ID: 385385
Sample Name: RQF 100021790.exe
Cookbook: default.jbs
Time: 12:13:12
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

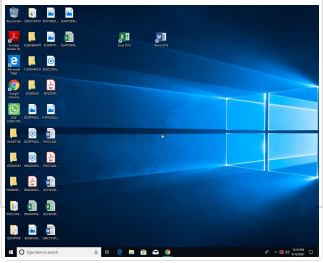
Analysis Report RQF 100021790.exe

Overview

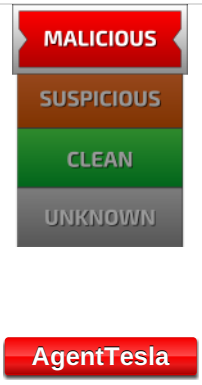
General Information

Sample Name:	RQF 100021790.exe
Analysis ID:	385385
MD5:	31f58bbbd330f88..
SHA1:	1795b60a6f387de.
SHA256:	c289703ef1a3645.
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection



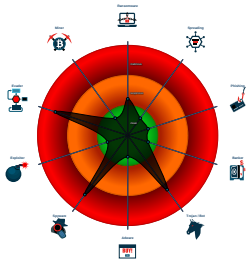
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- 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…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- RQF 100021790.exe (PID: 5380 cmdline: 'C:\Users\user\Desktop\RQF 100021790.exe' MD5: 31F58BBBD330F886E422D44E9C21DBF4)
  - RQF 100021790.exe (PID: 3920 cmdline: {path} MD5: 31F58BBBD330F886E422D44E9C21DBF4)
  - RQF 100021790.exe (PID: 6020 cmdline: {path} MD5: 31F58BBBD330F886E422D44E9C21DBF4)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "ekwe@yillyenterprise.com^1.kk2[?w-Yzmail.yillyenterprise.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.466065951.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.471510302.000000000291000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.207282678.0000000003F89000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RQF 100021790.exe PID: 5380	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RQF 100021790.exe PID: 5380	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 2 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.RQF 100021790.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.RQF 100021790.exe.41acc10.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.RQF 100021790.exe.41acc10.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Networking
- 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:

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

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)

Stealing of Sensitive Information:

- **Yara detected AgentTesla**
- **Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)**
- **Tries to harvest and steal browser information (history, passwords, etc)**
- **Tries to harvest and steal ftp login credentials**
- **Tries to steal Mail credentials (via file access)**

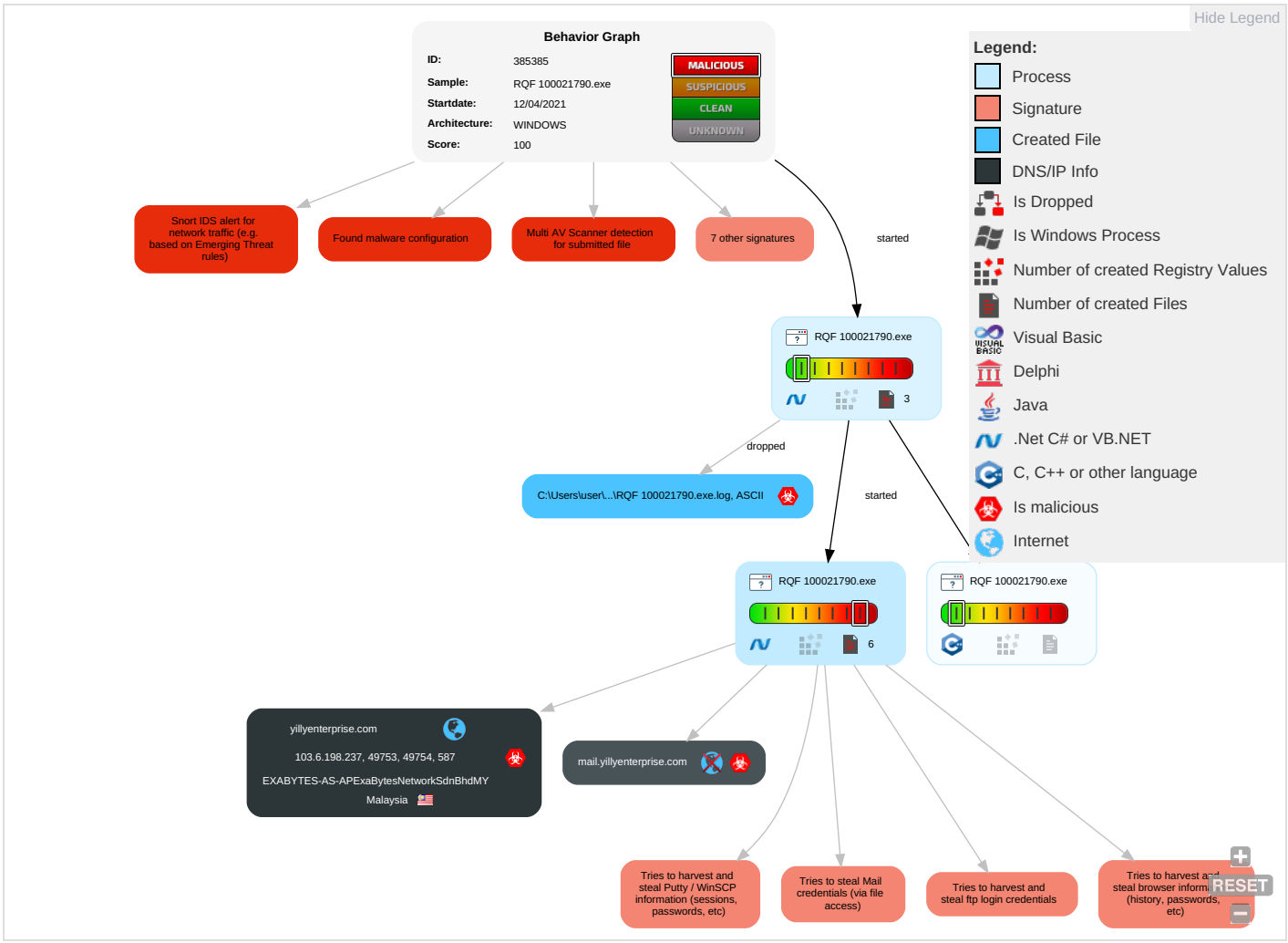
Remote Access Functionality:

- **Yara detected AgentTesla**

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	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 4	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)	Obfuscated Files or Information 2	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)	Software Packing 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 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	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	Process Injection 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

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
RQF 100021790.exe	31%	Virustotal		Browse
RQF 100021790.exe	15%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
RQF 100021790.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.RQF 100021790.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
yillyenterprise.com	0%	Virustotal		Browse
mail.yillyenterprise.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://BtAllR.com	0%	Avira URL Cloud	safe	
http://mail.yillyenterprise.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%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	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://Lt3kEzuSCIaIDgvv.com	0%	Avira URL Cloud	safe	
http://yillyenterprise.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
yillyenterprise.com	103.6.198.237	true	true	• 0%, Virustotal, Browse	unknown
mail.yillyenterprise.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RQF 100021790.exe, 00000003.00000002.471510302.0000000002971000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RQF 100021790.exe, 00000003.00000002.471510302.0000000002971000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://BtAllR.com	RQF 100021790.exe, 00000003.00000002.471510302.0000000002971000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.yillyenterprise.com	RQF 100021790.exe, 00000003.00000002.474061943.0000000002C46000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RQF 100021790.exe, 00000003.00000002.471510302.0000000002971000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	RQF 100021790.exe, 00000000.00000002.207282678.0000000003F89000.00000004.00000001.sdmp, RQF 100021790.exe, 00000003.00000002.466065951.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://Lt3kEzuSCIaIDgvv.com	RQF 100021790.exe, 00000003.00000002.473589734.0000000002BDD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://yillyenterprise.com	RQF 100021790.exe, 00000003.00000002.474061943.0000000002C46000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.6.198.237	yillyenterprise.com	Malaysia		46015	EXABYTES-AS-APExaBytesNetworkSdnBhdMY	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385385
Start date:	12.04.2021
Start time:	12:13:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RQF 100021790.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.spyw.evad.winEXE@5/2@4/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 38.9% • Quality standard deviation: 43.8%
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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.147.198.201, 13.64.90.137, 20.82.210.154, 40.88.32.150, 184.30.24.56, 92.122.213.247, 92.122.213.194, 67.26.137.254, 8.253.95.249, 8.253.95.120, 8.248.141.254, 67.27.159.126, 52.155.217.156, 20.54.26.129 • 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, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.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, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:14:00	API Interceptor	818x Sleep call for process: RQF 100021790.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.6.198.237	RFQ - HASTALLOY MATERIAL.exe	Get hash	malicious	Browse	
	#1002021.exe	Get hash	malicious	Browse	
	#100028153.exe	Get hash	malicious	Browse	
	#ENQ67548820.exe	Get hash	malicious	Browse	
	_0000628.EXE	Get hash	malicious	Browse	
	RFQ#100027386.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EXABYTES-AS-APExaBytesNetworkSdnBhdMY	IK8QsX6z2B1lPY0.exe	Get hash	malicious	Browse	• 137.59.110.57
	efaxHanglung_302.htm	Get hash	malicious	Browse	• 103.6.198.35
	RFQ - HASTALLOY MATERIAL.exe	Get hash	malicious	Browse	• 103.6.198.237
	#1002021.exe	Get hash	malicious	Browse	• 103.6.198.237
	PO AA21C04U3101-MTXGA6_PDF.exe	Get hash	malicious	Browse	• 137.59.110.57
	#100028153.exe	Get hash	malicious	Browse	• 103.6.198.237
	#ENQ67548820.exe	Get hash	malicious	Browse	• 103.6.198.237
	PO AA21C04U3101-MTXGA6_PDF.exe	Get hash	malicious	Browse	• 137.59.110.57
	New Order 1-4-2021_PDF.exe	Get hash	malicious	Browse	• 137.59.110.57
	New Order 1-4-2021_PDF.exe	Get hash	malicious	Browse	• 137.59.110.57
	TaTYytHaBk.exe	Get hash	malicious	Browse	• 110.4.47.139
	_0000628.EXE	Get hash	malicious	Browse	• 103.6.198.237
	confirm bank account details pdf.exe	Get hash	malicious	Browse	• 103.6.198.37
	RFQ#100027386.exe	Get hash	malicious	Browse	• 103.6.198.237
	SWIFT COPY.png.exe	Get hash	malicious	Browse	• 103.6.196.156
	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	• 103.6.196.156
	bank slip 10 285 USD..exe	Get hash	malicious	Browse	• 103.6.198.37
	1 Total New Invoices_Wendesday March 10_2021.xlsm	Get hash	malicious	Browse	• 137.59.109.40
	Request Quotation.exe	Get hash	malicious	Browse	• 103.6.198.37
	change certificate.exe	Get hash	malicious	Browse	• 103.6.196.156

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RQF 100021790.exe.log

Process:	C:\Users\user\Desktop\RQF 100021790.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RQF 100021790.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\bwxcnuey.tk5\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\RQF 100021790.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	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):	7.891722616606059
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:	RQF 100021790.exe
File size:	719360
MD5:	31f58bbbd330f886e422d44e9c21dbf4
SHA1:	1795b60a6f387dec4ac7a6c38119efa0138bdff7
SHA256:	c289703ef1a3645d2c1653c0f571a9abdeec2b404df429196c2523b0b17d9c4c
SHA512:	13c8c5151da7a0ac3409e7c7f2d50ec761377035694275b96f82c77e13979504bd05c68ae5d3a3bcb2fa6d5735f2433e4c98be0ad97e5aa6625f2f820bc542ec
SSDEEP:	12288:N67nnN27JO4zaE+ThxgcHzQC3n0eKR7gZxzhpsFifL:5l4zbYgor3nhX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....j.....0.....L..... .....@.. .....`.....@.....

File Icon

Icon Hash:	b04c9e9ab2c66a92

Static PE Info

General	
Entrypoint:	0x4acb9a
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:	0xCB6A8586 [Tue Feb 22 11:44:06 2078 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xacb48	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xae000	0x495c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xacb2c	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	0xaaba0	0xaac00	False	0.904438426519	data	7.89427057508	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x495c	0x4a00	False	0.932010135135	data	7.8688533795	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xae130	0x42c1	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xb23f4	0x14	data		
RT_VERSION	0xb2408	0x366	data		
RT_MANIFEST	0xb2770	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

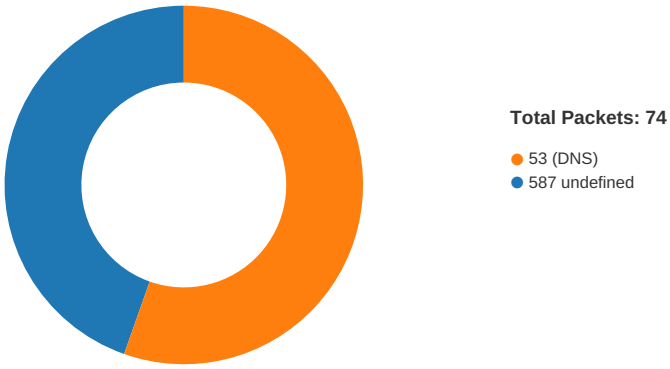
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Integra Wealth
Assembly Version	1.8.9.10
InternalName	wu.exe
FileVersion	1.9.1.0
CompanyName	Integra Wealth
LegalTrademarks	
Comments	
ProductName	ReplacementFallback
ProductVersion	1.9.1.0
FileDescription	ReplacementFallback
OriginalFilename	wu.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-12:15:45.696184	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49753	587	192.168.2.3	103.6.198.237
04/12/21-12:15:50.878674	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49754	587	192.168.2.3	103.6.198.237

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 12:15:42.762054920 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:43.071121931 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:43.071336985 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:43.782385111 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:43.783063889 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:44.092108965 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:44.094373941 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:44.402190924 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:44.402662039 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:44.751108885 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:44.752495050 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:44.761033058 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:45.069158077 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:45.072818041 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:45.383188963 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:45.383842945 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:45.690876007 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:45.690944910 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:45.696183920 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:45.696470976 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:45.696624041 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:45.696784019 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:46.004097939 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:46.004144907 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:46.441358089 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:46.490317106 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:47.621572971 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:47.930361032 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:47.930761099 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:47.932034016 CEST	49753	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:48.096860886 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:48.239238977 CEST	587	49753	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:48.391484976 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:48.391783953 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:49.080897093 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:49.081491947 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:49.373914003 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:49.374644995 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:49.668432951 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:49.669471025 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:49.994201899 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:49.994524956 CEST	49754	587	192.168.2.3	103.6.198.237

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 12:15:50.288446903 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:50.288921118 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:50.585438967 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:50.585814953 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:50.876641035 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:50.876692057 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:50.878473997 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:50.878674030 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:50.878762007 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:50.878869057 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:50.879036903 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:50.879120111 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:50.879215956 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:50.879287958 CEST	49754	587	192.168.2.3	103.6.198.237
Apr 12, 2021 12:15:51.170461893 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:51.170726061 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:51.170878887 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:51.625159025 CEST	587	49754	103.6.198.237	192.168.2.3
Apr 12, 2021 12:15:51.678492069 CEST	49754	587	192.168.2.3	103.6.198.237

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 12:13:51.586704969 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 12:13:52.469470024 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:13:52.520422935 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 12:13:53.392422915 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:13:53.441185951 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 12:13:54.293262959 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:13:54.342257977 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 12:13:55.530160904 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:13:55.581937075 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 12:13:57.751872063 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:13:57.811475039 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 12:13:58.640142918 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:13:58.688821077 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 12:13:59.625888109 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:13:59.675868034 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:05.710988998 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:05.759812117 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:07.595828056 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:07.647330046 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:08.479594946 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:08.528533936 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:19.542860031 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:19.596565962 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:20.452672005 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:20.501466036 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:23.887476921 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:23.939207077 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:25.828679085 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:25.882148981 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:26.902961016 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:26.951574087 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:27.705231905 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:27.753947973 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:28.474406004 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:28.533435106 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:29.341681004 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:29.400687933 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:29.711903095 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:29.772387981 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:38.205297947 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:38.264327049 CEST	53	54366	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 12:14:46.517821074 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:46.570503950 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:50.567768097 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:50.673624992 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:51.201191902 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:51.345591068 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:51.524884939 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:51.599174976 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:51.936480045 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:51.999366999 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:52.471220016 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:52.528228045 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:53.073225021 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:53.156069994 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:53.753889084 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:53.810863972 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:54.299735069 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:54.359675884 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:55.132415056 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:55.226861000 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:56.321180105 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:56.372930050 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 12:14:57.363403082 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:14:57.420798063 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 12, 2021 12:15:02.112020016 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:15:02.160840988 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 12, 2021 12:15:06.356405020 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:15:06.424463987 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 12, 2021 12:15:07.379235029 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:15:07.437526941 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 12, 2021 12:15:37.663800001 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:15:37.712726116 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 12, 2021 12:15:39.711788893 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:15:39.782140970 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 12, 2021 12:15:42.064769983 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:15:42.254080057 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 12, 2021 12:15:42.276153088 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:15:42.655107975 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 12, 2021 12:15:47.973196983 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:15:48.032934904 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 12, 2021 12:15:48.046407938 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:15:48.095315933 CEST	53	55708	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 12:15:42.064769983 CEST	192.168.2.3	8.8.8.8	0x6128	Standard query (0)	mail.yilly enterprise.com	A (IP address)	IN (0x0001)
Apr 12, 2021 12:15:42.276153088 CEST	192.168.2.3	8.8.8.8	0xaab	Standard query (0)	mail.yilly enterprise.com	A (IP address)	IN (0x0001)
Apr 12, 2021 12:15:47.973196983 CEST	192.168.2.3	8.8.8.8	0xa834	Standard query (0)	mail.yilly enterprise.com	A (IP address)	IN (0x0001)
Apr 12, 2021 12:15:48.046407938 CEST	192.168.2.3	8.8.8.8	0xe4ea	Standard query (0)	mail.yilly enterprise.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 12:15:42.254080057 CEST	8.8.8.8	192.168.2.3	0x6128	No error (0)	mail.yilly enterprise.com	yillyenterprise.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 12:15:42.254080057 CEST	8.8.8.8	192.168.2.3	0x6128	No error (0)	yillyenterprise.com		103.6.198.237	A (IP address)	IN (0x0001)
Apr 12, 2021 12:15:42.655107975 CEST	8.8.8.8	192.168.2.3	0xaab	No error (0)	mail.yilly enterprise.com	yillyenterprise.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 12:15:42.655107975 CEST	8.8.8.8	192.168.2.3	0xaab	No error (0)	yillyenterprise.com		103.6.198.237	A (IP address)	IN (0x0001)
Apr 12, 2021 12:15:48.032934904 CEST	8.8.8.8	192.168.2.3	0xa834	No error (0)	mail.yillyenterprise.com	yillyenterprise.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 12:15:48.032934904 CEST	8.8.8.8	192.168.2.3	0xa834	No error (0)	yillyenterprise.com		103.6.198.237	A (IP address)	IN (0x0001)
Apr 12, 2021 12:15:48.095315933 CEST	8.8.8.8	192.168.2.3	0xe4ea	No error (0)	mail.yillyenterprise.com	yillyenterprise.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 12:15:48.095315933 CEST	8.8.8.8	192.168.2.3	0xe4ea	No error (0)	yillyenterprise.com		103.6.198.237	A (IP address)	IN (0x0001)

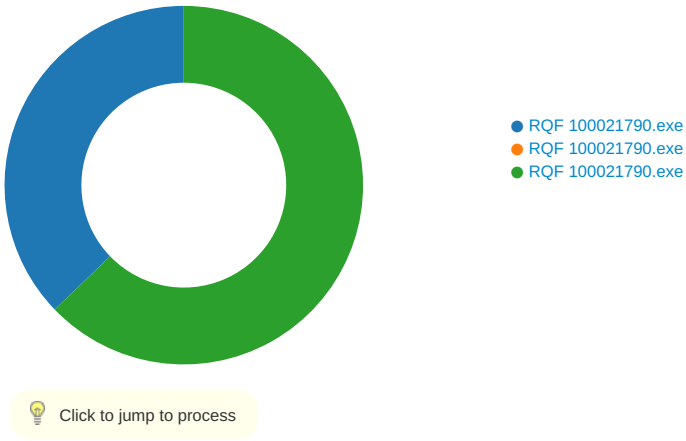
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 12:15:43.782385111 CEST	587	49753	103.6.198.237	192.168.2.3	220-naan.mschosting.com ESMTP Exim 4.94 #2 Mon, 12 Apr 2021 18:15:42 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 12, 2021 12:15:43.783063889 CEST	49753	587	192.168.2.3	103.6.198.237	EHLO 305090
Apr 12, 2021 12:15:44.092108965 CEST	587	49753	103.6.198.237	192.168.2.3	250-naan.mschosting.com Hello 305090 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 12, 2021 12:15:44.094373941 CEST	49753	587	192.168.2.3	103.6.198.237	AUTH login ZWt3ZUB5aWxseWVudGVycHJpc2UuY29t
Apr 12, 2021 12:15:44.402190924 CEST	587	49753	103.6.198.237	192.168.2.3	334 UGFzc3dvcmQ6
Apr 12, 2021 12:15:44.752495050 CEST	587	49753	103.6.198.237	192.168.2.3	235 Authentication succeeded
Apr 12, 2021 12:15:44.761033058 CEST	49753	587	192.168.2.3	103.6.198.237	MAIL FROM:<ekwe@yillyenterprise.com>
Apr 12, 2021 12:15:45.069158077 CEST	587	49753	103.6.198.237	192.168.2.3	250 OK
Apr 12, 2021 12:15:45.072818041 CEST	49753	587	192.168.2.3	103.6.198.237	RCPT TO:<ekwe@yillyenterprise.com>
Apr 12, 2021 12:15:45.383188963 CEST	587	49753	103.6.198.237	192.168.2.3	250 Accepted
Apr 12, 2021 12:15:45.383842945 CEST	49753	587	192.168.2.3	103.6.198.237	DATA
Apr 12, 2021 12:15:45.690944910 CEST	587	49753	103.6.198.237	192.168.2.3	354 Enter message, ending with "." on a line by itself
Apr 12, 2021 12:15:45.696784019 CEST	49753	587	192.168.2.3	103.6.198.237	.
Apr 12, 2021 12:15:46.441358089 CEST	587	49753	103.6.198.237	192.168.2.3	250 OK id=1lVtbc-0001fd-2u
Apr 12, 2021 12:15:47.621572971 CEST	49753	587	192.168.2.3	103.6.198.237	QUIT
Apr 12, 2021 12:15:47.930361032 CEST	587	49753	103.6.198.237	192.168.2.3	221 naan.mschosting.com closing connection
Apr 12, 2021 12:15:49.080897093 CEST	587	49754	103.6.198.237	192.168.2.3	220-naan.mschosting.com ESMTP Exim 4.94 #2 Mon, 12 Apr 2021 18:15:47 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 12, 2021 12:15:49.081491947 CEST	49754	587	192.168.2.3	103.6.198.237	EHLO 305090
Apr 12, 2021 12:15:49.373914003 CEST	587	49754	103.6.198.237	192.168.2.3	250-naan.mschosting.com Hello 305090 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 12, 2021 12:15:49.374644995 CEST	49754	587	192.168.2.3	103.6.198.237	AUTH login ZWt3ZUB5aWxseWVudGVycHJpc2UuY29t
Apr 12, 2021 12:15:49.668432951 CEST	587	49754	103.6.198.237	192.168.2.3	334 UGFzc3dvcmQ6
Apr 12, 2021 12:15:49.994201899 CEST	587	49754	103.6.198.237	192.168.2.3	235 Authentication succeeded
Apr 12, 2021 12:15:49.994524956 CEST	49754	587	192.168.2.3	103.6.198.237	MAIL FROM:<ekwe@yillyenterprise.com>
Apr 12, 2021 12:15:50.288446903 CEST	587	49754	103.6.198.237	192.168.2.3	250 OK
Apr 12, 2021 12:15:50.288921118 CEST	49754	587	192.168.2.3	103.6.198.237	RCPT TO:<ekwe@yillyenterprise.com>
Apr 12, 2021 12:15:50.585438967 CEST	587	49754	103.6.198.237	192.168.2.3	250 Accepted
Apr 12, 2021 12:15:50.585814953 CEST	49754	587	192.168.2.3	103.6.198.237	DATA
Apr 12, 2021 12:15:50.876692057 CEST	587	49754	103.6.198.237	192.168.2.3	354 Enter message, ending with "." on a line by itself
Apr 12, 2021 12:15:50.879287958 CEST	49754	587	192.168.2.3	103.6.198.237	.
Apr 12, 2021 12:15:51.625159025 CEST	587	49754	103.6.198.237	192.168.2.3	250 OK id=1lVtbh-0001iB-8z

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: RQF 100021790.exe PID: 5380 Parent PID: 5724

General

Start time:	12:13:59
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\RQF 100021790.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RQF 100021790.exe'
Imagebase:	0xbc0000
File size:	719360 bytes
MD5 hash:	31F58BBBD330F886E422D44E9C21DBF4
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: 00000000.00000002.207282678.0000000003F89000.00000004.00000001.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	6E0FCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6E0FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RQF 100021790.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	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\RQF 100021790.exe.log	unknown	1216	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: RQF 100021790.exe PID: 3920 Parent PID: 5380

General

Start time:	12:14:02
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\RQF 100021790.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x10000
File size:	719360 bytes
MD5 hash:	31F58BBBD330F886E422D44E9C21DBF4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RQF 100021790.exe PID: 6020 Parent PID: 5380

General

Start time:	12:14:02
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\RQF 100021790.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x530000
File size:	719360 bytes
MD5 hash:	31F58BBBD330F886E422D44E9C21DBF4
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: 00000003.00000002.466065951.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.471510302.0000000002971000.00000004.00000001.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	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Roaming\bwxcnuey.tk5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bwxcnuey.tk5\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	6CF4BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bwxcnuey.tk5\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	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bwxcnuey.tk5\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CF4DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bwxcnuey.tk5\Chrome\Default\Cookies	success or wait	1	6CF46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bwxcnuey.tk5\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 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	6CF4DD66	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\17ae5ee4-f7fe-4016-b300-89e8e17c5c45	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Roaming\bwxcnuey.tk5\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CF41B4F	ReadFile

Disassembly

Code Analysis