ID: 356766
Sample Name: lNCyFjhn7M
Cookbook: default.jbs
Time: 16:19:12
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

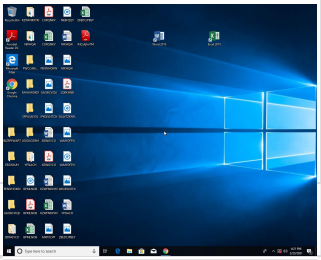
Analysis Report INCyFjhn7M

Overview

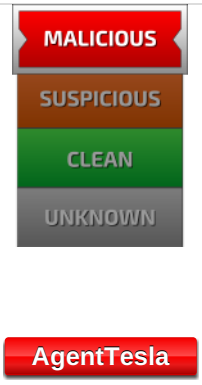
General Information

Sample Name:	INCyFjhn7M (renamed file extension from none to exe)
Analysis ID:	356766
MD5:	1ad8213451de5d..
SHA1:	62c394dfc309404..
SHA256:	152dabf84b039a8.
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection

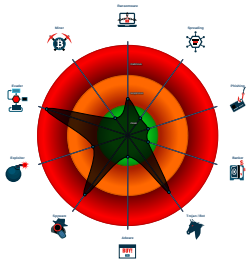


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Icon mismatch, binary includes an ic…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Found evasive API chain (trying to d…
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- INCyFjhn7M.exe (PID: 6996 cmdline: 'C:\Users\user\Desktop\INCyFjhn7M.exe' MD5: 1AD8213451DE5DAA4AD536CD9C70E9CE)
  - INCyFjhn7M.exe (PID: 7036 cmdline: C:\Users\user\Desktop\INCyFjhn7M.exe MD5: 1AD8213451DE5DAA4AD536CD9C70E9CE)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "E943pmspWkN",
  "URL: ": "https://femFzmplqt.net",
  "To: ": "",
  "ByHost: ": "mail.hybridgroupco.com:587",
  "Password: ": "RgZuUQv5z",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.326906613.0000000003C04000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.326698522.0000000002C01000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.589195869.0000000004002000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.590922380.0000000002F51000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.590922380.0000000002F51000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

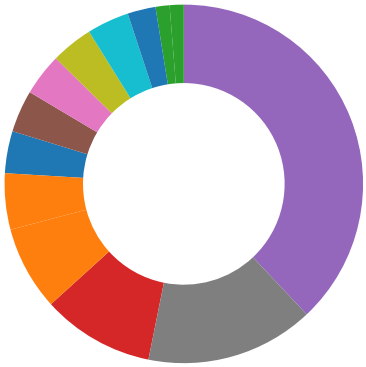
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.INCyFjhn7M.exe.3ec88a0.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.INCyFjhn7M.exe.3ec88a0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.INCyFjhn7M.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.INCyFjhn7M.exe.3d6bdd0.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.INCyFjhn7M.exe.3dc95f0.4.raw.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
- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large array initializations

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Malware Analysis System Evasion:

Yara detected AntiVM_3

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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:

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:

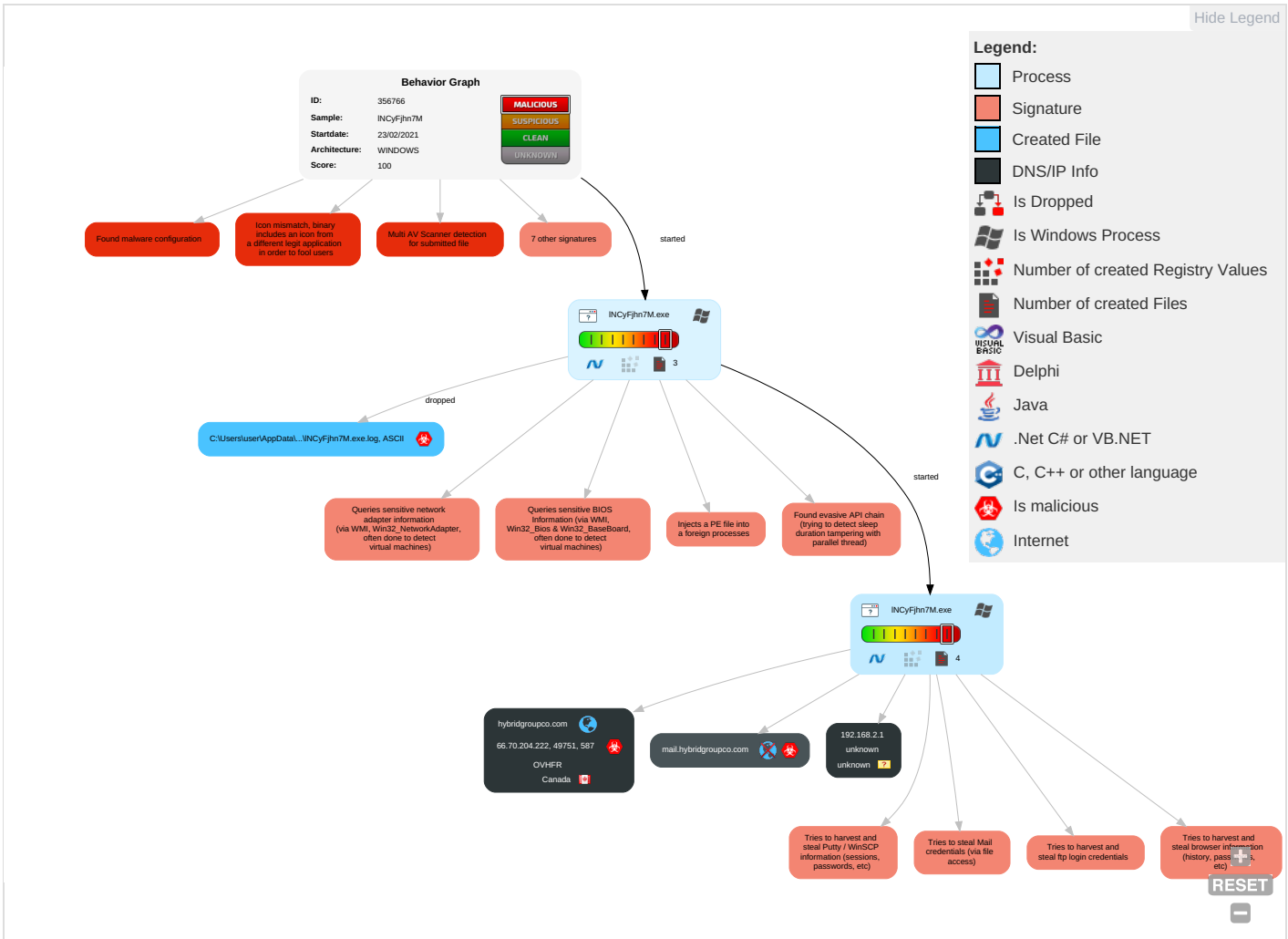
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3 1	Security Account Manager	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standarc Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Virtualization/Sandbox Evasion 1 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applicati Layer Protocc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar Control
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application La Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Us Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application La 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
INCyFjhn7M.exe	27%	Metadefender		Browse
INCyFjhn7M.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.INCyFjhn7M.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://femFzmplqt.net	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://cfWnht.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hybridgroupco.com	66.70.204.222	true	true		unknown
mail.hybridgroupco.com	unknown	unknown	true		unknown

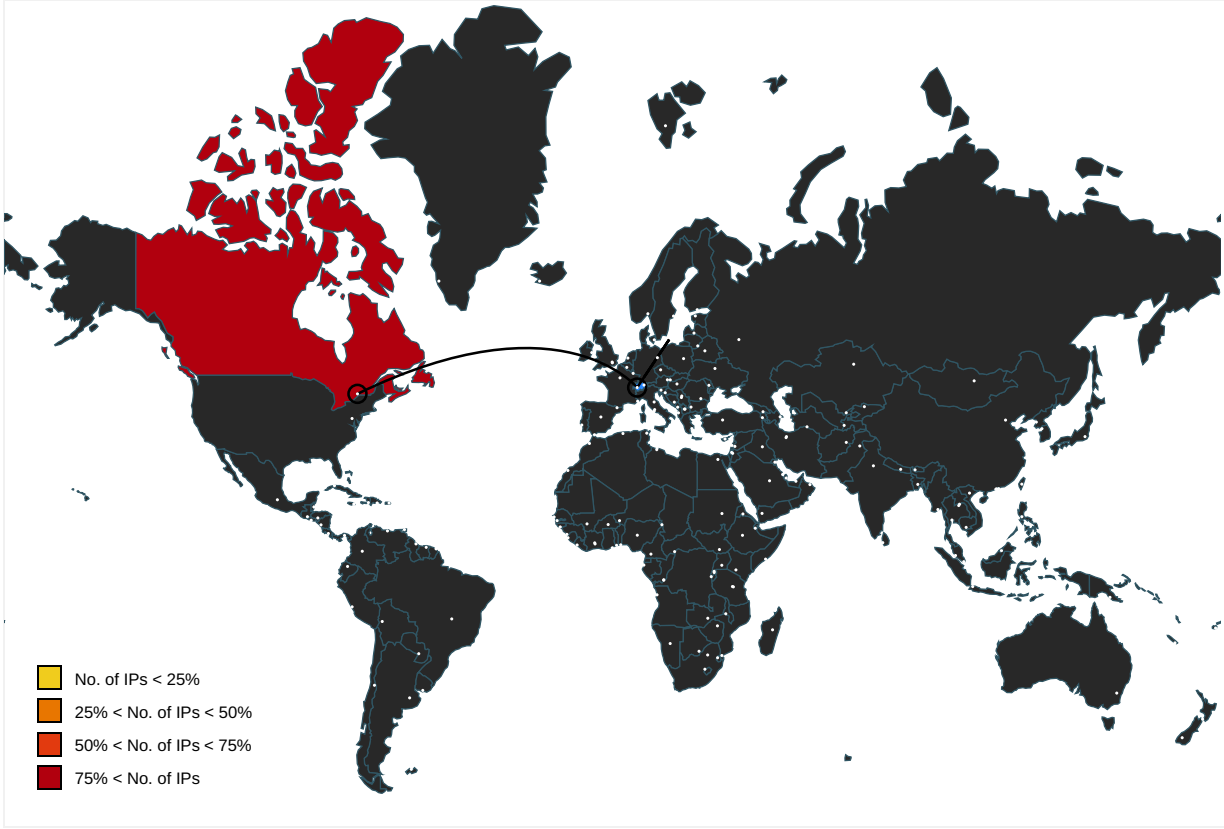
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://femFzmplqt.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	lNCyFjhn7M.exe, 00000001.00000002.590922380.0000000002F51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	lNCyFjhn7M.exe, 00000001.00000002.590922380.0000000002F51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cfWnht.com	lNCyFjhn7M.exe, 00000001.00000002.590922380.0000000002F51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	lNCyFjhn7M.exe, 00000001.00000002.590922380.0000000002F51000.00000004.00000001.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	lNCyFjhn7M.exe, 00000000.00000002.326906613.0000000003C04000.00000004.00000001.sdmp, lNCyFjhn7M.exe, 00000001.00000002.589195869.0000000000402000.00000040.00000001.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	lNCyFjhn7M.exe, 00000000.00000002.326698522.0000000002C01000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.70.204.222	unknown	Canada		16276	OVHFR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356766
Start date:	23.02.2021
Start time:	16:19:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INCyFjhn7M (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@1/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 51.104.139.180, 13.64.90.137, 40.88.32.150, 52.255.188.83, 23.211.6.115, 13.88.21.125, 8.248.131.254, 8.248.145.254, 8.248.115.254, 67.27.157.254, 67.27.157.126, 52.155.217.156, 51.103.5.159, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.104.144.132, 184.30.24.56 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-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 NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356766/sample/lNCyFjhn7M.exe

Simulations

Behavior and APIs

Time	Type	Description
16:20:00	API Interceptor	1017x Sleep call for process: lNCyFjhn7M.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.70.204.222	Purchase Order___pdf _____.exe	Get hash	malicious	Browse	
	KUmKV28Ffx.exe	Get hash	malicious	Browse	
	vWr4r97uMA.exe	Get hash	malicious	Browse	
	6UYAC8WAoJ.exe	Get hash	malicious	Browse	
	yTPzcGHfBU.exe	Get hash	malicious	Browse	
	vJsYQ8lJVIyRNtZ.exe	Get hash	malicious	Browse	
	SCAN G-0034905.EXE	Get hash	malicious	Browse	
	TT swift copy.xlsx	Get hash	malicious	Browse	
	RFQ_N0000000002.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	
	Advance import payment swift.xlsx	Get hash	malicious	Browse	
	Swift-Copy.exe	Get hash	malicious	Browse	
	6Tr3ZITOfx.exe	Get hash	malicious	Browse	
	Proforma-invoice.exe	Get hash	malicious	Browse	
	2101-0006N.exe	Get hash	malicious	Browse	
	Invoice-3990993.exe	Get hash	malicious	Browse	
	PARTS REQUEST SO_30005141.exe	Get hash	malicious	Browse	
	Yu2iMnAJBdOGPyv.exe	Get hash	malicious	Browse	
	CONTRACT AGREEMENT.exe	Get hash	malicious	Browse	
	PARTS REQUEST SO_30005141.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	Product List.exe	Get hash	malicious	Browse	• 144.217.69.193
	tEQjO7fbhJ.dll	Get hash	malicious	Browse	• 37.187.115.122
	qRoUqXAvyz.dll	Get hash	malicious	Browse	• 37.187.115.122
	v9tWEeYg4u.dll	Get hash	malicious	Browse	• 37.187.115.122
	1sAKtAszhK.dll	Get hash	malicious	Browse	• 37.187.115.122
	ClfwZpeLXt.dll	Get hash	malicious	Browse	• 37.187.115.122
	svhost.exe	Get hash	malicious	Browse	• 54.37.11.130
	SBll8nnAVc.dll	Get hash	malicious	Browse	• 37.187.115.122
	SecuriteInfo.com.Variant.Zusy.368685.25375.exe	Get hash	malicious	Browse	• 51.68.21.188
	0O9BJfVJi6fEMoS.exe	Get hash	malicious	Browse	• 94.23.162.163
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 51.68.21.186
	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• 198.27.88.111
	Quotation Reques.exe	Get hash	malicious	Browse	• 51.83.43.226
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 51.68.21.186
	iKohUejteO.dll	Get hash	malicious	Browse	• 37.187.115.122
	PO No. 104393019_pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	nTqV6fxGXT.exe	Get hash	malicious	Browse	• 51.254.175.184
	Purchase Order___pdf _____.exe	Get hash	malicious	Browse	• 66.70.204.222
	File Downloader [14.5].apk	Get hash	malicious	Browse	• 51.75.61.103
	PO_210222.exe	Get hash	malicious	Browse	• 213.186.33.5

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\INCyFjhn7M.exe.log	
Process:	C:\Users\user\Desktop\INCyFjhn7M.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.345872374885046
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:	INCyFjhn7M.exe
File size:	1058816
MD5:	1ad8213451de5daa4ad536cd9c70e9ce
SHA1:	62c394dfc3094044454f0d25775ca87e6749787e
SHA256:	152dabf84b039a8c1412d8dea323051ee96b1696c3e551a049801c8a320d23e7
SHA512:	52e7b9c4458d0629599d9153c529840fa02100e20e4045b79be9647cc535defed5b7ba58013e66b59925e55b104196331e2a5d135c9fbb942754b48d148779a
SSDEEP:	24576:oeUFmaVji138QK0okoUXWX0f0QuTACN2N8T:w5sMyAN0f0vZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...^Q3`.....P..F.....e... .....@.. .....@.....

File Icon

Icon Hash:	68c8d0f0ccccf0d6

Static PE Info

General

Entrypoint:	0x4e658e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6033515E [Mon Feb 22 06:38:22 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe653c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe8000	0x1dd0c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x106000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xe4594	0xe4600	False	0.703842321771	data	7.44014806301	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe8000	0x1dd0c	0x1de00	False	0.439788179916	data	5.78915682536	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x106000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe8220	0x918d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xf13b0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 16777215, next used block 16777215		
RT_ICON	0xf3958	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 16777215, next used block 16777215		
RT_ICON	0xf4a00	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xf4e68	0x10828	data		
RT_GROUP_ICON	0x105690	0x4c	data		
RT_GROUP_ICON	0x1056dc	0x14	data		
RT_VERSION	0x1056f0	0x42e	data		
RT_MANIFEST	0x105b20	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

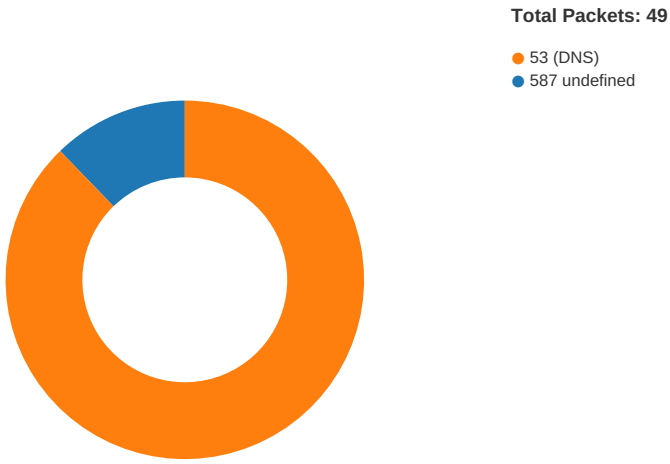
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2009 by Dan Ariely
Assembly Version	30.4.0.0
InternalName	StaticIndexRangePartitionForIList.exe
FileVersion	30.4.0.0
CompanyName	Book by Dan Ariely
LegalTrademarks	HarperCollins
Comments	HarperCollins
ProductName	Predictably Irrational
ProductVersion	30.4.0.0
FileDescription	Predictably Irrational
OriginalFilename	StaticIndexRangePartitionForIList.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:21:31.318799973 CET	49751	587	192.168.2.6	66.70.204.222
Feb 23, 2021 16:21:31.456989050 CET	587	49751	66.70.204.222	192.168.2.6
Feb 23, 2021 16:21:31.457139969 CET	49751	587	192.168.2.6	66.70.204.222
Feb 23, 2021 16:21:31.665958881 CET	49751	587	192.168.2.6	66.70.204.222
Feb 23, 2021 16:21:31.718816996 CET	587	49751	66.70.204.222	192.168.2.6
Feb 23, 2021 16:21:31.719008923 CET	49751	587	192.168.2.6	66.70.204.222
Feb 23, 2021 16:21:31.803447008 CET	587	49751	66.70.204.222	192.168.2.6
Feb 23, 2021 16:21:31.803639889 CET	49751	587	192.168.2.6	66.70.204.222
Feb 23, 2021 16:21:31.803764105 CET	587	49751	66.70.204.222	192.168.2.6
Feb 23, 2021 16:21:31.803836107 CET	49751	587	192.168.2.6	66.70.204.222

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:19:52.792135000 CET	58377	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:19:52.820775986 CET	55074	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:19:52.842531919 CET	53	58377	8.8.8.8	192.168.2.6
Feb 23, 2021 16:19:52.872036934 CET	53	55074	8.8.8.8	192.168.2.6
Feb 23, 2021 16:19:53.203574896 CET	54513	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:19:53.252281904 CET	53	54513	8.8.8.8	192.168.2.6
Feb 23, 2021 16:19:54.607425928 CET	62044	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:19:54.658279896 CET	53	62044	8.8.8.8	192.168.2.6
Feb 23, 2021 16:19:55.402612925 CET	63791	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:19:55.454396963 CET	53	63791	8.8.8.8	192.168.2.6
Feb 23, 2021 16:19:56.085376024 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:19:56.155441046 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 16:19:56.271311998 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:19:56.323894024 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 16:19:57.539115906 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:19:57.590812922 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 16:19:58.791845083 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:19:58.840635061 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:00.154516935 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:00.205974102 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:02.735378027 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:02.792649031 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:03.938746929 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:03.990463972 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:05.118819952 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:05.170947075 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:06.277662992 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:06.328031063 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:07.139245987 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:07.190906048 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:08.570271969 CET	53781	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:20:08.619371891 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:09.345731974 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:09.397114992 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:10.477902889 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:10.526721954 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:11.701636076 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:11.753155947 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:13.449300051 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:13.497988939 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:15.916193962 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:15.967675924 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:18.307005882 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:18.367248058 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:29.234811068 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:29.286530018 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:48.007652044 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:48.076380968 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:48.227662086 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:48.282083988 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:49.480954885 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:49.557606936 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:50.114592075 CET	50010	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:50.176856995 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:50.295696020 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:50.352776051 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:50.758799076 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:50.837150097 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:51.097122908 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:51.171380997 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:51.273034096 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:51.336597919 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:51.807199001 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:51.869164944 CET	53	62208	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:52.487684965 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:52.552273989 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:53.173250914 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:53.233581066 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:54.306849003 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:54.361346960 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:55.820264101 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:55.884043932 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:56.319617987 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:56.381660938 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 16:20:56.967324972 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:20:57.028439045 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 16:21:26.924931049 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:21:26.973581076 CET	53	59329	8.8.8.8	192.168.2.6
Feb 23, 2021 16:21:27.380459070 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:21:27.452419043 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 16:21:31.233412981 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:21:31.303832054 CET	53	56129	8.8.8.8	192.168.2.6
Feb 23, 2021 16:21:33.438165903 CET	58177	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:21:33.501554966 CET	53	58177	8.8.8.8	192.168.2.6
Feb 23, 2021 16:21:51.188939095 CET	50700	53	192.168.2.6	8.8.8.8
Feb 23, 2021 16:21:51.237684011 CET	53	50700	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 16:21:31.233412981 CET	192.168.2.6	8.8.8.8	0x4a25	Standard query (0)	mail.hybridgroupco.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 16:21:31.303832054 CET	8.8.8.8	192.168.2.6	0x4a25	No error (0)	mail.hybridgroupco.com	hybridgroupco.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 16:21:31.303832054 CET	8.8.8.8	192.168.2.6	0x4a25	No error (0)	hybridgroupco.com		66.70.204.222	A (IP address)	IN (0x0001)

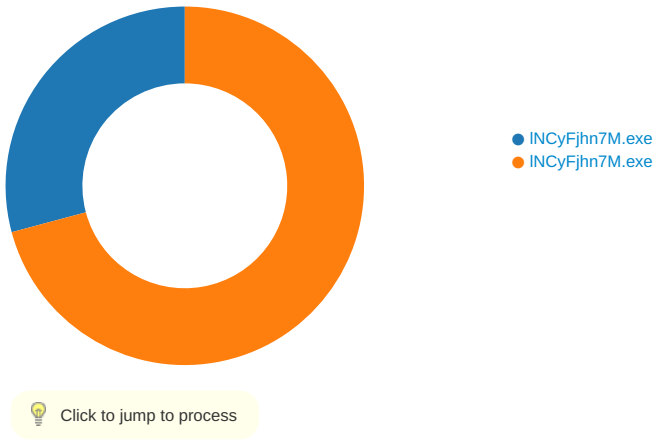
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 23, 2021 16:21:31.718816996 CET	587	49751	66.70.204.222	192.168.2.6	220-server.wlcserver.com ESMTP Exim 4.93 #2 Tue, 23 Feb 2021 19:21:31 +0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 23, 2021 16:21:31.803447008 CET	587	49751	66.70.204.222	192.168.2.6	421 server.wlcserver.com lost input connection

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: lNCyFjhn7M.exe PID: 6996 Parent PID: 6008

General

Start time:	16:19:59
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\lNCyFjhn7M.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\lNCyFjhn7M.exe'
Imagebase:	0x540000
File size:	1058816 bytes
MD5 hash:	1AD8213451DE5DAA4AD536CD9C70E9CE
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: 00000000.00000002.326906613.0000000003C04000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.326698522.0000000002C01000.00000004.00000001.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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\lNCyFjhn7M.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\lNCyFjhn7M.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: lNCyFjhn7M.exe PID: 7036 Parent PID: 6996

General

Start time:	16:20:00
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\lNCyFjhn7M.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\lNCyFjhn7M.exe
Imagebase:	0x890000
File size:	1058816 bytes
MD5 hash:	1AD8213451DE5DAA4AD536CD9C70E9CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.589195869.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.590922380.0000000002F51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.590922380.0000000002F51000.00000004.00000001.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	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5A3104F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5A3104F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5A3104F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\fc3b44d4-ba77-4541-afd7-f0aa1759ec88	unknown	4096	success or wait	1	5A3104F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5A3104F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5A3104F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5A3104F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5A3104F	ReadFile

Disassembly

Code Analysis