ID: 321397
Sample Name:
jF6LSw9bnC.exe
Cookbook: default.jbs
Time: 11:48:17
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

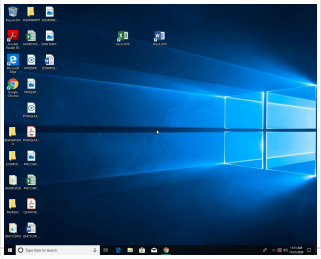
Analysis Report jF6LSw9bnC.exe

Overview

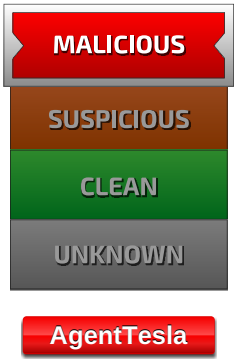
General Information

Sample Name:	jF6LSw9bnC.exe
Analysis ID:	321397
MD5:	020bc13012ce4d..
SHA1:	46f8ff39e0d5f476..
SHA256:	265e971392e878..
Tags:	exe

Most interesting Screenshot:



Detection

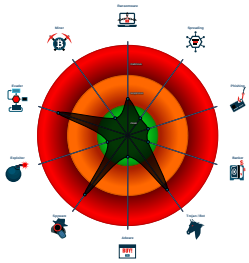


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Hides that the sample has been dow…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Moves itself to temp directory
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- jF6LSw9bnC.exe (PID: 5864 cmdline: 'C:\Users\user\Desktop\jF6LSw9bnC.exe' MD5: 020BC13012CE4DB6E204CB1ED174851E)
  - jF6LSw9bnC.exe (PID: 6056 cmdline: jF6LSw9bnC.exe MD5: 020BC13012CE4DB6E204CB1ED174851E)
  - jF6LSw9bnC.exe (PID: 6024 cmdline: jF6LSw9bnC.exe MD5: 020BC13012CE4DB6E204CB1ED174851E)
  - jF6LSw9bnC.exe (PID: 5888 cmdline: jF6LSw9bnC.exe MD5: 020BC13012CE4DB6E204CB1ED174851E)
- YYtJku.exe (PID: 5004 cmdline: 'C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe' MD5: 020BC13012CE4DB6E204CB1ED174851E)
  - YYtJku.exe (PID: 6124 cmdline: YYtJku.exe MD5: 020BC13012CE4DB6E204CB1ED174851E)
- YYtJku.exe (PID: 5940 cmdline: 'C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe' MD5: 020BC13012CE4DB6E204CB1ED174851E)
  - YYtJku.exe (PID: 4092 cmdline: YYtJku.exe MD5: 020BC13012CE4DB6E204CB1ED174851E)
  - YYtJku.exe (PID: 4260 cmdline: YYtJku.exe MD5: 020BC13012CE4DB6E204CB1ED174851E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "AmggJD",
  "URL: ": "https://cmY5Rn8HrJ6zxDC.com",
  "To: ": "ralcerreca@valle-maule.cl",
  "ByHost: ": "us2.smtp.mailhostbox.com:587",
  "Password: ": "gxpTPioxht6x4ob",
  "From: ": "ralcerreca@valle-maule.cl"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.469149092.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000003.212487577.0000000005CE5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.475373692.000000000339 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.475373692.000000000339 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000E.00000002.334212460.00000000058F5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 23 entries				

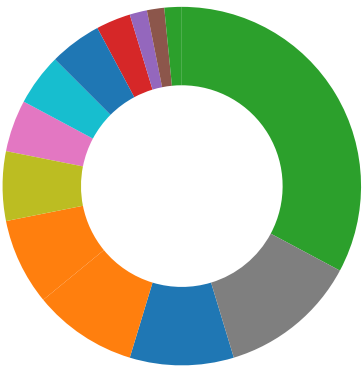
Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.YYtJku.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.2.YYtJku.exe.5810000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.jF6LSw9bnC.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.2.YYtJku.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
12.2.YYtJku.exe.56c0000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Moves itself to temp directory

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

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)

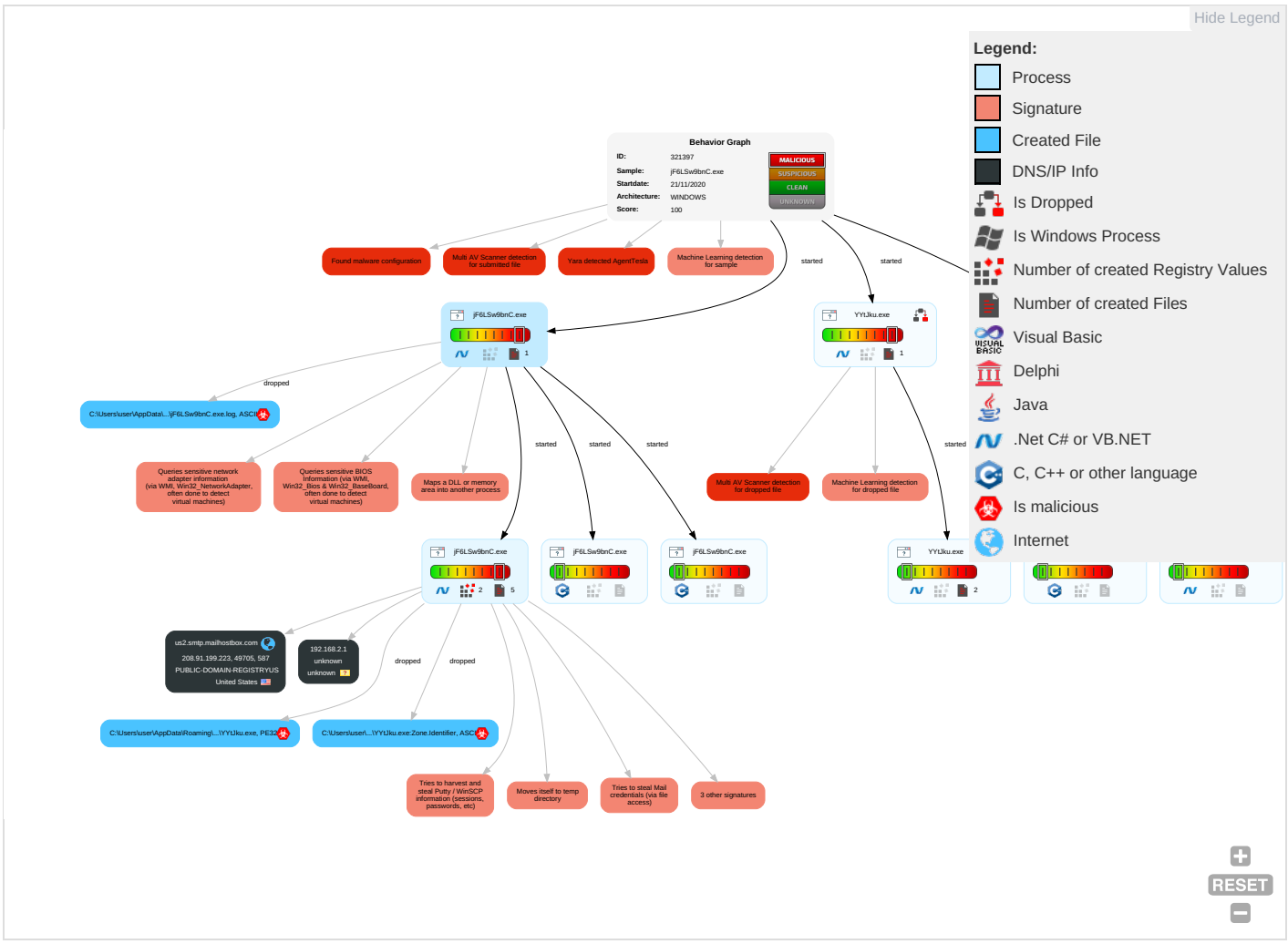
Remote Access Functionality:

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

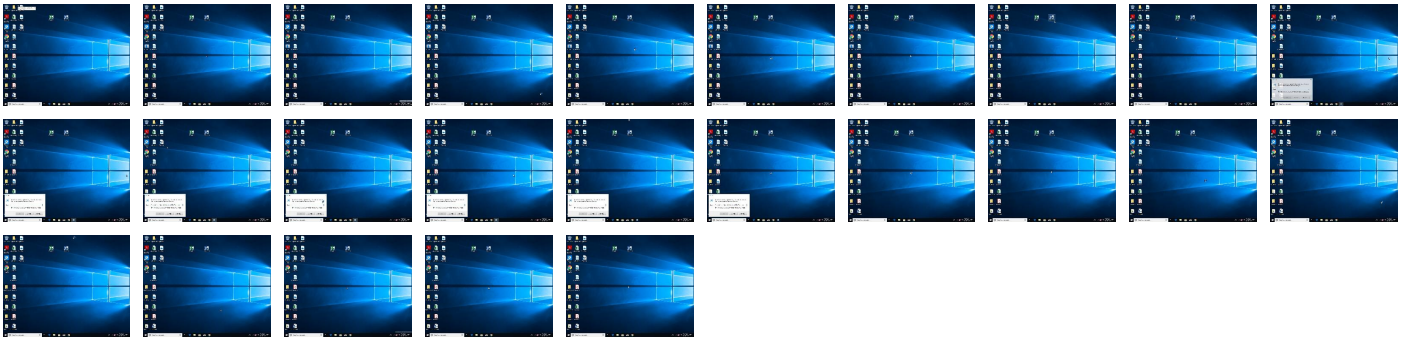
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
jF6LSw9bnC.exe	46%	Virustotal		Browse
jF6LSw9bnC.exe	48%	ReversingLabs	ByteCode-MSIL.Spyware.Wacatac	
jF6LSw9bnC.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	46%	Virustotal		Browse
C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	48%	ReversingLabs	ByteCode-MSIL.Spyware.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.YYtJku.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.2.YYtJku.exe.5810000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
3.2.jF6LSw9bnC.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
16.2.YYtJku.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.2.YYtJku.exe.56c0000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.jF6LSw9bnC.exe.59a0000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://HsjGXz.com	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://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://cmY5Rn8HrJ6zxDC.com	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high

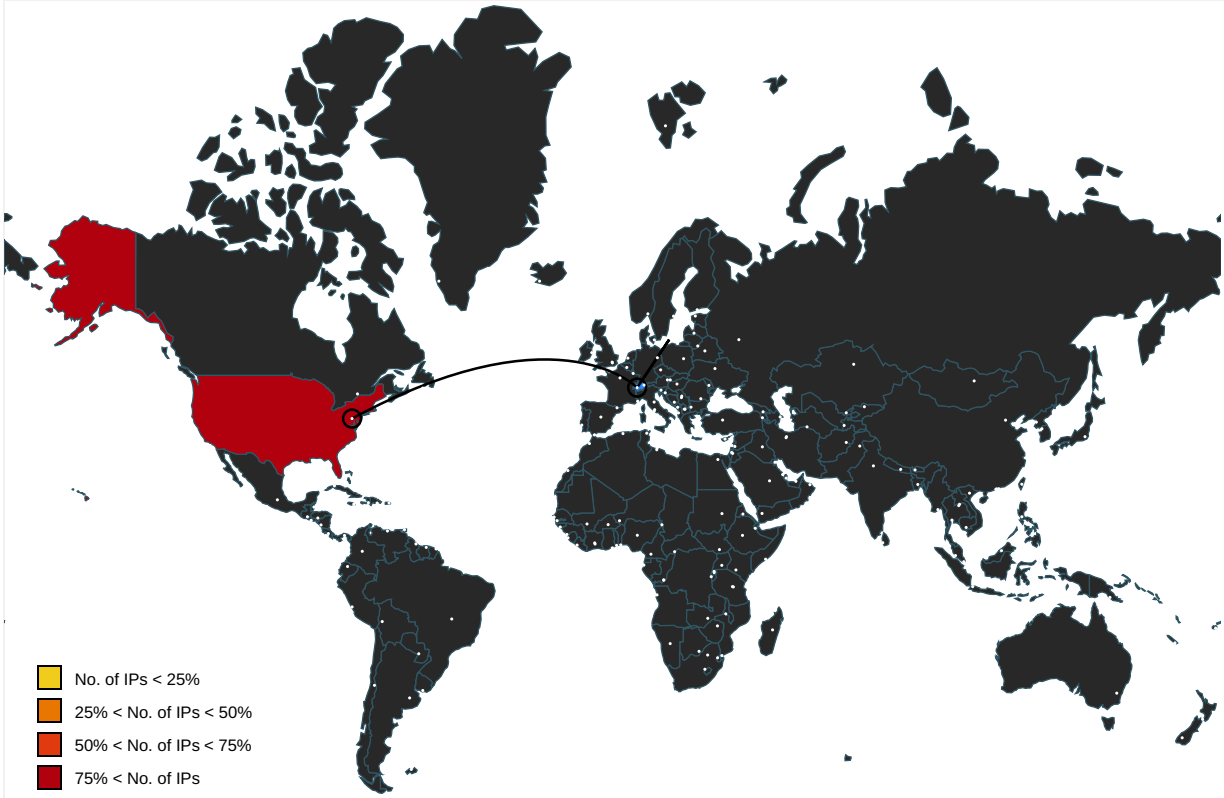
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	jF6LSw9bnC.exe, 00000003.00000002.481145752.0000000006B80000.00000004.00000001.sdmp	false	URL Reputation: safe URL Reputation: safe URL Reputation: safe URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	jF6LSw9bnC.exe, 00000003.00000002.475373692.0000000003391000.00000004.00000001.sdmp, YYtJku.exe, 0000000D.00000002.474483881.0000000002F91000.00000004.00000001.sdmp, YYtJku.exe, 00000010.00000002.474773451.0000000003471000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://HsjGXz.com	YYtJku.exe, 00000010.00000002.474773451.0000000003471000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	YYtJku.exe, 00000010.00000002.474773451.0000000003471000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	jF6LSw9bnC.exe, 00000003.00000002.481145752.0000000006B80000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	jF6LSw9bnC.exe, 00000003.00000002.478242440.00000000036EA000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	jF6LSw9bnC.exe, 00000003.00000002.475373692.0000000003391000.00000004.00000001.sdmp, YYtJku.exe, 0000000D.00000002.474483881.0000000002F91000.00000004.00000001.sdmp, YYtJku.exe, 00000010.00000002.474773451.0000000003471000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	jF6LSw9bnC.exe, 00000000.00000003.212487577.0000000005CE5000.00000004.00000001.sdmp, jF6LSw9bnC.exe, 00000003.00000002.469106569.0000000000402000.00000040.00000001.sdmp, YYtJku.exe, 0000000C.00000002.307682957.0000000004B54000.00000004.00000001.sdmp, YYtJku.exe, 0000000D.00000002.469108481.0000000000402000.00000040.00000001.sdmp, YYtJku.exe, 0000000E.00000002.334212460.00000000058F5000.00000004.00000001.sdmp, YYtJku.exe, 00000010.00000002.469149092.0000000000402000.00000040.00000001.sdmp	false		high
http://https://cmY5Rn8HrJ6zxDC.com	jF6LSw9bnC.exe, 00000003.00000002.475373692.0000000003391000.00000004.00000001.sdmp, jF6LSw9bnC.exe, 00000003.00000002.478507569.0000000003712000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0A	jF6LSw9bnC.exe, 00000003.00000002.481145752.0000000006B80000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	jF6LSw9bnC.exe, 00000003.00000002.475373692.0000000003391000.00000004.00000001.sdmp, YYtJku.exe, 0000000D.00000002.474483881.0000000002F91000.00000004.00000001.sdmp, YYtJku.exe, 00000010.00000002.474773451.0000000003471000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	jF6LSw9bnC.exe, 00000000.00000003.212487577.0000000005CE5000.00000004.00000001.sdmp, jF6LSw9bnC.exe, 00000003.00000002.469106569.0000000000402000.00000040.00000001.sdmp, YYtJku.exe, 0000000C.00000002.307682957.0000000004B54000.00000004.00000001.sdmp, YYtJku.exe, 0000000D.00000002.469108481.0000000000402000.00000040.00000001.sdmp, YYtJku.exe, 0000000E.00000002.334212460.00000000058F5000.00000004.00000001.sdmp, YYtJku.exe, 00000010.00000002.469149092.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.orgGETMozilla/5.0	YYtJku.exe, 00000010.00000002.474773451.0000000003471000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.223	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321397
Start date:	21.11.2020
Start time:	11:48:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	jF6LSw9bnC.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@9215/4@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.1%) • Quality average: 23.2% • Quality standard deviation: 35.3%
HCA Information:	• Successful, ratio: 87% • 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): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.42.151.234, 40.88.32.150, 23.210.248.85 • Excluded domains from analysis (whitelisted): skypedataprdcoleus15.cloudapp.net, fs.microsoft.com, blobcollector.events.data.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolwus16.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • 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
11:49:25	API Interceptor	768x Sleep call for process: jF6LSw9bnC.exe modified
11:49:38	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run YYtJku C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
11:49:46	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run YYtJku C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
11:50:05	API Interceptor	881x Sleep call for process: YYtJku.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	yQDGREHA9h.exe	Get hash	malicious	Browse	
	PO1.xlsx	Get hash	malicious	Browse	
	Vd58qg0dhp.exe	Get hash	malicious	Browse	
	Wrong Transfer Payment - Chk Clip Copy.exe	Get hash	malicious	Browse	
	Doc.exe	Get hash	malicious	Browse	
	SWIFT.exe	Get hash	malicious	Browse	
	TNT Receipt_AWB87993766478.exe	Get hash	malicious	Browse	
	BALANCE PAYMENT.exe	Get hash	malicious	Browse	
	remittance advice_pdf_____.exe	Get hash	malicious	Browse	
	4Pqkg8wt6j.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.461.28807.exe	Get hash	malicious	Browse	
	sOZgfrw6FT.exe	Get hash	malicious	Browse	
	Steel Clik PO#7770022460.exe	Get hash	malicious	Browse	
	P.O. #HBG00356.doc (2).exe	Get hash	malicious	Browse	
	lA1LHK759T.exe	Get hash	malicious	Browse	
	bOp4cgWZkD.exe	Get hash	malicious	Browse	
	5uWZrHiNrw.exe	Get hash	malicious	Browse	
	LUD6Fjo15x.exe	Get hash	malicious	Browse	
	Akribis Systems Pte New PO2006115.exe	Get hash	malicious	Browse	
	5NFH9k6VIL.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	yQDGREHA9h.exe	Get hash	malicious	Browse	• 208.91.199.223
	mcsrXx9lfD.exe	Get hash	malicious	Browse	• 208.91.199.225
	Bill # 2.xlsx	Get hash	malicious	Browse	• 208.91.198.143
	PO1.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 208.91.199.224
	0hgHwEkIWY.exe	Get hash	malicious	Browse	• 208.91.198.143
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order List.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Shipping doc.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	OrV86zxFWHW1j0f.exe	Get hash	malicious	Browse	• 208.91.199.224
	XDMBhLJxD1Qf7JW.exe	Get hash	malicious	Browse	• 208.91.199.224
	me4qssWAMQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	Vd58qg0dhp.exe	Get hash	malicious	Browse	• 208.91.199.223
	15egpuWfT3.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details.exe	Get hash	malicious	Browse	• 208.91.198.143
	Wrong Transfer Payment - Chk Clip Copy.exe	Get hash	malicious	Browse	• 208.91.199.223
	WireTransfer Copy767.exe	Get hash	malicious	Browse	• 208.91.199.225
	DOH0003675550.pdf.exe	Get hash	malicious	Browse	• 208.91.199.224

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	yQDGREHA9h.exe	Get hash	malicious	Browse	• 208.91.199.223
	mcsrXx9lfD.exe	Get hash	malicious	Browse	• 208.91.199.225
	fattura.exe	Get hash	malicious	Browse	• 162.222.226.70
	Pagamento.exe	Get hash	malicious	Browse	• 162.222.226.70
	PO1.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 208.91.199.224
	Zahlung.exe	Get hash	malicious	Browse	• 162.222.226.70
	0hgHwEkIWY.exe	Get hash	malicious	Browse	• 208.91.198.143
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	Zahlung.exe	Get hash	malicious	Browse	• 162.222.226.70
	Lieferadresse.exe	Get hash	malicious	Browse	• 162.222.226.70
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order List.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Shipping doc.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	OrV86zxFWHW1j0f.exe	Get hash	malicious	Browse	• 208.91.199.224
	XDMBhLJxD1Qf7JW.exe	Get hash	malicious	Browse	• 208.91.199.224
	me4qssWAMQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	Vd58qg0dhp.exe	Get hash	malicious	Browse	• 208.91.199.223
	15egpuWfT3.exe	Get hash	malicious	Browse	• 208.91.199.224

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	Catalog of our new order.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\YYtJku.exe.log	
Process:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.350410246151501
Encrypted:	false
SSDEEP:	6:Q3La/xwcE73FKDLIP12MUAvvr3tDLIP12MUAvvR+uTL2LDY3U21v:Q3La/hg1KDLI4M9tDLI4MWuPk21v
MD5:	EE0BB4B63A030A0BF7087CB0AEBD07BC
SHA1:	9A4ADFB6336E22D49503B4B99FFC25A7882AE202
SHA-256:	6CBBAF20B7871B931A8A0B1D54890DC0E6C9ED78E7DEC5E2AB2F6D12DF349DFF
SHA-512:	47644A669A15A83D0BAA1F801BB34E36B1F8FE700E5C7A4396D684FE85AFFF6B32F511AEDD0E304DB48383E04A5044CA1B313D559737F5CD967CC00F8FDFC38B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\jF6LSw9bnC.exe.log	
Process:	C:\Users\user\Desktop\jF6LSw9bnC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.350410246151501
Encrypted:	false
SSDEEP:	6:Q3La/xwcE73FKDLIP12MUAvvr3tDLIP12MUAvvR+uTL2LDY3U21v:Q3La/hg1KDLI4M9tDLI4MWuPk21v
MD5:	EE0BB4B63A030A0BF7087CB0AEBD07BC
SHA1:	9A4ADFB6336E22D49503B4B99FFC25A7882AE202
SHA-256:	6CBBAF20B7871B931A8A0B1D54890DC0E6C9ED78E7DEC5E2AB2F6D12DF349DFF
SHA-512:	47644A669A15A83D0BAA1F801BB34E36B1F8FE700E5C7A4396D684FE85AFFF6B32F511AEDD0E304DB48383E04A5044CA1B313D559737F5CD967CC00F8FDFC38B
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..

C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	
Process:	C:\Users\user\Desktop\jF6LSw9bnC.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	618496
Entropy (8bit):	7.861639609576483

C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	
Encrypted:	false
SSDEEP:	12288:QCuRfLw9sjK8YFIxdsk9fE4ZSgexsOGnAZK0yCcxx:iREr9kFZTOlZ4CW
MD5:	020BC13012CE4DB6E204CB1ED174851E
SHA1:	46F8FF39E0D5F476B0C2E3A1C8FEEFDFEC32A0B2
SHA-256:	265E971392E878A245DEF23CC9544060FCAFBDC0C61C66CF128688F3D64E2179
SHA-512:	891367401D14B9E41FC0379FC0BDC04526E023E01F6E91C731D14C790B8B6483A11761C34B2D5A673B73ACD45761D11916E6A4A6D692C9E4955AD86F7B00B079
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 48%
Joe Sandbox View:	• Filename: Catalog of our new order.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...:._.....h.....N.... .....@.. .....T.. ..@.....K.....B..... ....H.....text...Tg... ...h..... ..`.rsrc...B.....j.....@..@.rel oc.....n.....@..B.....0.....H.....`.....q..pu.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D. E.F.G.H.I.J.K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(.....*..*..(....*.(.....(....(.....(....(....o.....*&...o....*.(....*.(....*.r. ..p.....*6..{b...(^...*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\jF6LSw9bnC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.861639609576483
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	jF6LSw9bnC.exe
File size:	618496
MD5:	020bc13012ce4db6e204cb1ed174851e
SHA1:	46f8ff39e0d5f476b0c2e3a1c8feefdfec32a0b2
SHA256:	265e971392e878a245def23cc9544060fcafbdc0c61c66cf128688f3d64e2179
SHA512:	891367401d14b9e41fc0379fc0bdc04526e023e01f6e91c731d14c790b8b6483a11761c34b2d5a673b73acd45761d11916e6a4a6d692c9e4955ad86f7b00b079
SSDEEP:	12288:QCuRfLw9sjK8YFIxdsk9fE4ZSgexsOGnAZK0yCcxx:iREr9kFZTOlZ4CW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....:._.....h.....N.... .....@.. .....T.. ..@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49874e
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:	0x5FB7B03A [Fri Nov 20 12:02:02 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x98700	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9a000	0x242	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x96754	0x96800	False	0.918753893272	data	7.86673164949	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9a000	0x242	0x400	False	0.310546875	data	3.56952524932	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

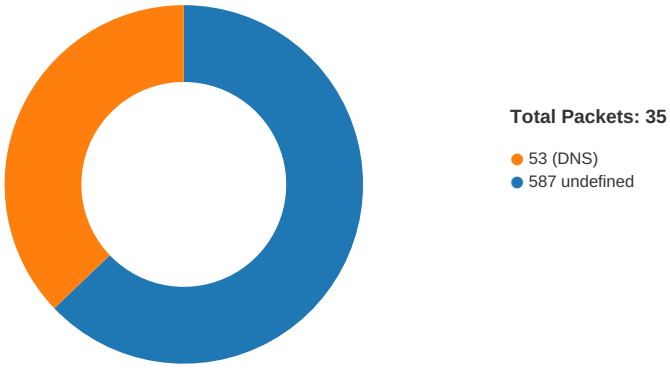
Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x9a058	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 11:50:53.307959080 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:53.447977066 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:53.448226929 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:54.152650118 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.153371096 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:54.293317080 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.293366909 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.293935061 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:54.433954000 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.480770111 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:54.504533052 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:54.645961046 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.646023989 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.646064997 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.646094084 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.646126032 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:54.646131992 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.646325111 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:54.699486017 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:54.786266088 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.793934107 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:54.938110113 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:54.981004953 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:55.197941065 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:55.338047028 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:55.340867996 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:55.481883049 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:55.483176947 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:55.625559092 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:55.627223015 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:55.768594027 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:55.769537926 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:55.940599918 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:55.941596985 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:56.081958055 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:56.084464073 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:56.084712982 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:56.086075068 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:56.086263895 CET	49705	587	192.168.2.3	208.91.199.223
Nov 21, 2020 11:50:56.224912882 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:56.226118088 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:56.281492949 CET	587	49705	208.91.199.223	192.168.2.3
Nov 21, 2020 11:50:56.324687958 CET	49705	587	192.168.2.3	208.91.199.223

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 11:49:00.342525005 CET	58643	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:00.369796038 CET	53	58643	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:01.159915924 CET	60985	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:01.195913076 CET	53	60985	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:01.985521078 CET	50200	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:02.031909943 CET	53	50200	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:03.110939026 CET	51281	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:03.138370037 CET	53	51281	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:03.988863945 CET	49199	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:04.024777889 CET	53	49199	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:05.080199957 CET	50620	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:05.107399940 CET	53	50620	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:06.511970043 CET	64938	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:06.539222956 CET	53	64938	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:07.384519100 CET	60152	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:07.420312881 CET	53	60152	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:08.051018000 CET	57544	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 11:49:08.086694002 CET	53	57544	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:08.867675066 CET	55984	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:08.894915104 CET	53	55984	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:09.683259010 CET	64185	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:09.710575104 CET	53	64185	8.8.8.8	192.168.2.3
Nov 21, 2020 11:49:34.136075020 CET	65110	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:49:34.175523996 CET	53	65110	8.8.8.8	192.168.2.3
Nov 21, 2020 11:50:53.140547037 CET	58361	53	192.168.2.3	8.8.8.8
Nov 21, 2020 11:50:53.176415920 CET	53	58361	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 11:50:53.140547037 CET	192.168.2.3	8.8.8.8	0xe2aa	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 11:50:53.176415920 CET	8.8.8.8	192.168.2.3	0xe2aa	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 21, 2020 11:50:53.176415920 CET	8.8.8.8	192.168.2.3	0xe2aa	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 21, 2020 11:50:53.176415920 CET	8.8.8.8	192.168.2.3	0xe2aa	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 21, 2020 11:50:53.176415920 CET	8.8.8.8	192.168.2.3	0xe2aa	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

SMTP Packets

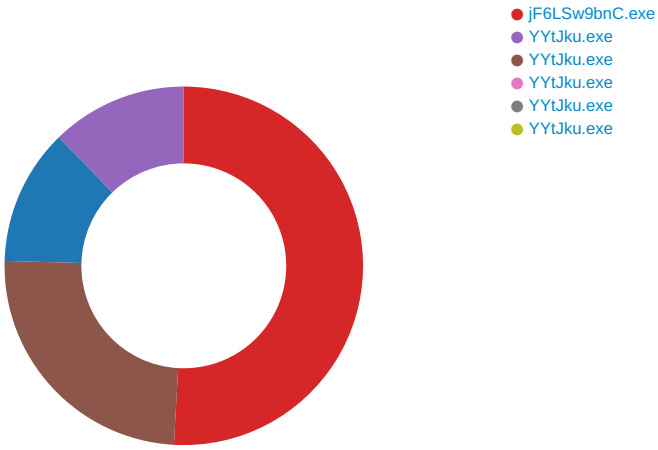
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 21, 2020 11:50:54.152650118 CET	587	49705	208.91.199.223	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 21, 2020 11:50:54.153371096 CET	49705	587	192.168.2.3	208.91.199.223	EHLO 585948
Nov 21, 2020 11:50:54.293366909 CET	587	49705	208.91.199.223	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Nov 21, 2020 11:50:54.293935061 CET	49705	587	192.168.2.3	208.91.199.223	STARTTLS
Nov 21, 2020 11:50:54.433954000 CET	587	49705	208.91.199.223	192.168.2.3	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior

● jF6LSw9bnC.exe
● jF6LSw9bnC.exe
● jF6LSw9bnC.exe



System Behavior

Analysis Process: jF6LSw9bnC.exe PID: 5864 Parent PID: 5592

General

Start time:	11:49:05
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\jF6LSw9bnC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\jF6LSw9bnC.exe'
Imagebase:	0xfe0000
File size:	618496 bytes
MD5 hash:	020BC13012CE4DB6E204CB1ED174851E
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: 00000000.00000003.212487577.0000000005CE5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.224466566.0000000005CE5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.224130542.00000000059A2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.223257236.0000000005044000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\jF6LSw9bnC.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E21C78D	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\jF6LSw9bnC.exe.log	unknown	315	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 44 72 61 77 69 6e 67 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 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 30 33 31 39 5f 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_3	success or wait	1	6E21C907	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	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile

Analysis Process: jF6LSw9bnC.exe PID: 6056 Parent PID: 5864

General

Start time:	11:49:11
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\jF6LSw9bnC.exe
Wow64 process (32bit):	false
Commandline:	jF6LSw9bnC.exe
Imagebase:	0x260000
File size:	618496 bytes
MD5 hash:	020BC13012CE4DB6E204CB1ED174851E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: jF6LSw9bnC.exe PID: 6024 Parent PID: 5864

General

Start time:	11:49:12
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\jF6LSw9bnC.exe
Wow64 process (32bit):	false
Commandline:	jF6LSw9bnC.exe
Imagebase:	0x210000
File size:	618496 bytes
MD5 hash:	020BC13012CE4DB6E204CB1ED174851E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: jF6LSw9bnC.exe PID: 5888 Parent PID: 5864

General

Start time:	11:49:12
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\jF6LSw9bnC.exe
Wow64 process (32bit):	true
Commandline:	jF6LSw9bnC.exe
Imagebase:	0xf50000
File size:	618496 bytes
MD5 hash:	020BC13012CE4DB6E204CB1ED174851E
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: 00000003.00000002.475373692.0000000003391000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.475373692.0000000003391000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.469106569.0000000000402000.00000040.00000001.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	6DF0CF06	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	6DF0CF06	unknown
C:\Users\user\AppData\Roaming\YYtJku	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD5BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CD5DD66	CopyFileW
C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD5DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe:Zone.Identifier	success or wait	1	667BA1A	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\jF6LSw9bnC.exe	C:\Users\user\AppData\Local\Temp\tmpG710.tmp	success or wait	1	667C032	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3a b0 b7 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 68 09 00 00 06 00 00 00 00 00 00 4e 87 09 00 00 20 00 00 00 a0 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 09 00 00 02 00 00 ac 54 0a 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...:.._.......... ....h..........N.... ....@.. ....T....@................	success or wait	3	6CD5DD66	CopyFileW
C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CD5DD66	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	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile

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	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\8a95f74b-deb7-4d33-9ab4-dd6c9dcc72dc	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD51B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Windows\CurrentVersion\Run	YYtJku	unicode	C:\Users\user\AppData\Roaming\ YYtJku\YYtJku.exe	success or wait	1	6CD5646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Mic rosoft\Windows\CurrentVersion\ Explorer\StartupApproved\Run	YYtJku	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CD5DE2E	RegSetValueExW

Analysis Process: YYtJku.exe PID: 5004 Parent PID: 3388

General

Start time:	11:49:46
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe'
Imagebase:	0xaf0000
File size:	618496 bytes
MD5 hash:	020BC13012CE4DB6E204CB1ED174851E
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: 0000000C.00000002.304664651.000000000117A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.307682957.0000000004B54000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.308785428.00000000056C2000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Virustotal, Browse • Detection: 48%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\YYtJku.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E21C78D	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\YYtJku.exe.log	unknown	315	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 44 72 61 77 69 6e 67 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 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 30 33 31 39 5f 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_3	success or wait	1	6E21C907	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	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile

Analysis Process: YYtJku.exe PID: 6124 Parent PID: 5004

General

Start time:	11:49:52
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
Wow64 process (32bit):	true
Commandline:	YYtJku.exe
Imagebase:	0xb30000
File size:	618496 bytes
MD5 hash:	020BC13012CE4DB6E204CB1ED174851E
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: 0000000D.00000002.474483881.0000000002F91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.474483881.0000000002F91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.469108481.0000000000402000.00000040.00000001.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	6DF0CF06	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	6DF0CF06	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	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD51B4F	ReadFile

Analysis Process: YYtJku.exe PID: 5940 Parent PID: 3388

General

Start time:	11:49:55
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe'
Imagebase:	0xbc0000
File size:	618496 bytes
MD5 hash:	020BC13012CE4DB6E204CB1ED174851E
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: 0000000E.00000002.334212460.00000000058F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.334155127.0000000005812000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.332958672.0000000004B64000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: YYtJku.exe PID: 4092 Parent PID: 5940

General

Start time:	11:50:02
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
Wow64 process (32bit):	false
Commandline:	YYtJku.exe
Imagebase:	0x230000
File size:	618496 bytes
MD5 hash:	020BC13012CE4DB6E204CB1ED174851E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: YYtJku.exe PID: 4260 Parent PID: 5940

General

Start time:	11:50:02
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
Wow64 process (32bit):	true
Commandline:	YYtJku.exe
Imagebase:	0xd90000
File size:	618496 bytes
MD5 hash:	020BC13012CE4DB6E204CB1ED174851E
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: 00000010.00000002.469149092.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.474773451.0000000003471000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.474773451.0000000003471000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis