ID: 404238
Sample Name:
lT2TTQACRLGKK8w.exe
Cookbook: default.jbs
Time: 20:36:06
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

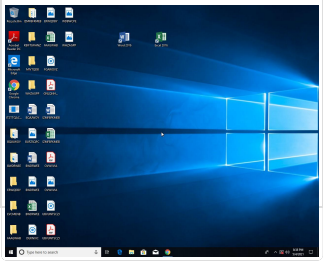
Analysis Report IT2TTQACRLGKK8w.exe

Overview

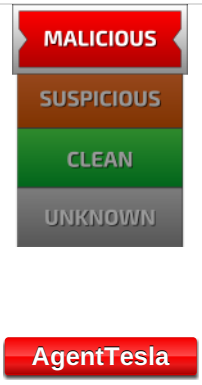
General Information

Sample Name:	IT2TTQACRLGKK8w.exe
Analysis ID:	404238
MD5:	8c2987ef2599664.
SHA1:	2b8425dbc57e93..
SHA256:	b1f7ca6e53ff7dd…
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

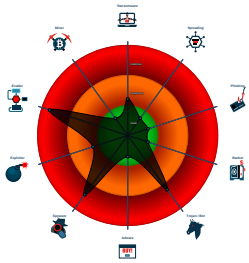


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- IT2TTQACRLGKK8w.exe (PID: 6980 cmdline: 'C:\Users\user\Desktop\IT2TTQACRLGKK8w.exe' MD5: 8C2987EF25996649BE1A2D6F2150A30D)
  - IT2TTQACRLGKK8w.exe (PID: 7092 cmdline: C:\Users\user\Desktop\IT2TTQACRLGKK8w.exe MD5: 8C2987EF25996649BE1A2D6F2150A30D)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "office3@iykmoreentrprise.orgrwkWCM328mail.iykmoreentrprise.org"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.911137710.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.912431014.0000000002A21000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.656573147.000000000412000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.655179728.000000000317000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: IT2TTQACRLGKK8w.exe PID: 7092	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 3 entries

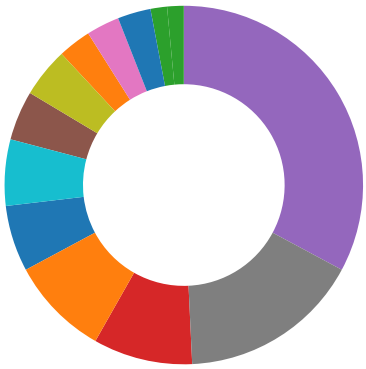
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.IT2TTQACRLGKK8w.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.IT2TTQACRLGKK8w.exe.4234ac8.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.IT2TTQACRLGKK8w.exe.4234ac8.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- 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

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

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)

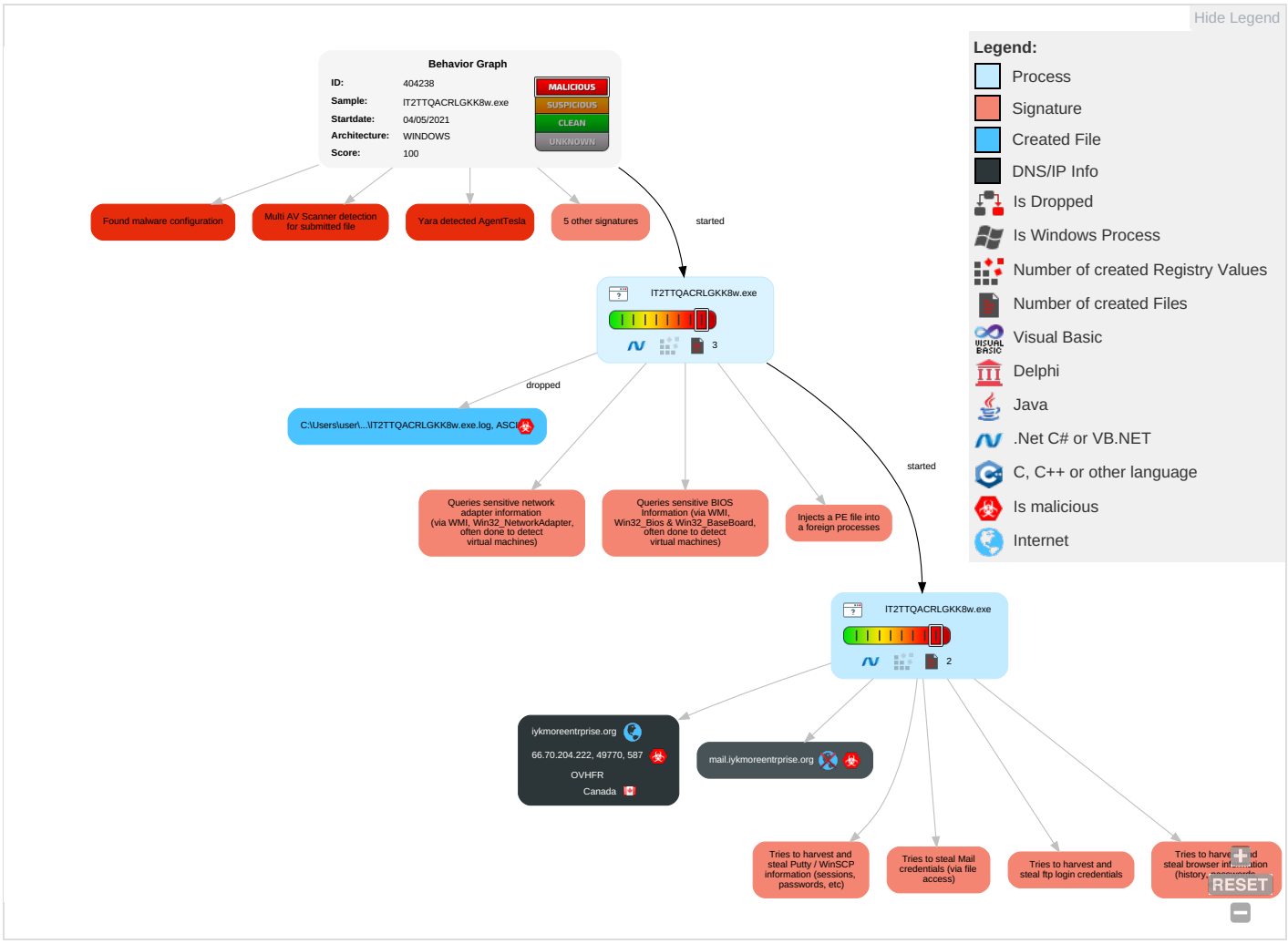
Remote Access Functionality:

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

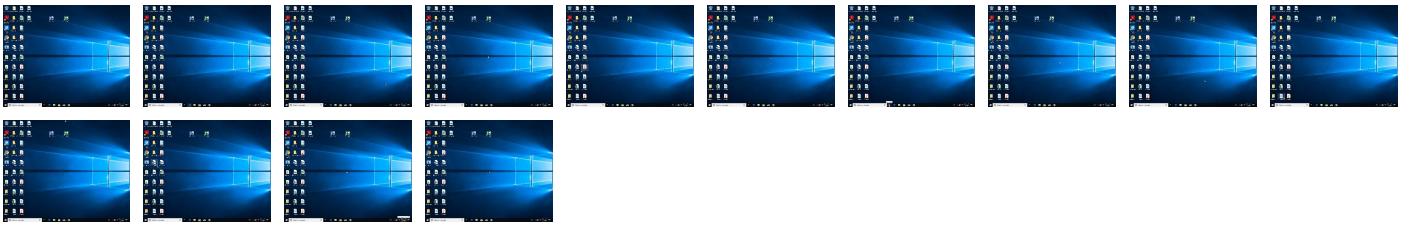
Behavior Graph



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
IT2TTQACRLGKK8w.exe	19%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	
IT2TTQACRLGKK8w.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.IT2TTQACRLGKK8w.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.iykmoreentrprise.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://iykmoreentrprise.org	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://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	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://go.microsoft.cz	0%	Avira URL Cloud	safe	
http://https://wl0H8jlTH4n9kj.org	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://NdOlex.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://mail.iykmoreentrprise.org	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

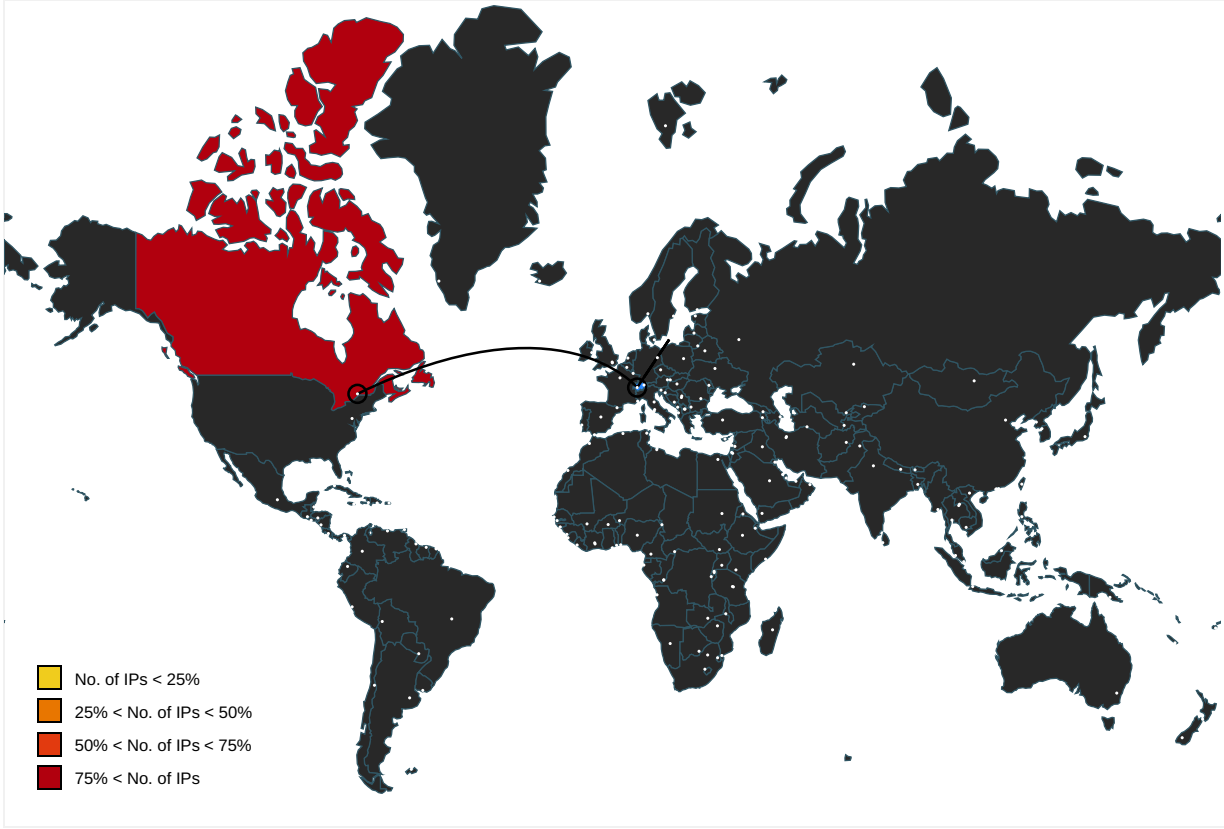
Name	IP	Active	Malicious	Antivirus Detection	Reputation
iykmoreentrprise.org	66.70.204.222	true	true		unknown
mail.iykmoreentrprise.org	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	IT2TTQACRLGKK8w.exe, 00000002.00000002.912431014.0000000002A21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iykmoreentrprise.org	IT2TTQACRLGKK8w.exe, 00000002.00000002.912804837.0000000002D88000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	IT2TTQACRLGKK8w.exe, 00000002.00000002.912431014.0000000002A21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://vbcity.com/forums/t/51894.aspx	IT2TTQACRLGKK8w.exe	false		high
http://cps.letsencrypt.org0	IT2TTQACRLGKK8w.exe, 00000002.00000003.869228156.0000000000FA7000.00000004.00000001.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%tordir%%ha	IT2TTQACRLGKK8w.exe, 00000002.00000002.912431014.0000000002A21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://go.microsoft.cz	IT2TTQACRLGKK8w.exe, 00000002.00000002.912109224.0000000000F03000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wl0H8jlTH4n9kj.org	IT2TTQACRLGKK8w.exe, 00000002.00000002.912725062.0000000002D32000.00000004.00000001.sdmp, IT2TTQACRLGKK8w.exe, 00000002.00000002.912880410.0000000002DB5000.00000004.00000001.sdmp, IT2TTQACRLGKK8w.exe, 00000002.00000002.912771188.0000000002D7E000.00000004.00000001.sdmp, IT2TTQACRLGKK8w.exe, 00000002.00000002.912865775.0000000002DAD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	IT2TTQACRLGKK8w.exe, 00000002.00000003.869228156.0000000000FA7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	IT2TTQACRLGKK8w.exe, 00000002.00000002.912431014.0000000002A21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://NdOlex.com	IT2TTQACRLGKK8w.exe, 00000002.00000002.912431014.0000000002A21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	IT2TTQACRLGKK8w.exe, 00000000.00000002.655099093.0000000003121000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	IT2TTQACRLGKK8w.exe, 00000000.00000002.656573147.0000000004129000.00000004.00000001.sdmp, IT2TTQACRLGKK8w.exe, 00000002.00000002.911137710.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	IT2TTQACRLGKK8w.exe, 00000000.00000002.655179728.0000000003174000.00000004.00000001.sdmp	false		high
http://mail.iykmoreentrprise.org	IT2TTQACRLGKK8w.exe, 00000002.00000002.912804837.0000000002D88000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%$	IT2TTQACRLGKK8w.exe, 00000002.00000002.912431014.0000000002A21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://cps.root-x1.letsencrypt.org0	IT2TTQACRLGKK8w.exe, 00000002.00000003.869228156.0000000000FA7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0	IT2TTQACRLGKK8w.exe, 00000002.00000003.869228156.0000000000FA7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/MrCylops	IT2TTQACRLGKK8w.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.70.204.222	iykmoreentrprise.org	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404238
Start date:	04.05.2021
Start time:	20:36:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IT2TTQACRLGKK8w.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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@2/1
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 • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.139.144, 13.88.21.125, 13.64.90.137, 40.88.32.150, 52.147.198.201, 20.82.210.154, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 40.64.101.146, 2.20.142.209, 2.20.142.210, 20.50.102.62 • Excluded domains from analysis (whitelisted): mw1eap.displaycatalog.md.mp.microsoft.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.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, consumerrp-displaycatalog-aks2eap-uswest.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, displaycatalog-uswesteap.md.mp.microsoft.com.akadns.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:36:55	API Interceptor	816x Sleep call for process: IT2TTQACRLGKK8w.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.70.204.222	pd9EeXdsQtNb3dQ.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.MSIL_Troj.ASI.genEldorado.27642.exe	Get hash	malicious	Browse	
	MZyeln5mSFOjxMx.exe	Get hash	malicious	Browse	
	FFrIJMwrI9cxeIZ.exe	Get hash	malicious	Browse	
	cljz48xwqb2VSBN.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QTY 98657 RFQ MANDATE 020521.0003YDK.exe	Get hash	malicious	Browse	
	foakTEjUOvL9nBY.exe	Get hash	malicious	Browse	
	n4QstFh7YkjVcrU.exe	Get hash	malicious	Browse	
	AVuOP2vLzIMRG88.exe	Get hash	malicious	Browse	
	316e3796_by_Libranalysis.exe	Get hash	malicious	Browse	
	GQTY 98657 RFQ MANDATE 28421.02AWYD.exe	Get hash	malicious	Browse	
	VJNPltkyHyI3CCo.exe	Get hash	malicious	Browse	
	0L2qr7kJMh40sxq.exe	Get hash	malicious	Browse	
	ApuE9QrdQxe7Um6.exe	Get hash	malicious	Browse	
	77iET1jNLJyV8ez.exe	Get hash	malicious	Browse	
	bOkrXdoYekZPyWI.exe	Get hash	malicious	Browse	
	ayZYB5SkqMPA06M.exe	Get hash	malicious	Browse	
	fyZ6iHys7ClIHFR.exe	Get hash	malicious	Browse	
	uMLNLd9kgPez84h.exe	Get hash	malicious	Browse	
	YQfInBo2DDpDfIX.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
OVHFR	165395_BHU.msi	Get hash	malicious	Browse	• 158.69.144.121
	jEEGrwHI1H.exe	Get hash	malicious	Browse	• 51.195.61.169
	6R9cyNLikC.exe	Get hash	malicious	Browse	• 51.195.61.169
	c862293a_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	29ec7ed7_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	c862293a_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	29ec7ed7_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	37d2a6e3_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	0f003adb_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	a5a88fbb_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	d2d35294_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	58917039_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	636f06a6_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	37d2a6e3_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	0f003adb_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	a5a88fbb_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	636f06a6_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	d2d35294_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IT2TTQACRLGKK8w.exe.log

Process:	C:\Users\user\Desktop\IT2TTQACRLGKK8w.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IT2TTQACRLGKK8w.exe.log	
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.481252144870754
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:	IT2TTQACRLGKK8w.exe
File size:	694272
MD5:	8c2987ef25996649be1a2d6f2150a30d
SHA1:	2b8425dbc57e93fbb2a9bf6d45a491ccc15f0d5d
SHA256:	b1f7ca6e53ff7dd757a49539f5e5c18bfeabbe24b06270ce08df45f1c2effff
SHA512:	381ad7adbbe661b1bf4e58a94c8b885ad2f94cdb994dede6f94025c6587218653cb79c1fa0b8ecb9c8e8682c2cafb64d3247aa5d4cb99f883dbb44ed1d96e0bb
SSDEEP:	12288:Yt/TBPnNHKManc2gOAQLJtQYxMxJrw9a76Yij+fKFKATuQyrz9+srtgO3pP2:YqfQYx8J09uk6fKEDp1L5P2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4aaa12
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:	0x9913AE82 [Sat May 20 13:58:26 2051 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xaa9c0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0x60c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xaa9a4	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	0xa8a18	0xa8c00	False	0.79830150463	data	7.4929930225	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x60c	0x800	False	0.32958984375	data	3.4332919236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	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_VERSION	0xac090	0x37c	data		
RT_MANIFEST	0xac41c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

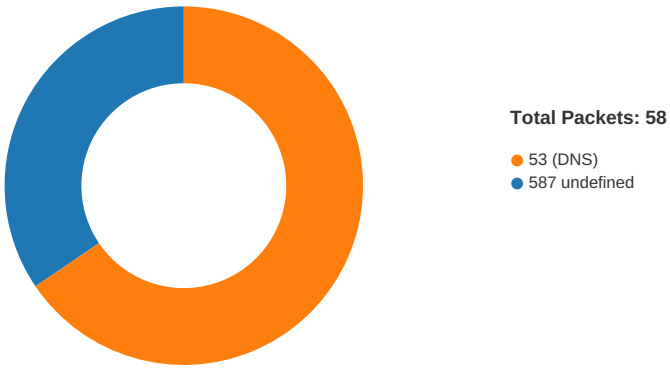
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:38:36.071686983 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:36.201476097 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:36.201631069 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:36.358669043 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:36.359447002 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:36.492664099 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:36.493119955 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:36.624587059 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:36.671040058 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:36.711306095 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:36.847898006 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:36.847923994 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:36.847935915 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:36.848001957 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:36.857160091 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:36.994720936 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:37.046267033 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:37.305923939 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:37.436254978 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:37.438693047 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:37.568897009 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:37.570415020 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:37.721539021 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:37.722697020 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:37.854373932 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:37.855051994 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:37.985609055 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:37.986335039 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:38.116169930 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:38.119088888 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:38.119370937 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:38.120187998 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:38.120382071 CEST	49770	587	192.168.2.4	66.70.204.222
May 4, 2021 20:38:38.251784086 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:38.251806021 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:38.252053022 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:38.252562046 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:38.253463984 CEST	587	49770	66.70.204.222	192.168.2.4
May 4, 2021 20:38:38.296133041 CEST	49770	587	192.168.2.4	66.70.204.222

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:36:46.585772991 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 20:36:46.634201050 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 20:36:48.053796053 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 20:36:48.105243921 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 20:36:49.203061104 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 20:36:49.254549980 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 20:36:50.551326036 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 20:36:50.608330965 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 20:36:52.393086910 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 20:36:52.442821026 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 20:36:53.377943993 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 20:36:53.429469109 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 20:36:54.522610903 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 20:36:54.582078934 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 20:36:56.112008095 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 20:36:56.163491011 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 20:36:57.362030983 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:36:57.410797119 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 20:36:58.707501888 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 20:36:58.756108999 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 20:36:59.895889044 CEST	56627	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:36:59.947436094 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 20:37:01.627568960 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:01.677361012 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 20:37:02.856363058 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:02.907125950 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 20:37:05.890660048 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:05.939929008 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 20:37:07.141864061 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:07.192564964 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 20:37:07.913377047 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:07.975424051 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 20:37:09.184504032 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:09.236638069 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 20:37:11.567977905 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:11.619905949 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 20:37:12.461430073 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:12.512180090 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 20:37:16.670963049 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:16.721472979 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 20:37:21.651101112 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:21.709496975 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 20:37:38.350974083 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:38.500468969 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 20:37:39.094322920 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:39.154207945 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 20:37:39.712543964 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:39.772344112 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 20:37:40.102238894 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:40.167395115 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 20:37:40.205920935 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:40.350033045 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 20:37:41.551826000 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:41.609040976 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 20:37:41.638432980 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:41.695399046 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 20:37:42.965420008 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:43.028286934 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 20:37:43.536386013 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:43.667934895 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 20:37:44.458900928 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:44.516117096 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 20:37:45.366816044 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:45.424849987 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 20:37:45.950923920 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:45.999566078 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 20:37:54.138750076 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 20:37:54.188909054 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 20:38:26.354702950 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 20:38:26.406428099 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 20:38:28.856625080 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 20:38:28.917644978 CEST	53	60689	8.8.8.8	192.168.2.4
May 4, 2021 20:38:35.787714005 CEST	64206	53	192.168.2.4	8.8.8.8
May 4, 2021 20:38:35.867779970 CEST	53	64206	8.8.8.8	192.168.2.4
May 4, 2021 20:38:35.883652925 CEST	50904	53	192.168.2.4	8.8.8.8
May 4, 2021 20:38:35.956926107 CEST	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:38:35.787714005 CEST	192.168.2.4	8.8.8.8	0xd34c	Standard query (0)	mail.iykmo reentrprise.org	A (IP address)	IN (0x0001)
May 4, 2021 20:38:35.883652925 CEST	192.168.2.4	8.8.8.8	0x4b1b	Standard query (0)	mail.iykmo reentrprise.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:38:35.867779970 CEST	8.8.8.8	192.168.2.4	0xd34c	No error (0)	mail.iykmoreentrprise.org	iykmoreentrprise.org		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:38:35.867779970 CEST	8.8.8.8	192.168.2.4	0xd34c	No error (0)	iykmoreentrprise.org		66.70.204.222	A (IP address)	IN (0x0001)
May 4, 2021 20:38:35.956926107 CEST	8.8.8.8	192.168.2.4	0x4b1b	No error (0)	mail.iykmoreentrprise.org	iykmoreentrprise.org		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:38:35.956926107 CEST	8.8.8.8	192.168.2.4	0x4b1b	No error (0)	iykmoreentrprise.org		66.70.204.222	A (IP address)	IN (0x0001)

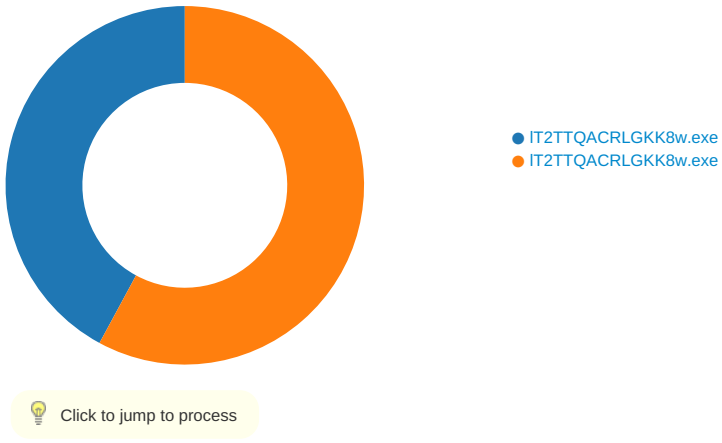
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 20:38:36.358669043 CEST	587	49770	66.70.204.222	192.168.2.4	220-server.wlcserver.com ESMTP Exim 4.94 #2 Tue, 04 May 2021 22:38:36 +0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 4, 2021 20:38:36.359447002 CEST	49770	587	192.168.2.4	66.70.204.222	EHLO 849224
May 4, 2021 20:38:36.492664099 CEST	587	49770	66.70.204.222	192.168.2.4	250-server.wlcserver.com Hello 849224 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-STARTTLS 250 HELP
May 4, 2021 20:38:36.493119955 CEST	49770	587	192.168.2.4	66.70.204.222	STARTTLS
May 4, 2021 20:38:36.624587059 CEST	587	49770	66.70.204.222	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: lT2TTQACRLGKK8w.exe PID: 6980 Parent PID: 5972

General

Start time:	20:36:53
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\IT2TTQACRLGKK8w.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IT2TTQACRLGKK8w.exe'
Imagebase:	0xcb0000
File size:	694272 bytes
MD5 hash:	8C2987EF25996649BE1A2D6F2150A30D
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: 00000000.00000002.656573147.0000000004129000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.655179728.0000000003174000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IT2TTQACRLGKK8w.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IT2TTQACRLGKK8w.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D4DC907	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: IT2TTQACRLGKK8w.exe PID: 7092 Parent PID: 6980

General

Start time:	20:36:57
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\IT2TTQACRLGKK8w.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\IT2TTQACRLGKK8w.exe
Imagebase:	0x6f0000
File size:	694272 bytes
MD5 hash:	8C2987EF25996649BE1A2D6F2150A30D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.911137710.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.912431014.0000000002A21000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\a7df3299-2529-4f0f-a49b-925ded3ec4c1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C011B4F	ReadFile

Disassembly

Code Analysis