ID: 383981
Sample Name: #1002021.exe
Cookbook: default.jbs
Time: 13:33:12
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

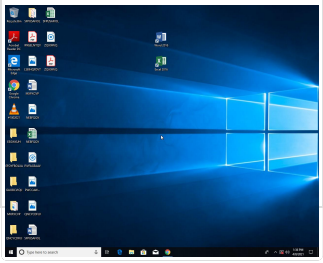
Analysis Report #1002021.exe

Overview

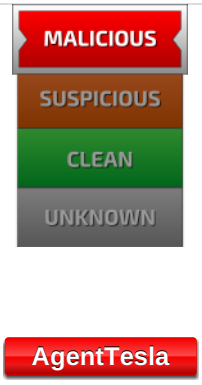
General Information

Sample Name:	#1002021.exe
Analysis ID:	383981
MD5:	6208b654193633..
SHA1:	62a31f0f710ce7a..
SHA256:	c1f2ef3f7a994ad…
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection



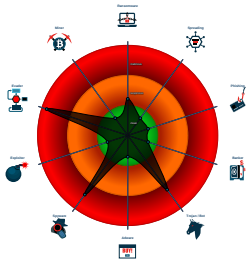
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains method …
- .NET source code contains very larg…
- .NET source code references suspic…
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- #1002021.exe (PID: 4612 cmdline: 'C:\Users\user\Desktop\#1002021.exe' MD5: 6208B6541936333F498204D1EC7234DB)
  - #1002021.exe (PID: 2672 cmdline: {path} MD5: 6208B6541936333F498204D1EC7234DB)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "ekwe@yillyenterprise.com^1.kk2[?w-Yzmail.yillyenterprise.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.497062143.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.507026512.0000000002B41000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.260493550.000000000422000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: #1002021.exe PID: 4612	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: #1002021.exe PID: 4612	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 2 entries

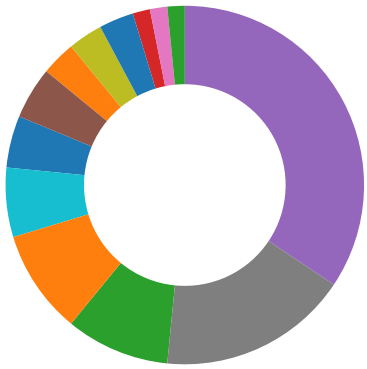
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.#1002021.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.#1002021.exe.43d9ba0.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.#1002021.exe.43d9ba0.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

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

Multi AV Scanner detection for submitted file

Networking:

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

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

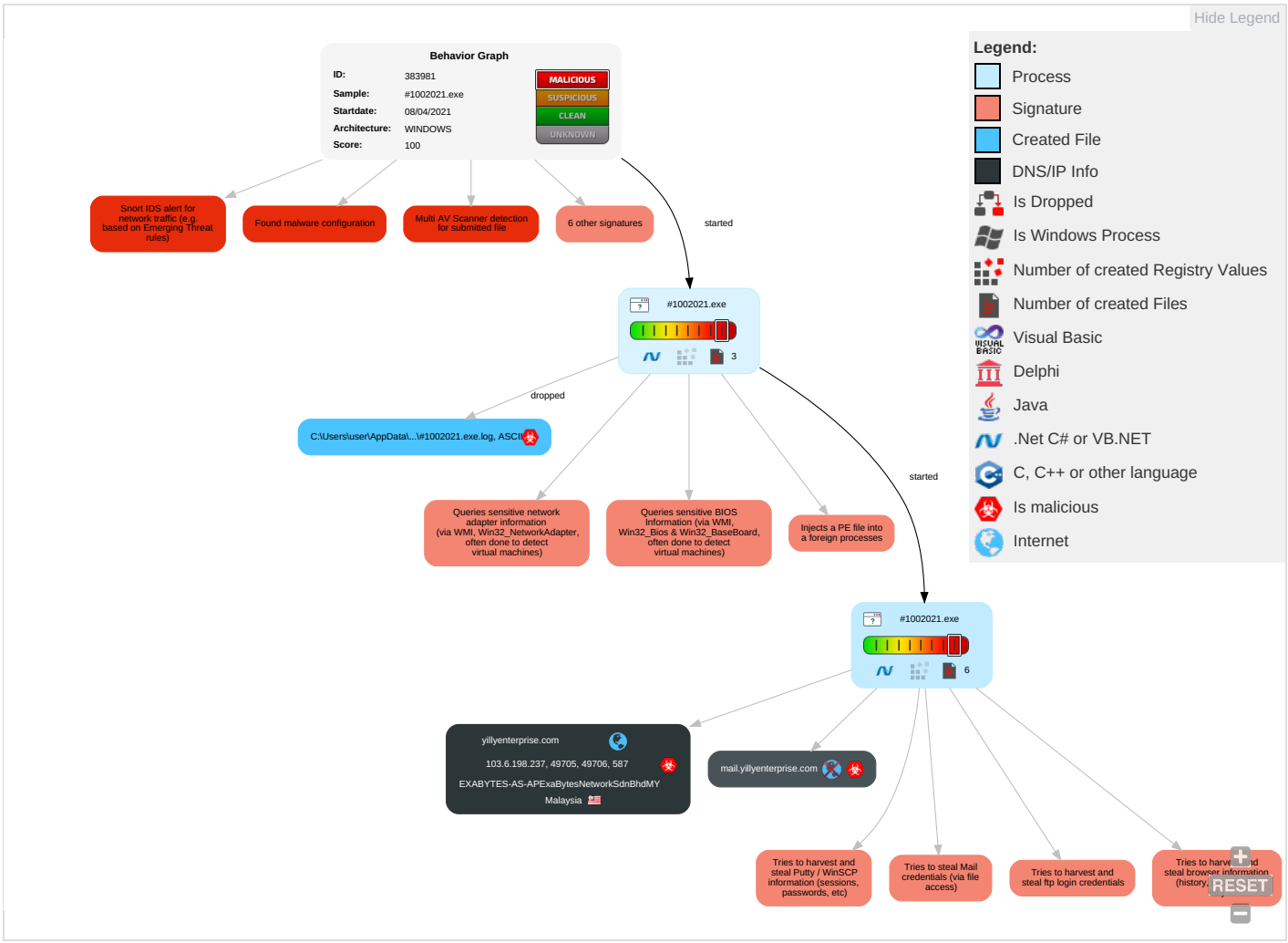
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 2 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3 1	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	Application Window Discovery 1	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	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

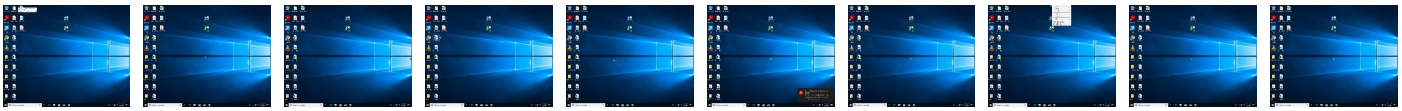
Behavior Graph



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
#1002021.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.#1002021.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
yillyenterprise.com	0%	Virustotal		Browse
mail.yillyenterprise.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-uPo	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://5TEa8DtAtM9Dv.org	0%	Avira URL Cloud	safe	
http://fontfabrik.com)x	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.zhongyicts.com.cn(ii	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnrh	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.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.comexcyx	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.carterandcone.comypo	0%	Avira URL Cloud	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.carterandcone.comB	0%	Avira URL Cloud	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.founder.com.cn/cnk	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgreta	0%	Avira URL Cloud	safe	
http://www.carterandcone.comEac	0%	Avira URL Cloud	safe	
http://www.carterandcone.comroagx	0%	Avira URL Cloud	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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.founder.com.cn/cnosoxk	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.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.sandoll.co.krF	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sandoll.co.krtp	0%	Avira URL Cloud	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	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	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://www.carterandcone.comig	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.urwpp.defl	0%	Avira URL Cloud	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.tiro.comz	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.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comct	0%	Avira URL Cloud	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
yillyenterprise.com	103.6.198.237	true	true	• 0%, Virustotal, Browse	unknown
mail.yillyenterprise.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	#1002021.exe, 00000002.00000002.507026512.0000000002B41000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	#1002021.exe, 00000000.00000002.268152409.0000000006200000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comn-uPo	#1002021.exe, 00000000.00000003.236527692.000000000612F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn-u	#1002021.exe, 00000000.00000003.236527692.000000000612F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	#1002021.exe, 00000000.00000002.268152409.0000000006200000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/michel-pi/EasyBot.Net	#1002021.exe	false		high
http://www.fontbureau.com/designers?	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false		high
http://5TEa8DtAtM9Dv.org	#1002021.exe, 00000002.0000000 2.509134848.0000000002DA9000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com)x	#1002021.exe, 00000000.0000000 3.232954091.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersX	#1002021.exe, 00000000.0000000 3.241516438.000000000612B000.0 0000004.00000001.sdmp	false		high
http://www.tiro.com	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn(ii	#1002021.exe, 00000000.0000000 3.235656212.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers	#1002021.exe, 00000000.0000000 3.247066207.000000000612B000.0 0000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnrh	#1002021.exe, 00000000.0000000 3.235268592.0000000006132000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	#1002021.exe, 00000000.0000000 3.236527692.000000000612F000.0 0000004.00000001.sdmp, #100202 1.exe, 00000000.00000003.23682 5430.000000000612F000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comexcyx	#1002021.exe, 00000000.0000000 3.236825430.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com.	#1002021.exe, 00000000.0000000 3.236527692.000000000612F000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comypo	#1002021.exe, 00000000.0000000 3.236993027.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	#1002021.exe, 00000000.0000000 3.231945776.0000000006112000.0 0000004.00000001.sdmp, #100202 1.exe, 00000000.00000002.26815 2409.0000000006200000.00000002 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comB	#1002021.exe, 00000000.0000000 3.236050979.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersh	#1002021.exe, 00000000.0000000 3.240592424.000000000612B000.0 0000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	#1002021.exe, 00000000.0000000 3.244015705.000000000612B000.0 0000004.00000001.sdmp, #100202 1.exe, 00000000.00000003.24383 2328.000000000612B000.00000004 .00000001.sdmp, #1002021.exe, 00000000.00000002.268152409.00 0000006200000.00000002.000000 01.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	#1002021.exe, 00000000.0000000 3.233010054.000000000612B000.0 0000004.00000001.sdmp, #100202 1.exe, 00000000.00000002.26815 2409.0000000006200000.00000002 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnk	#1002021.exe, 00000000.0000000 3.234673870.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comgreta	#1002021.exe, 00000000.0000000 2.259657704.00000000018D7000.0 0000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comEac	#1002021.exe, 00000000.0000000 3.236345460.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comroagx	#1002021.exe, 00000000.0000000 3.236050979.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersb	#1002021.exe, 00000000.0000000 3.241760287.000000000612B000.0 0000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	#1002021.exe, 00000000.0000000 3.238160871.0000000006132000.0 0000004.00000001.sdmp, #100202 1.exe, 00000000.00000003.23783 4875.0000000006133000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnosoxk	#1002021.exe, 00000000.0000000 3.234746931.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	#1002021.exe, 00000000.0000000 3.234231804.000000000612B000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.coma	#1002021.exe, 00000000.0000000 3.231945776.0000000006112000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krF	#1002021.exe, 00000000.0000000 3.234231804.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krtp	#1002021.exe, 00000000.0000000 3.234356458.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	#1002021.exe, 00000000.0000000 3.239769294.000000000612B000.0 0000004.00000001.sdmp, #100202 1.exe, 00000000.00000003.24206 0423.000000000612B000.00000004 .00000001.sdmp, #1002021.exe, 00000000.00000003.241903401.00 0000000006137000.00000004.000000 01.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	#1002021.exe, 00000000.0000000 3.235727969.000000000612F000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.como.	#1002021.exe, 00000000.0000000 3.236258079.000000000612F000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	#1002021.exe, 00000000.0000000 3.237834875.0000000006133000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comig	#1002021.exe, 00000000.0000000 3.236345460.000000000612F000.0 0000004.00000001.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	#1002021.exe, 00000000.0000000 2.260493550.0000000004229000.0 0000004.00000001.sdmp, #100202 1.exe, 00000002.00000002.49706 2143.0000000000402000.00000040 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.defl	#1002021.exe, 00000000.0000000 3.239769294.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coma	#1002021.exe, 00000000.0000000 3.236527692.000000000612F000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.comz	#1002021.exe, 00000000.0000000 3.235341381.00000000018DC000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	#1002021.exe, 00000002.0000000 2.507026512.0000000002B41000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmll	#1002021.exe, 00000000.0000000 3.241434699.000000000614E000.0 0000004.00000001.sdmp	false		high
http://www.carterandcone.come	#1002021.exe, 00000000.0000000 3.236527692.000000000612F000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comd	#1002021.exe, 00000000.0000000 3.236825430.000000000612F000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comct	#1002021.exe, 00000000.0000000 3.236345460.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comslnt	#1002021.exe, 00000000.0000000 3.236993027.000000000612F000.0 0000004.00000001.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	#1002021.exe, 00000002.0000000 2.507026512.0000000002B41000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cnw	#1002021.exe, 00000000.0000000 3.235656212.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/:oS	#1002021.exe, 00000000.0000000 3.234887417.0000000006132000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krm	#1002021.exe, 00000000.0000000 3.234356458.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deFyYl	#1002021.exe, 00000000.0000000 3.241903401.0000000006137000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coms	#1002021.exe, 00000000.0000000 3.236136279.000000000612F000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnhk	#1002021.exe, 00000000.0000000 3.234673870.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.krkrF	#1002021.exe, 00000000.0000000 3.234356458.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	#1002021.exe, 00000000.0000000 3.233272249.000000000612B000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	#1002021.exe, 00000000.0000000 3.236050979.000000000612F000.0 0000004.00000001.sdmp, #100202 1.exe, 00000000.00000002.26815 2409.0000000006200000.00000002 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	#1002021.exe, 00000000.0000000 3.235151202.0000000006132000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	#1002021.exe, 00000000.0000000 3.235268592.0000000006132000.0 0000004.00000001.sdmp, #100202 1.exe, 00000000.00000003.23474 6931.000000000612B000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	#1002021.exe, 00000000.0000000 3.241066365.000000000614E000.0 0000004.00000001.sdmp, #100202 1.exe, 00000000.00000003.24115 5918.000000000612B000.00000004 .00000001.sdmp, #1002021.exe, 00000000.00000002.268152409.00 00000006200000.00000002.000000 01.sdmp	false		high
http://www.carterandcone.comhly	#1002021.exe, 00000000.0000000 3.236825430.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cna	#1002021.exe, 00000000.0000000 3.235656212.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlP	#1002021.exe, 00000000.0000000 3.241881177.000000000614E000.0 0000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cnsofD	#1002021.exe, 00000000.0000000 3.235656212.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype./	#1002021.exe, 00000000.0000000 3.244015705.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	#1002021.exe, 00000000.0000000 3.239769294.000000000612B000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comadilo	#1002021.exe, 00000000.0000000 3.236825430.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.det	#1002021.exe, 00000000.0000000 3.239667019.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comona	#1002021.exe, 00000000.0000000 3.236345460.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com(s	#1002021.exe, 00000000.0000000 3.232991542.000000000612B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers8	#1002021.exe, 00000000.0000000 2.268152409.0000000006200000.0 0000002.00000001.sdmp	false		high
http://BtAllR.com	#1002021.exe, 00000002.0000000 2.507026512.0000000002B41000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.yillyenterprise.com	#1002021.exe, 00000002.0000000 2.509235147.0000000002DF0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comncy	#1002021.exe, 00000000.0000000 3.236050979.000000000612F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	#1002021.exe, 00000000.0000000 3.240149325.000000000612B000.0 0000004.00000001.sdmp	false		high
http://yillyenterprise.com	#1002021.exe, 00000002.0000000 2.509235147.0000000002DF0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnnie	#1002021.exe, 00000000.0000000 3.235268592.0000000006132000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.6.198.237	yillyenterprise.com	Malaysia		46015	EXABYTES-AS-APExaBytesNetworkSdnBhdMY	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383981
Start date:	08.04.2021
Start time:	13:33:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#1002021.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:	14
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% (good quality ratio 0%) • Quality average: 51% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 99% • 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, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 95.100.54.203, 52.255.188.83, 40.88.32.150, 205.185.216.10, 205.185.216.42 • Excluded domains from analysis (whitelisted): fs.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.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
13:34:12	API Interceptor	689x Sleep call for process: #1002021.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.6.198.237	#100028153.exe	Get hash	malicious	Browse	
	#ENQ67548820.exe	Get hash	malicious	Browse	
	_0000628.EXE	Get hash	malicious	Browse	
	RFQ#100027386.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EXABYTES-AS-APExaBytesNetworkSdnBhdMY	PO AA21C04U3101-MTXGA6_PDF.exe	Get hash	malicious	Browse	• 137.59.110.57
	#100028153.exe	Get hash	malicious	Browse	• 103.6.198.237
	#ENQ67548820.exe	Get hash	malicious	Browse	• 103.6.198.237
	PO AA21C04U3101-MTXGA6_PDF.exe	Get hash	malicious	Browse	• 137.59.110.57
	New Order 1-4-2021_PDF.exe	Get hash	malicious	Browse	• 137.59.110.57
	New Order 1-4-2021_PDF.exe	Get hash	malicious	Browse	• 137.59.110.57
	TaTYytHaBk.exe	Get hash	malicious	Browse	• 110.4.47.139
	_0000628.EXE	Get hash	malicious	Browse	• 103.6.198.237
	confirm bank account details pdf.exe	Get hash	malicious	Browse	• 103.6.198.37
	RFQ#100027386.exe	Get hash	malicious	Browse	• 103.6.198.237
	SWIFT COPY.png.exe	Get hash	malicious	Browse	• 103.6.196.156
	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	• 103.6.196.156
	bank slip 10 285 USD..exe	Get hash	malicious	Browse	• 103.6.198.37
	1 Total New Invoices_Wendesday March 10_2021.xlsm	Get hash	malicious	Browse	• 137.59.109.40
	Request Quotation.exe	Get hash	malicious	Browse	• 103.6.198.37
	change certificate.exe	Get hash	malicious	Browse	• 103.6.196.156
	Products Lists.exe	Get hash	malicious	Browse	• 103.6.196.156
	payment and Bank confirm.exe	Get hash	malicious	Browse	• 103.6.198.37
	Scanned Copy.exe	Get hash	malicious	Browse	• 103.6.196.156
	Scanned Copy.exe	Get hash	malicious	Browse	• 103.6.196.156

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#1002021.exe.log	
Process:	C:\Users\user\Desktop\#1002021.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\Roaming\jvbxs1bu.tzq\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\#1002021.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

C:\Users\user\AppData\Roaming\jvbxs1bu.tzq\Chrome\Default\Cookies	
SHA1:	DF5EE16ECF4B3B02E312F935AE81D4C5D2E91CA8
SHA-256:	39B4E45A062DEA6F541C18FA1A15C5C0DB43A59673A26E2EB5B8A4345EE767AE
SHA-512:	3CF87455263E395313E779D4F440D8405D86244E04B5F577BB9FA2F4A2069DE019D340F6B2F6EF420DEE3D3DEEFD4B58DA3FCA3BB802DE348E1A810D6379CC3B
Malicious:	false
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):	7.85966850681175
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:	#1002021.exe
File size:	812032
MD5:	6208b6541936333f498204d1ec7234db
SHA1:	62a31f0f710ce7af593ff6ce28d22b8fe1ca8097
SHA256:	c1f2ef3f7a994adba520b81e95a6c792a263d574247d66b7d1e3edce99a4910d
SHA512:	e4096f7151f1b2d8334fce72171cc2d15ad6db7f2dd073d969d376e4e1afc7d32e4f058fc4cc92dd0ccad48a0494f37526ed62139b21b2e0517c26e8c2ca2a1e
SSDEEP:	24576:QWqx8H2Lu1CzjFYERRLdRJEO0Kb5e5Z1dPoOv1xJNESy:iiaiER1dl0KOZ1FoOv1xzty
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....n`.....0..:...(.....Y... ...`....@.. .....@.....

File Icon

Icon Hash:	12b2b2f069f0d6a8

Static PE Info

General	
Entrypoint:	0x4b5992
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:	0x606EA71C [Thu Apr 8 06:47:56 2021 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

General	
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
mov dword ptr [eax+4Eh], edx
inc edi
or eax, 000A1A0Ah
add byte ptr [eax], al
add byte ptr [ecx+45h], cl
dec esi
inc esp
scasb
inc edx
pushad
add byte ptr [eax], 00000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb5940	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0x124fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xca000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb39b0	0xb3a00	False	0.905251011221	data	7.89650748238	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x124fc	0x12600	False	0.824776785714	data	7.32099896967	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xca000	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	0xb6220	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb6ac8	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0xb7030	0xd49e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xc44d0	0x25a8	data		
RT_ICON	0xc6a78	0x10a8	data		
RT_ICON	0xc7b20	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xc7f88	0x5a	data		
RT_VERSION	0xc7fe4	0x32c	data		
RT_MANIFEST	0xc8310	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

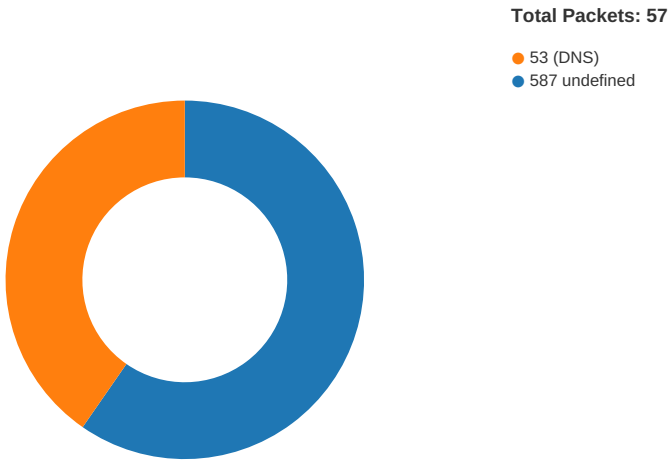
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018 - 2021
Assembly Version	3.1.0.5
InternalName	H.exe
FileVersion	3.1.0.5
CompanyName	
LegalTrademarks	
Comments	
ProductName	Image Manager
ProductVersion	3.1.0.5
FileDescription	Image Manager
OriginalFilename	H.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:36:02.138163	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49705	587	192.168.2.7	103.6.198.237
04/08/21-13:36:08.550492	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49706	587	192.168.2.7	103.6.198.237

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:36:00.308623075 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:00.466739893 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:00.467614889 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:01.137983084 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:01.138521910 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:01.296506882 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:01.299990892 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:01.459542036 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:01.460814953 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:01.651850939 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:01.652968884 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:01.812494993 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:01.813287020 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:01.974700928 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:01.975182056 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:02.133290052 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:02.133307934 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:02.138163090 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:02.138336897 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:02.138469934 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:02.138586998 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:02.296458960 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:02.296482086 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:05.547955036 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:05.590473890 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:06.851862907 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:07.012679100 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:07.012996912 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:07.014355898 CEST	49705	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:07.014781952 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:07.171219110 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:07.171348095 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:07.172239065 CEST	587	49705	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:07.487416029 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:07.487638950 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:07.644337893 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:07.644555092 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:07.800918102 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:07.801172018 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:07.978279114 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:08.027883053 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.071701050 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.233066082 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:08.233257055 CEST	49706	587	192.168.2.7	103.6.198.237

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:36:08.390316010 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:08.390476942 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.548403025 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:08.548432112 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:08.550410986 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.550492048 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.550518990 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.550554037 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.550637007 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.550657034 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.550661087 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.550676107 CEST	49706	587	192.168.2.7	103.6.198.237
Apr 8, 2021 13:36:08.706649065 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:08.706670046 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:08.706681967 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:11.958472013 CEST	587	49706	103.6.198.237	192.168.2.7
Apr 8, 2021 13:36:12.013428926 CEST	49706	587	192.168.2.7	103.6.198.237

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:34:19.735174894 CEST	61952	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:19.752474070 CEST	53	61952	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:20.758141994 CEST	56217	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:20.770637989 CEST	53	56217	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:21.843661070 CEST	63354	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:21.862265110 CEST	53	63354	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:22.156939983 CEST	53129	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:22.170968056 CEST	53	53129	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:22.935903072 CEST	62452	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:22.948343039 CEST	53	62452	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:24.252343893 CEST	57820	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:24.264970064 CEST	53	57820	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:25.264617920 CEST	50848	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:25.277242899 CEST	53	50848	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:26.485866070 CEST	61242	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:26.497875929 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:27.884309053 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:27.896723032 CEST	53	58562	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:28.616936922 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:28.629602909 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:30.039819956 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:30.053356886 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:30.991672993 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:31.004616976 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:31.773818970 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:31.786288023 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:32.758627892 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:32.771891117 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:33.777765036 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:33.790277004 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:34.611301899 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:34.623920918 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:35.923217058 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:35.935611963 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:37.182908058 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:37.196460009 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:37.874840021 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:37.888325930 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:38.735637903 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:38.749036074 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 8, 2021 13:34:49.110804081 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:34:49.123847008 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 8, 2021 13:35:59.881308079 CEST	58052	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:36:00.025511980 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 8, 2021 13:36:00.043958902 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 8, 2021 13:36:00.180869102 CEST	53	54008	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:35:59.881308079 CEST	192.168.2.7	8.8.8.8	0x561	Standard query (0)	mail.yilly enterprise.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:36:00.043958902 CEST	192.168.2.7	8.8.8.8	0x294c	Standard query (0)	mail.yilly enterprise.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:36:00.025511980 CEST	8.8.8.8	192.168.2.7	0x561	No error (0)	mail.yilly enterprise.com	yillyenterprise.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:36:00.025511980 CEST	8.8.8.8	192.168.2.7	0x561	No error (0)	yillyenter prise.com		103.6.198.237	A (IP address)	IN (0x0001)
Apr 8, 2021 13:36:00.180869102 CEST	8.8.8.8	192.168.2.7	0x294c	No error (0)	mail.yilly enterprise.com	yillyenterprise.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:36:00.180869102 CEST	8.8.8.8	192.168.2.7	0x294c	No error (0)	yillyenter prise.com		103.6.198.237	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 8, 2021 13:36:01.137983084 CEST	587	49705	103.6.198.237	192.168.2.7	220-naan.mschosting.com ESMTP Exim 4.94 #2 Thu, 08 Apr 2021 19:36:00 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 8, 2021 13:36:01.138521910 CEST	49705	587	192.168.2.7	103.6.198.237	EHLO 562258
Apr 8, 2021 13:36:01.296506882 CEST	587	49705	103.6.198.237	192.168.2.7	250-naan.mschosting.com Hello 562258 [185.32.222.8] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 8, 2021 13:36:01.299990892 CEST	49705	587	192.168.2.7	103.6.198.237	AUTH login ZWt3ZUB5aWxseWVudGVycHJpc2UuY29t
Apr 8, 2021 13:36:01.459542036 CEST	587	49705	103.6.198.237	192.168.2.7	334 UGFzc3dvcmQ6
Apr 8, 2021 13:36:01.651850939 CEST	587	49705	103.6.198.237	192.168.2.7	235 Authentication succeeded
Apr 8, 2021 13:36:01.652968884 CEST	49705	587	192.168.2.7	103.6.198.237	MAIL FROM:<ekwe@yillyenterprise.com>
Apr 8, 2021 13:36:01.812494993 CEST	587	49705	103.6.198.237	192.168.2.7	250 OK
Apr 8, 2021 13:36:01.813287020 CEST	49705	587	192.168.2.7	103.6.198.237	RCPT TO:<ekwe@yillyenterprise.com>
Apr 8, 2021 13:36:01.974700928 CEST	587	49705	103.6.198.237	192.168.2.7	250 Accepted
Apr 8, 2021 13:36:01.975182056 CEST	49705	587	192.168.2.7	103.6.198.237	DATA
Apr 8, 2021 13:36:02.133307934 CEST	587	49705	103.6.198.237	192.168.2.7	354 Enter message, ending with "." on a line by itself
Apr 8, 2021 13:36:02.138586998 CEST	49705	587	192.168.2.7	103.6.198.237	.
Apr 8, 2021 13:36:05.547955036 CEST	587	49705	103.6.198.237	192.168.2.7	250 OK id=1lUSx7-0001j3-7A
Apr 8, 2021 13:36:06.851862907 CEST	49705	587	192.168.2.7	103.6.198.237	QUIT
Apr 8, 2021 13:36:07.012679100 CEST	587	49705	103.6.198.237	192.168.2.7	221 naan.mschosting.com closing connection
Apr 8, 2021 13:36:07.487416029 CEST	587	49706	103.6.198.237	192.168.2.7	220-naan.mschosting.com ESMTP Exim 4.94 #2 Thu, 08 Apr 2021 19:36:06 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 8, 2021 13:36:07.487638950 CEST	49706	587	192.168.2.7	103.6.198.237	EHLO 562258
Apr 8, 2021 13:36:07.644337893 CEST	587	49706	103.6.198.237	192.168.2.7	250-naan.mschosting.com Hello 562258 [185.32.222.8] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 8, 2021 13:36:07.644555092 CEST	49706	587	192.168.2.7	103.6.198.237	AUTH login ZWt3ZUB5aWxseWVudGVycHJpc2UuY29t
Apr 8, 2021 13:36:07.800918102 CEST	587	49706	103.6.198.237	192.168.2.7	334 UGFzc3dvcmQ6

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 8, 2021 13:36:07.978279114 CEST	587	49706	103.6.198.237	192.168.2.7	235 Authentication succeeded
Apr 8, 2021 13:36:08.071701050 CEST	49706	587	192.168.2.7	103.6.198.237	MAIL FROM:<ekwe@yillyenterprise.com>
Apr 8, 2021 13:36:08.233066082 CEST	587	49706	103.6.198.237	192.168.2.7	250 OK
Apr 8, 2021 13:36:08.233257055 CEST	49706	587	192.168.2.7	103.6.198.237	RCPT TO:<ekwe@yillyenterprise.com>
Apr 8, 2021 13:36:08.390316010 CEST	587	49706	103.6.198.237	192.168.2.7	250 Accepted
Apr 8, 2021 13:36:08.390476942 CEST	49706	587	192.168.2.7	103.6.198.237	DATA
Apr 8, 2021 13:36:08.548432112 CEST	587	49706	103.6.198.237	192.168.2.7	354 Enter message, ending with "." on a line by itself
Apr 8, 2021 13:36:08.550676107 CEST	49706	587	192.168.2.7	103.6.198.237	.
Apr 8, 2021 13:36:11.958472013 CEST	587	49706	103.6.198.237	192.168.2.7	250 OK id=1lUSxD-0001lg-KU

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: #1002021.exe PID: 4612 Parent PID: 5680

General

Start time:	13:34:01
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\#1002021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\#1002021.exe'
Imagebase:	0xd70000
File size:	812032 bytes
MD5 hash:	6208B6541936333F498204D1EC7234DB
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: 00000000.00000002.260493550.0000000004229000.00000004.00000001.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	6D57CF06	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	6D57CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#1002021.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D88C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#1002021.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	6D88C907	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	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile

Analysis Process: #1002021.exe PID: 2672 Parent PID: 4612

General

Start time:	13:34:14
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\#1002021.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x790000
File size:	812032 bytes
MD5 hash:	6208B6541936333F498204D1EC7234DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.497062143.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.507026512.0000000002B41000.00000004.00000001.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	6D57CF06	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	6D57CF06	unknown
C:\Users\user\AppData\Roaming\jvbxs1bu.tzq	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C3CBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\jvbxs1bu.tzq\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	6C3CBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\jvbxs1bu.tzq\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	6C3CBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jvbxs1bu.tzq\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	6C3CDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jvbxs1bu.tzq\Chrome\Default\Cookies	success or wait	1	6C3C6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jvbxs1bu.tzq\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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C3CDD66	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	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C3C1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\721ac9f9-74c4-46ef-8d38-e7051d0f45dc	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C3C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C3C1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C3C1B4F	ReadFile
C:\Users\user\AppData\Roaming\jvbxs1bu.tzq\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C3C1B4F	ReadFile

Disassembly

Code Analysis