzK.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CECDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp91A5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEC7038	GetTempFileNameW
C:\Users\user\AppData\Roaming\qxsok1rs.4ec	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CECBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\qxsok1rs.4ec\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	6CECBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\qxsok1rs.4ec\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	6CECBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\qxsok1rs.4ec\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6CECDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp91A5.tmp	success or wait	1	6CEC6A95	DeleteFileW
C:\Users\user\AppData\Roaming\qxsok1rs.4ec\Chrome\Default\Cookies	success or wait	1	6CEC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\FLahHLuGzK.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 8e c7 fe 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 b6 0c 00 00 b0 05 00 00 00 00 00 f6 d5 0c 00 00 20 00 00 00 e0 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 12 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....P................. ....@.. ....@................	success or wait	5	6CECDD66	CopyFileW
C:\Users\user\AppData\Roaming\FLahHLuGzK.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CECDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp91A5.tmp	unknown	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CEC1B4F	WriteFile
C:\Users\user\AppData\Roaming\ qxsok1rs.4ec\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 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	6CECDD66	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	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CEC1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\2c84845b-1b18-4199-86a1-559b58eb377f	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CEC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CEC1B4F	ReadFile
C:\Users\user\AppData\Roaming\qxsok1rs.4ec\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CEC1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6852 Parent PID: 6644

General

Start time:	21:52:43
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\FLahHLuGzK' /XML 'C:\Users\user\AppData\Local\Temp\tmp91A5.tmp'
Imagebase:	0x11a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp91A5.tmp	unknown	2	success or wait	1	11AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp91A5.tmp	unknown	1644	success or wait	1	11AABD9	ReadFile

Analysis Process: conhost.exe PID: 6860 Parent PID: 6852

General

Start time:	21:52:43
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis