ID: 358290
Sample Name: inmyB8Hxr9.exe
Cookbook: default.jbs
Time: 11:41:54
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

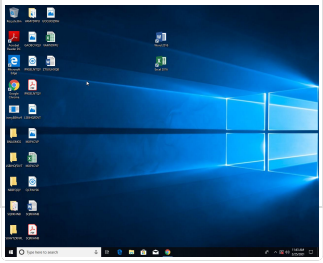
Analysis Report inmyB8Hxr9.exe

Overview

General Information

Sample Name:	inmyB8Hxr9.exe
Analysis ID:	358290
MD5:	92353a80e0debe..
SHA1:	c32c9b86699e7b..
SHA256:	2617f602bd4c119.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

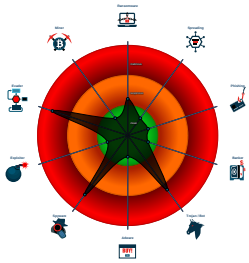
AgentTesla

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

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- .NET source code contains very larg…
- Binary contains a suspicious time st…
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- inmyB8Hxr9.exe (PID: 6176 cmdline: 'C:\Users\user\Desktop\inmyB8Hxr9.exe' MD5: 92353A80E0DEBE2E697F96A6E6BF8623)
  - inmyB8Hxr9.exe (PID: 6456 cmdline: C:\Users\user\Desktop\inmyB8Hxr9.exe MD5: 92353A80E0DEBE2E697F96A6E6BF8623)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "armyscheme@yandex.combrowse9jasmtp.yandex.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.258344568.0000000003E9 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.257896287.0000000002E9 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.488867520.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.493510413.000000000332 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: inmyB8Hxr9.exe PID: 6176	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 3 entries

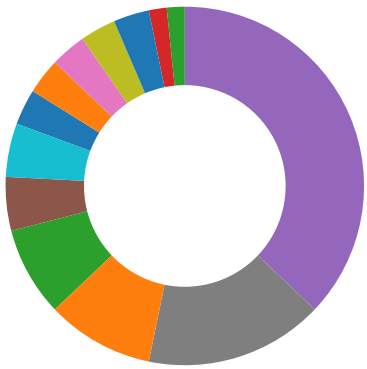
Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.inmyB8Hxr9.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.inmyB8Hxr9.exe.2ed2ce4.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.inmyB8Hxr9.exe.4150c30.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.inmyB8Hxr9.exe.4150c30.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.inmyB8Hxr9.exe.3ff6960.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Compliance:

Uses 32bit PE files

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

System Summary:

.NET source code contains very large array initializations

.NET source code contains very large strings

Data Obfuscation:

Binary contains a suspicious time stamp

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

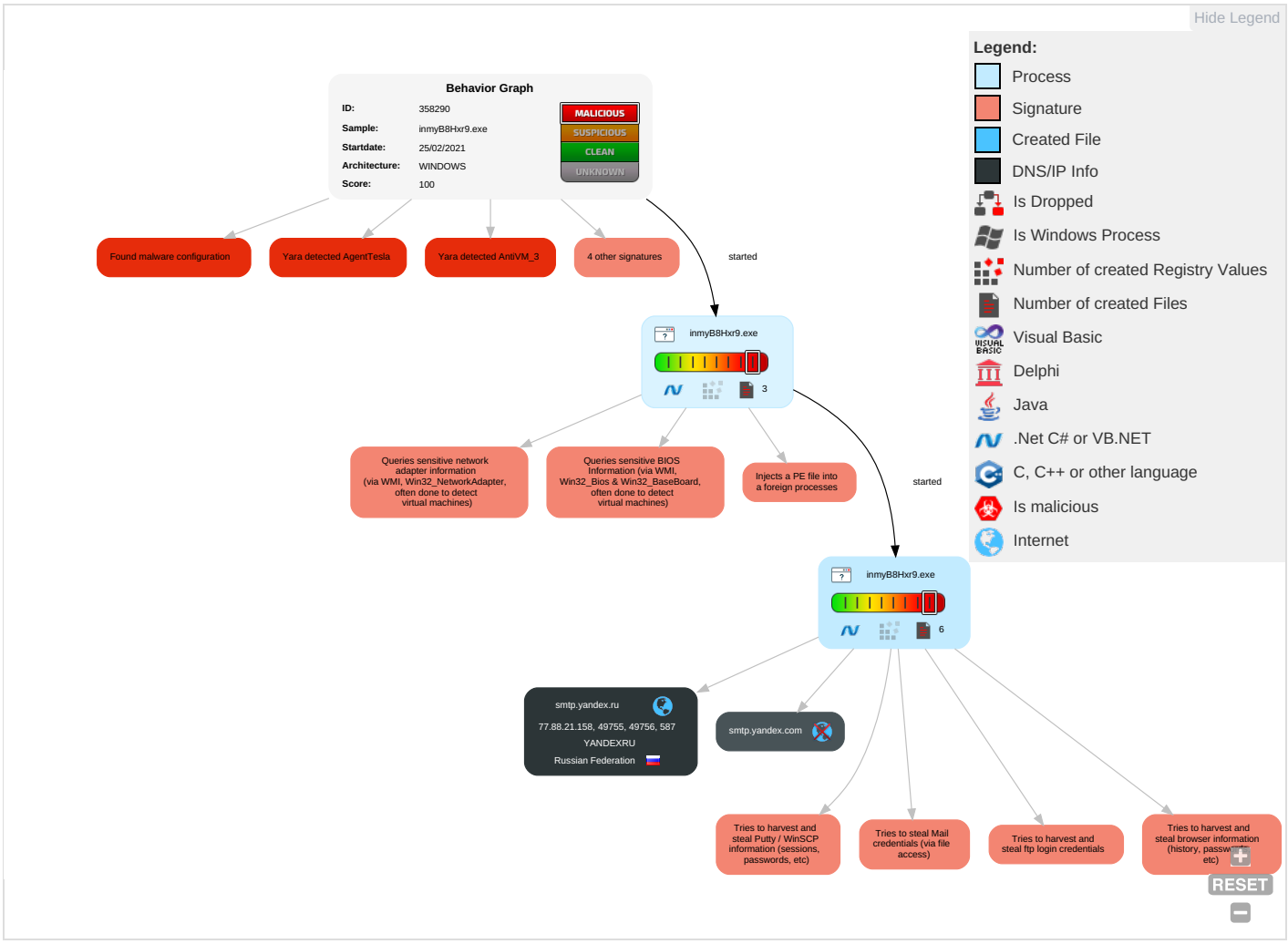
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

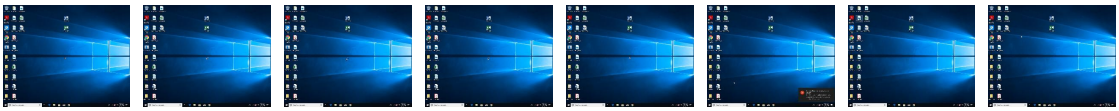
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.inmyB8Hxr9.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://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	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://api.ipify.org%or	0%	Avira URL Cloud	safe	
http://subca.ocsp	0%	Avira URL Cloud	safe	
http://www.urwpp.deras	0%	Avira URL Cloud	safe	
http://https://MT1MZ9ctOV.com	0%	Avira URL Cloud	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://www.tiro.comL	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://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	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://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.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.sajatypeworks.comR	0%	Avira URL Cloud	safe	
http://www.urwpp.deoi	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fonts.com$T	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.founder.com.cn/cna	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.founder.com.cn/cnn-u	0%	Avira URL Cloud	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://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	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	

Source	Detection	Scanner	Label	Link
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	
http://www.sajatypeworks.comnog	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/icro	0%	Avira URL Cloud	safe	
http://tempuri.org/NorthWindAzureForInsertsDataSet.xsd	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://tTAnFc.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/T	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/p	0%	Avira URL Cloud	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/B	0%	Avira URL Cloud	safe	
http://www.tiro.com~	0%	Avira URL Cloud	safe	
http://www.urwpp.deE	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	inmyB8Hxr9.exe, 00000005.00000002.493510413.0000000003321000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%or	inmyB8Hxr9.exe, 00000005.00000002.493510413.0000000003321000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://subca.ocsp	inmyB8Hxr9.exe, 00000005.00000002.499410701.0000000006F10000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

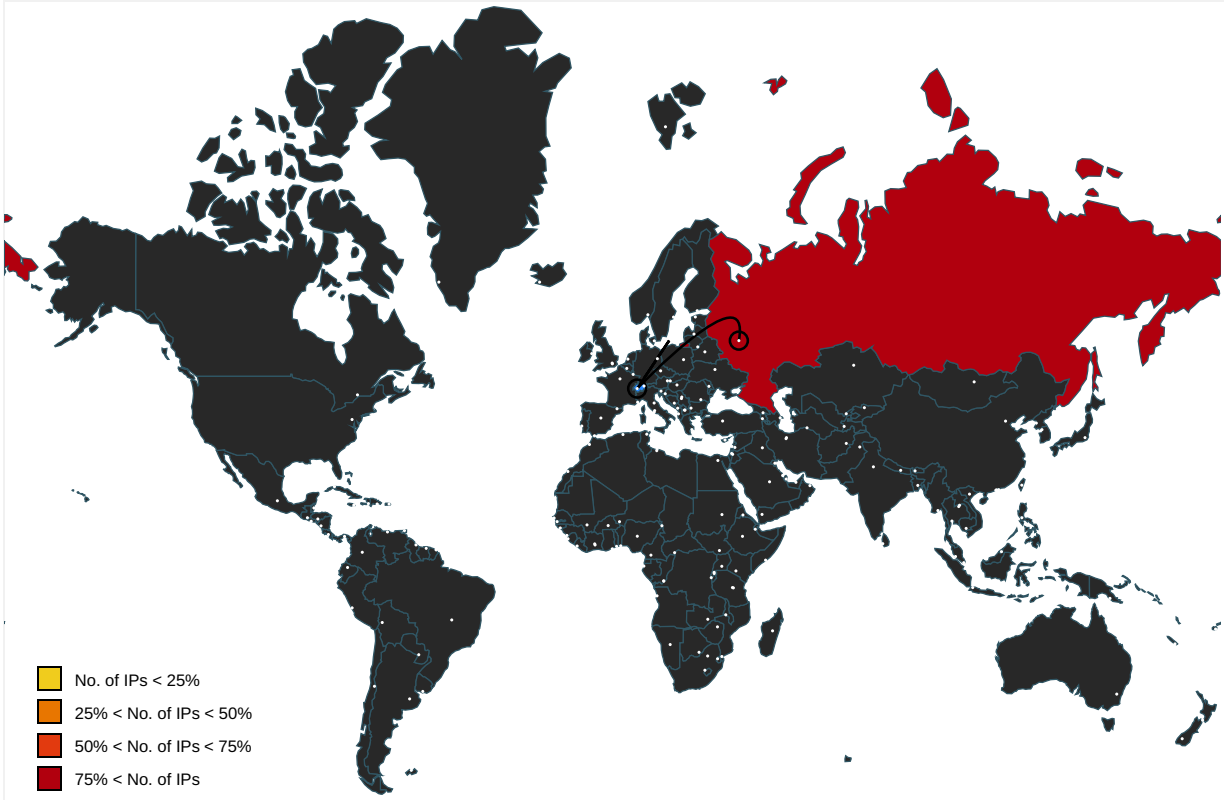
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false		high
http://yandex.crl.certum.pl/ycasha2.crl0q	inmyB8Hxr9.exe, 00000005.00000002.492268429.0000000001693000.00000004.00000020.sdmp	false		high
http://www.urwpp.deras	inmyB8Hxr9.exe, 00000000.00000003.235925261.00000000061AF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://MT1MZ9ctOV.com	inmyB8Hxr9.exe, 00000005.00000002.493510413.0000000003321000.00000004.00000001.sdmp, inmyB8Hxr9.exe, 00000005.00000002.495917462.00000000035F9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comL	inmyB8Hxr9.exe, 00000000.00000003.233032175.00000000061AB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp, inmyB8Hxr9.exe, 00000000.00000003.239051427.0000000006196000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	inmyB8Hxr9.exe, 00000000.00000002.257896287.0000000002E91000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp, inmyB8Hxr9.exe, 00000000.00000003.228044355.000000000123D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://subca.ocsp-certum.com0.	inmyB8Hxr9.exe, 00000005.00000002.492268429.0000000001693000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/9	inmyB8Hxr9.exe, 00000000.00000003.233383073.0000000006196000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ca.cer09	inmyB8Hxr9.exe, 00000005.00000002.492268429.0000000001693000.00000004.00000020.sdmp	false		high
http://www.founder.com.cn/cn/cThe	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp, inmyB8Hxr9.exe, 00000000.00000003.228876956.00000000061CD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlH	inmyB8Hxr9.exe, 00000000.00000003.237383973.00000000061A2000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/8	inmyB8Hxr9.exe, 00000000.00000003.233581560.0000000006196000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comR	inmyB8Hxr9.exe, 00000000.00000003.228044355.000000000123D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deoi	inmyB8Hxr9.exe, 00000000.00000003.235852868.00000000061AF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	inmyB8Hxr9.exe, 00000005.00000002.499445380.0000000006F36000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com$T	inmyB8Hxr9.exe, 00000000.00000003.228450601.00000000061CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cna	inmyB8Hxr9.exe, 00000000.00000003.230938048.00000000061A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	inmyB8Hxr9.exe, 00000005.00000002.493510413.0000000003321000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.founder.com.cn/cnn-u	inmyB8Hxr9.exe, 00000000.00000003.230580473.0000000006193000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp, inmyB8Hxr9.exe, 00000000.00000003.228342810.00000000061CD000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	inmyB8Hxr9.exe, 00000000.00000003.235925261.00000000061AF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	inmyB8Hxr9.exe, 00000000.00000002.257896287.0000000002E91000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/#	inmyB8Hxr9.exe, 00000000.00000003.236276224.00000000061AF000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.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	inmyB8Hxr9.exe, 00000000.00000002.258344568.0000000003E91000.00000004.00000001.sdmp, inmyB8Hxr9.exe, 00000005.00000002.488867520.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certum.pl/CPS0	inmyB8Hxr9.exe, 00000005.00000002.499445380.0000000006F36000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.comnog	inmyB8Hxr9.exe, 00000000.00000003.228044355.000000000123D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/icro	inmyB8Hxr9.exe, 00000000.00000003.233698671.0000000006196000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/NorthWindAzureForInsertsDataSet.xsd	inmyB8Hxr9.exe	false	• Avira URL Cloud: safe	unknown
http://repository.certum.pl/ycasha2.cer0	inmyB8Hxr9.exe, 00000005.00000002.492268429.0000000001693000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	inmyB8Hxr9.exe, 00000000.00000002.263525691.0000000006190000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	inmyB8Hxr9.exe, 00000005.00000002.493510413.0000000003321000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://tTAnFc.com	inmyB8Hxr9.exe, 00000005.00000002.493510413.0000000003321000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF	inmyB8Hxr9.exe, 00000000.00000003.239051427.0000000006196000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ctnca.cer09	inmyB8Hxr9.exe, 00000005.00000002.499445380.0000000006F36000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/T	inmyB8Hxr9.exe, 00000000.00000003.233698671.0000000006196000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	inmyB8Hxr9.exe, 00000005.00000002.493510413.0000000003321000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.certum.pl/ctnca.crl0k	inmyB8Hxr9.exe, 00000005.00000002.499445380.0000000006F36000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/p	inmyB8Hxr9.exe, 00000000.00000003.233698671.0000000006196000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comlic	inmyB8Hxr9.exe, 00000000.00000003.233076818.00000000061AB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certum.pl/CPS0	inmyB8Hxr9.exe, 00000005.00000002.492268429.0000000001693000.00000004.00000020.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/	inmyB8Hxr9.exe, 00000000.00000003.233698671.0000000006196000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/B	inmyB8Hxr9.exe, 00000000.00000003.233698671.0000000006196000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://smtp.yandex.com	inmyB8Hxr9.exe, 00000005.00000002.495653968.00000000035D6000.00000004.00000001.sdmp	false		high
http://www.tiro.com~	inmyB8Hxr9.exe, 00000000.00000003.233076818.00000000061AB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deE	inmyB8Hxr9.exe, 00000000.00000003.235925261.00000000061AF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://yandex.ocsp-responder.com03	inmyB8Hxr9.exe, 00000005.00000002.492268429.0000000001693000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false		high
http://crls.yandex.net/certum/ycasha2.crl0-	inmyB8Hxr9.exe, 00000005.00000002.492268429.0000000001693000.00000004.00000020.sdmp	false		high
http://www.founder.com.cn/cn3	inmyB8Hxr9.exe, 00000000.00000003.230314823.0000000006193000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	inmyB8Hxr9.exe, 00000000.00000003.233894474.0000000006196000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnft	inmyB8Hxr9.exe, 00000000.00000003.230580473.0000000006193000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	inmyB8Hxr9.exe, 00000000.00000003.239051427.0000000006196000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	inmyB8Hxr9.exe, 00000000.00000002.263693385.0000000006280000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comitu	inmyB8Hxr9.exe, 00000000.00000003.239051427.0000000006196000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comals	inmyB8Hxr9.exe, 00000000.00000003.239051427.0000000006196000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.certum.pl/ca.crl0h	inmyB8Hxr9.exe, 00000005.00000002.492268429.0000000001693000.00000004.00000020.sdmp	false		high
http://www.sajatypeworks.com#	inmyB8Hxr9.exe, 00000000.00000003.228044355.000000000123D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnYaHf	inmyB8Hxr9.exe, 00000000.00000003.231091128.00000000061A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	unknown	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358290
Start date:	25.02.2021
Start time:	11:41:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	inmyB8Hxr9.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/2@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 17.5% • Quality standard deviation: 32.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 51.104.139.180, 204.79.197.200, 13.107.21.200, 104.42.151.234, 23.211.6.115, 184.30.20.56, 52.255.188.83, 51.11.168.160, 52.147.198.201, 92.122.213.194, 92.122.213.247, 67.26.73.254, 8.248.143.254, 8.253.95.249, 8.253.95.120, 67.26.83.254, 51.103.5.186, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:42:55	API Interceptor	714x Sleep call for process: inmyB8Hxr9.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.88.21.158	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	
	KBU0o30E6s.exe	Get hash	malicious	Browse	
	FspMzSMtYA.exe	Get hash	malicious	Browse	
	w0dAcJpIm1.exe	Get hash	malicious	Browse	
	VfUlDo471c.exe	Get hash	malicious	Browse	
	FEB PROCESSED.xlsx	Get hash	malicious	Browse	
	q13a8EbUPB.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe	Get hash	malicious	Browse	
	PO Contract -SCPL0882021 & sales contract ZD.1.190 22021_PDF.exe	Get hash	malicious	Browse	
	pass.exe	Get hash	malicious	Browse	
	nXKdiUgIYy.exe	Get hash	malicious	Browse	
	x4cXV3784J.exe	Get hash	malicious	Browse	
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	
	emI0MqOvFw.exe	Get hash	malicious	Browse	
	ZnsXrCAriL.exe	Get hash	malicious	Browse	
	zyp9gbDQHw.exe	Get hash	malicious	Browse	
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	
	MI3eskSuv2.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.yandex.ru	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	• 77.88.21.158
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	• 77.88.21.158
	KBU0o30E6s.exe	Get hash	malicious	Browse	• 77.88.21.158
	FspMzSMtYA.exe	Get hash	malicious	Browse	• 77.88.21.158
	w0dAcJpIm1.exe	Get hash	malicious	Browse	• 77.88.21.158
	VfUlDo471c.exe	Get hash	malicious	Browse	• 77.88.21.158
	FEB PROCESSED.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	q13a8EbUPB.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO Contract -SCPL0882021 & sales contract ZD.1.190 22021_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	pass.exe	Get hash	malicious	Browse	• 77.88.21.158
	nXKdiUgIYy.exe	Get hash	malicious	Browse	• 77.88.21.158
	x4cXV3784J.exe	Get hash	malicious	Browse	• 77.88.21.158
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	emI0MqOvFw.exe	Get hash	malicious	Browse	• 77.88.21.158
	ZnsXrCAriL.exe	Get hash	malicious	Browse	• 77.88.21.158
	zyp9gbDQHw.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	MI3eskSuv2.exe	Get hash	malicious	Browse	• 77.88.21.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YANDEXRU	rtofwqxq.exe	Get hash	malicious	Browse	• 87.250.250.22
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	• 77.88.21.158
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	• 77.88.21.158
	KBU0o30E6s.exe	Get hash	malicious	Browse	• 77.88.21.158
	FspMzSMtYA.exe	Get hash	malicious	Browse	• 77.88.21.158

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Wd8LBdddKD.exe	Get hash	malicious	Browse	• 37.9.96.19
	Wd8LBdddKD.exe	Get hash	malicious	Browse	• 37.9.96.14
	w0dAcJpIm1.exe	Get hash	malicious	Browse	• 77.88.21.158
	VfUlDo471c.exe	Get hash	malicious	Browse	• 77.88.21.158
	FEB PROCESSED.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	q13a8EbUPB.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO Contract -SCPL0882021 & sales contract ZD.1.190 22021_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	pass.exe	Get hash	malicious	Browse	• 77.88.21.158
	nXKdiUgIYy.exe	Get hash	malicious	Browse	• 77.88.21.158
	x4cXV3784J.exe	Get hash	malicious	Browse	• 77.88.21.158
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	emI0MqOvFw.exe	Get hash	malicious	Browse	• 77.88.21.158
	ZnsXrCAriL.exe	Get hash	malicious	Browse	• 77.88.21.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\inmyB8Hxr9.exe.log	
Process:	C:\Users\user\Desktop\inmyB8Hxr9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.336334182031907
Encrypted:	false
SSDEEP:	48:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHsAmHK2HKSHKKHKs:lrq5qXEwCYqhQnoPtlxHeqzNM/q2qSqY
MD5:	B9E8D9BC061D6715808BB3A28CECBA2B
SHA1:	6F18CD63C12AEC962D089F215658FD5BE1789BC3
SHA-256:	716E082F23E093EBCA2C8F994745CC7D62457D7359BBE555B75E275CE8EEEDC7
SHA-512:	6D97D3E34CBCC5C0CCF845E285F98DE1824A825AB1D306D20ED164B0B74270CED9AB694E40831EC796E9F823BB4E369166006E555D7BBD000A33A0FDA601F86
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\bmtbedok.fh2\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\inmyB8Hxr9.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6969296358976265
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBo2+tYeF+X:T5LLOpEO5J/Kn7U1uBo2UYeQ
MD5:	A9DBC7B8E523ABE3B02D77DBF2FCD645
SHA1:	DF5EE16ECF4B3B02E312F935AE81D4C5D2E91CA8
SHA-256:	39B4E45A062DEA6F541C18FA1A15C5C0DB43A59673A26E2EB5B8A4345EE767AE
SHA-512:	3CF87455263E395313E779D4F440D8405D86244E04B5F577BB9FA2F4A2069DE019D340F6B2F6EF420DEE3D3DEEFD4B58DA3FCA3BB802DE348E1A810D6379CCB
Malicious:	false

C:\Users\user\AppData\Roaming\bmtbedok.fh2\Chrome\Default\Cookies

Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.646038972317263
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	inmyB8Hxr9.exe
File size:	471552
MD5:	92353a80e0debe2e697f96a6e6bf8623
SHA1:	c32c9b86699e7bd40b613b86136ce3101dbc1cfa
SHA256:	2617f602bd4c11985c40f6987daa563241cc8deb402fb895952c8a73102caad5
SHA512:	a6e941ce3b38c31a6b708b75d2645daa2b70c0404402ca99562b609c217f505864e9e1148f38ca26ef755c8ce3aa4e5ea05801c88c1a144cfda767935e0a9758
SSDEEP:	6144:tWAyFAvZUtFPysCWk9BMWnb4cVeZZjaNsUQZQ5r0Kw1tdgls/CVIgcw:t9vaFDCWinZYDaNPyqcmgCVI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z.o.....P..(.....bF... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x474662
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:	0x936FA27A [Wed May 20 05:54:02 2048 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74610	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x76000	0x5ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x78000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x745f4	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	0x72668	0x72800	False	0.828368074509	data	7.65934034445	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x5ec	0x600	False	0.434895833333	data	4.2233743472	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x76090	0x35c	data		
RT_MANIFEST	0x763fc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

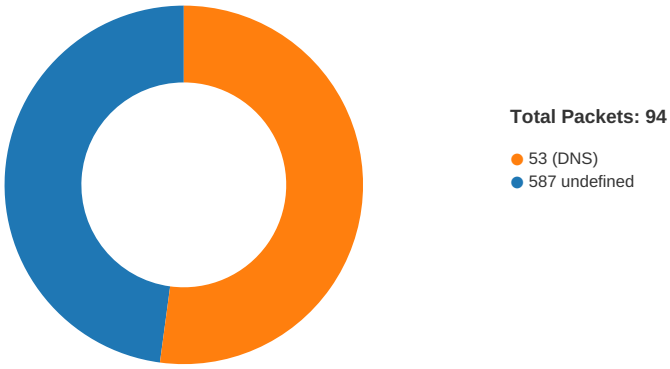
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020 - 2021
Assembly Version	6.4.0.2
InternalName	RemotingException.exe
FileVersion	6.4.0.2
CompanyName	
LegalTrademarks	
Comments	
ProductName	Table Adapter
ProductVersion	6.4.0.2
FileDescription	Table Adapter
OriginalFilename	RemotingException.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:44:34.046395063 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:34.125173092 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.127857924 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:34.350579977 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.351052999 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:34.429783106 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.429825068 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.430308104 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:34.508950949 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.562391996 CET	49755	587	192.168.2.7	77.88.21.158

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:44:34.563309908 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:34.642993927 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.643043995 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.643062115 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.643075943 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.643291950 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:34.684010983 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:34.763072014 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.812367916 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:34.850516081 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:34.929224014 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:34.932694912 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:35.011464119 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:35.015842915 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:35.107203007 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:35.108191967 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:35.194267035 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:35.194888115 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:35.278779030 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:35.279474020 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:35.358289957 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:35.362770081 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:35.362977028 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:35.363086939 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:35.363194942 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:35.441519976 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:35.441700935 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:35.933480978 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:35.984292030 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.262196064 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.341094971 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.341125965 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.341344118 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.358294010 CET	49755	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.359647989 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.436418056 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.436630964 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.436882973 CET	587	49755	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.672813892 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.673166990 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.749855042 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.749901056 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.750427008 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.827478886 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.828208923 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.906649113 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.906694889 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.906724930 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.906744003 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.907273054 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.911943913 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:37.989012957 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:37.991524935 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.068325996 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.069495916 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.146559954 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.147315979 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.264954090 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.431253910 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.431829929 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.508644104 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.516283989 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.516767025 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.596788883 CET	587	49756	77.88.21.158	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:44:38.597311974 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.678741932 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.681421041 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.681723118 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.681936979 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.682125092 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.682379007 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.682642937 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.682818890 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.682925940 CET	49756	587	192.168.2.7	77.88.21.158
Feb 25, 2021 11:44:38.759532928 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.759665966 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.759701014 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.759718895 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:38.800888062 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:39.391064882 CET	587	49756	77.88.21.158	192.168.2.7
Feb 25, 2021 11:44:39.437783957 CET	49756	587	192.168.2.7	77.88.21.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:42:32.427639008 CET	56590	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:32.468344927 CET	60501	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:32.476778030 CET	53	56590	8.8.8.8	192.168.2.7
Feb 25, 2021 11:42:32.519934893 CET	53	60501	8.8.8.8	192.168.2.7
Feb 25, 2021 11:42:33.195080042 CET	53775	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:33.253907919 CET	53	53775	8.8.8.8	192.168.2.7
Feb 25, 2021 11:42:34.428811073 CET	51837	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:34.480299950 CET	53	51837	8.8.8.8	192.168.2.7
Feb 25, 2021 11:42:35.619589090 CET	55411	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:35.671304941 CET	53	55411	8.8.8.8	192.168.2.7
Feb 25, 2021 11:42:36.585953951 CET	63668	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:36.644691944 CET	53	63668	8.8.8.8	192.168.2.7
Feb 25, 2021 11:42:36.846215010 CET	54640	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:36.899503946 CET	53	54640	8.8.8.8	192.168.2.7
Feb 25, 2021 11:42:38.043723106 CET	58739	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:38.094341993 CET	53	58739	8.8.8.8	192.168.2.7
Feb 25, 2021 11:42:39.541865110 CET	60338	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:39.590574980 CET	53	60338	8.8.8.8	192.168.2.7
Feb 25, 2021 11:42:41.001439095 CET	58717	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:41.061307907 CET	53	58717	8.8.8.8	192.168.2.7
Feb 25, 2021 11:42:42.243355989 CET	59762	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:42:42.291981936 CET	53	59762	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:01.412602901 CET	54329	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:01.471852064 CET	53	54329	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:16.114504099 CET	58052	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:16.163260937 CET	53	58052	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:17.442075014 CET	54008	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:17.471110106 CET	59451	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:17.499337912 CET	53	54008	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:17.519926071 CET	53	59451	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:18.251144886 CET	52914	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:18.303877115 CET	53	52914	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:19.420806885 CET	64569	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:19.471337080 CET	53	64569	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:20.257886887 CET	52816	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:20.312728882 CET	53	52816	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:21.417933941 CET	50781	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:21.468277931 CET	53	50781	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:22.592530012 CET	54230	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:22.641251087 CET	53	54230	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:23.429610968 CET	54911	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:23.478418112 CET	53	54911	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:24.269021988 CET	49958	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:43:24.317871094 CET	53	49958	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:24.842926979 CET	50860	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:24.904547930 CET	53	50860	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:25.099401951 CET	50452	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:25.148288012 CET	53	50452	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:26.331104040 CET	59730	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:26.388473034 CET	53	59730	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:27.255508900 CET	59310	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:27.310013056 CET	53	59310	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:27.970890045 CET	51919	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:28.019889116 CET	53	51919	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:28.124042034 CET	64296	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:28.172827959 CET	53	64296	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:28.202331066 CET	56680	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:28.251082897 CET	53	56680	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:29.264763117 CET	58820	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:29.313488007 CET	53	58820	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:35.879561901 CET	60983	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:35.938563108 CET	53	60983	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:45.902324915 CET	49247	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:45.959479094 CET	53	49247	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:46.589550018 CET	52286	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:46.653069019 CET	53	52286	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:47.336214066 CET	56064	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:47.394696951 CET	53	56064	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:47.898294926 CET	63744	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:47.960324049 CET	53	63744	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:48.491719961 CET	61457	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:48.551793098 CET	53	61457	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:48.572540045 CET	58367	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:48.644999027 CET	53	58367	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:49.100601912 CET	60599	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:49.160178900 CET	53	60599	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:49.368459940 CET	59571	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:49.863250017 CET	52689	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:49.923577070 CET	53	52689	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:50.374083996 CET	59571	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:50.434259892 CET	53	59571	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:51.513500929 CET	50290	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:51.575829029 CET	53	50290	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:52.486165047 CET	60427	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:52.545607090 CET	53	60427	8.8.8.8	192.168.2.7
Feb 25, 2021 11:43:53.005680084 CET	56209	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:43:53.066025972 CET	53	56209	8.8.8.8	192.168.2.7
Feb 25, 2021 11:44:11.447969913 CET	59582	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:44:11.522476912 CET	53	59582	8.8.8.8	192.168.2.7
Feb 25, 2021 11:44:14.721700907 CET	60949	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:44:14.770591021 CET	53	60949	8.8.8.8	192.168.2.7
Feb 25, 2021 11:44:32.821062088 CET	58542	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:44:32.872997999 CET	53	58542	8.8.8.8	192.168.2.7
Feb 25, 2021 11:44:33.821827888 CET	59179	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:44:33.881989956 CET	53	59179	8.8.8.8	192.168.2.7
Feb 25, 2021 11:44:33.966233015 CET	60927	53	192.168.2.7	8.8.8.8
Feb 25, 2021 11:44:34.023236990 CET	53	60927	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 11:44:33.821827888 CET	192.168.2.7	8.8.8.8	0xb513	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Feb 25, 2021 11:44:33.966233015 CET	192.168.2.7	8.8.8.8	0xc334	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 11:44:33.881989956 CET	8.8.8.8	192.168.2.7	0xb513	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:44:33.881989956 CET	8.8.8.8	192.168.2.7	0xb513	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Feb 25, 2021 11:44:34.023236990 CET	8.8.8.8	192.168.2.7	0xc334	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:44:34.023236990 CET	8.8.8.8	192.168.2.7	0xc334	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

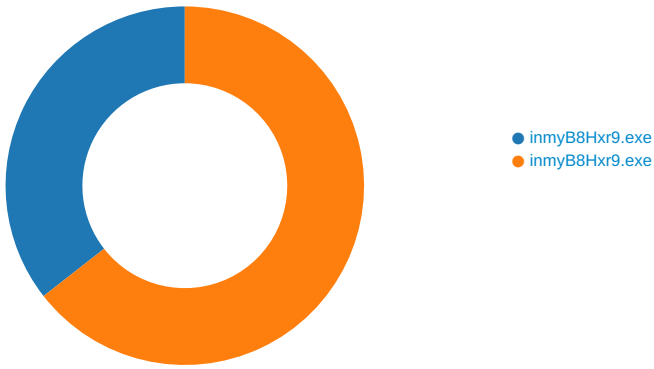
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 11:44:34.350579977 CET	587	49755	77.88.21.158	192.168.2.7	220 vla3-3dd1bd6927b2.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Feb 25, 2021 11:44:34.351052999 CET	49755	587	192.168.2.7	77.88.21.158	EHLO 609290
Feb 25, 2021 11:44:34.429825068 CET	587	49755	77.88.21.158	192.168.2.7	250-vla3-3dd1bd6927b2.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Feb 25, 2021 11:44:34.430308104 CET	49755	587	192.168.2.7	77.88.21.158	STARTTLS
Feb 25, 2021 11:44:34.508950949 CET	587	49755	77.88.21.158	192.168.2.7	220 Go ahead
Feb 25, 2021 11:44:37.672813892 CET	587	49756	77.88.21.158	192.168.2.7	220 iva6-2d18925256a6.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Feb 25, 2021 11:44:37.673166990 CET	49756	587	192.168.2.7	77.88.21.158	EHLO 609290
Feb 25, 2021 11:44:37.749901056 CET	587	49756	77.88.21.158	192.168.2.7	250-iva6-2d18925256a6.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Feb 25, 2021 11:44:37.750427008 CET	49756	587	192.168.2.7	77.88.21.158	STARTTLS
Feb 25, 2021 11:44:37.827478886 CET	587	49756	77.88.21.158	192.168.2.7	220 Go ahead

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: inmyB8Hxr9.exe PID: 6176 Parent PID: 5664

General

Start time:	11:42:42
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\inmyB8Hxr9.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\inmyB8Hxr9.exe'
Imagebase:	0xa70000
File size:	471552 bytes
MD5 hash:	92353A80E0DEBE2E697F96A6E6BF8623
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: 00000000.00000002.258344568.0000000003E91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.257896287.0000000002E91000.00000004.00000001.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	6D3ACF06	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	6D3ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\inmyB8Hxr9.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\inmyB8Hxr9.exe.log	unknown	1594	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D6BC907	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	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D385705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D38CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1F1B4F	ReadFile

Analysis Process: inmyB8Hxr9.exe PID: 6456 Parent PID: 6176

General

Start time:	11:42:56
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\inmyB8Hxr9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\inmyB8Hxr9.exe
Imagebase:	0xf10000
File size:	471552 bytes
MD5 hash:	92353A80E0DEBE2E697F96A6E6BF8623
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: 00000005.00000002.488867520.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.493510413.0000000003321000.00000004.00000001.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	6D3ACF06	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	6D3ACF06	unknown
C:\Users\user\AppData\Roaming\bmtbedok.fh2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1FBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bmtbedok.fh2\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	6C1FBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bmtbedok.fh2\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	6C1FBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bmtbedok.fh2\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C1FDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bmtbedok.fh2\Chrome\Default\Cookies	success or wait	1	6C1F6A95	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\Roaming\bmtbedok.fh2\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C1FDD66	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	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D385705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D38CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1F1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\5e206ded-25d6-4e58-9588-6c064bd5eb95	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1F1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1F1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C1F1B4F	ReadFile
C:\Users\user\AppData\Roaming\bmtbedok.fh2\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C1F1B4F	ReadFile

Disassembly

Code Analysis

Code Analysis