ID: 385473
Sample Name: BILL-OOO566876.exe
Cookbook: default.jbs
Time: 15:16:17
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

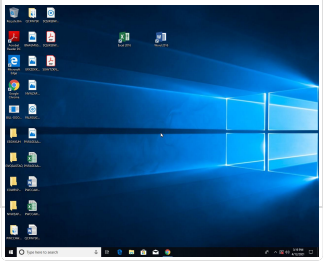
Analysis Report BILL-OOO566876.exe

Overview

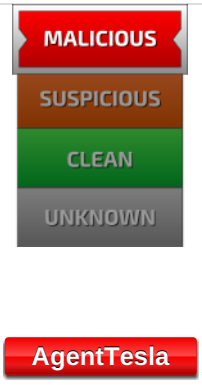
General Information

Sample Name:	BILL-OOO566876.exe
Analysis ID:	385473
MD5:	1c84862e5b015b..
SHA1:	a3e0a0bda2cdef9.
SHA256:	ea29689e038f2a8.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



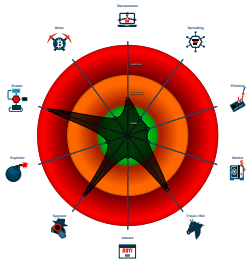
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Found evasive API chain (trying to d…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- BILL-OOO566876.exe (PID: 1308 cmdline: 'C:\Users\user\Desktop\BILL-OOO566876.exe' MD5: 1C84862E5B015BCECF6A194D17172DCF)
  - BILL-OOO566876.exe (PID: 1156 cmdline: {path} MD5: 1C84862E5B015BCECF6A194D17172DCF)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "rainie.wang@syntrnomh.comTdn$AuZro1smtp.syntrnomh.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.476024928.0000000002E51000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.476024928.0000000002E51000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.222165033.0000000003F36000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.469525382.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: BILL-OOO566876.exe PID: 1156	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 3 entries

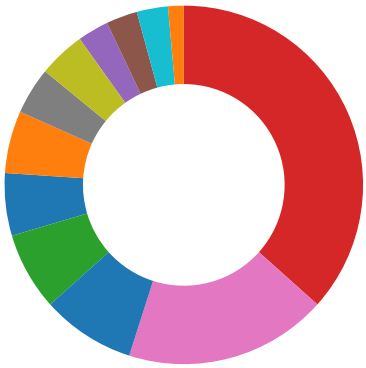
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.BILL-OOO566876.exe.40f75c0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.BILL-OOO566876.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.BILL-OOO566876.exe.40f75c0.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.BILL-OOO566876.exe.3fb6720.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

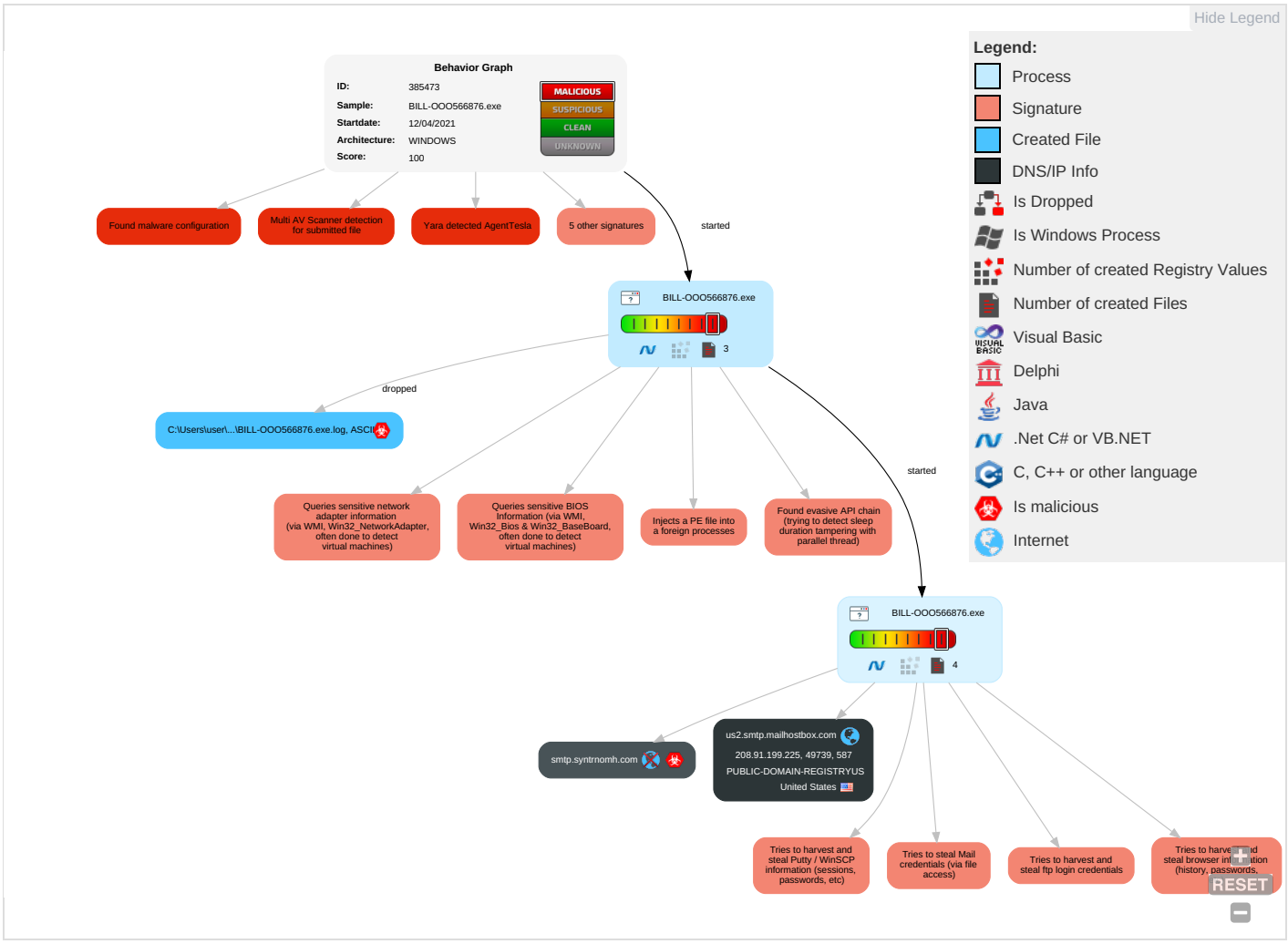
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

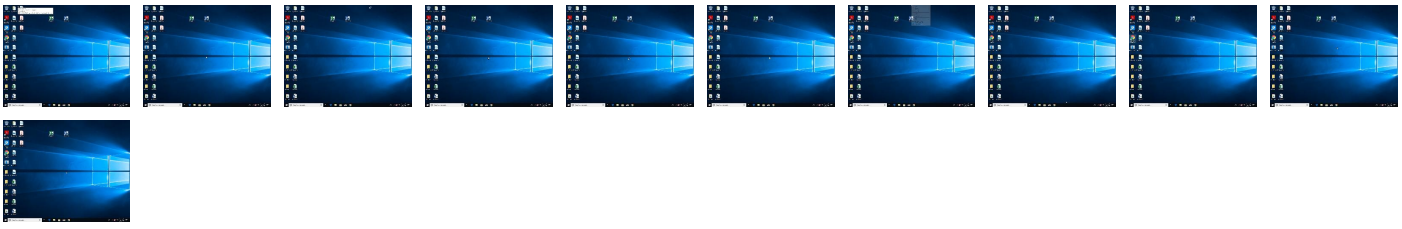
Behavior Graph



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

Source	Detection	Scanner	Label	Link
BILL-OOO566876.exe	25%	Virustotal		Browse
BILL-OOO566876.exe	16%	Metadefender		Browse
BILL-OOO566876.exe	52%	ReversingLabs	Win32.Trojan.AgentTesla	
BILL-OOO566876.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.BILL-OOO566876.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.fonts.comno	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	
http://hBlbMr.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://https://8chan.moe/	0%	Avira URL Cloud	safe	
http://YdPNTdHEQXue9T.orgl;	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.com)	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.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.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.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.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.comx	0%	URL Reputation	safe	
http://www.fonts.comx	0%	URL Reputation	safe	
http://www.fonts.comx	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.fontbureau.com=	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.tiro.comx	0%	Avira URL Cloud	safe	
http://https://8kun.top/	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	

Source	Detection	Scanner	Label	Link
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.carterandcone.comY	0%	Avira URL Cloud	safe	
http://www.carterandcone.comu	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://https://raw.githubusercontent.com/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://YdPNTdHEQXue9T.org	0%	Avira URL Cloud	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high
smtp.syntrnomh.com	unknown	unknown	true		unknown

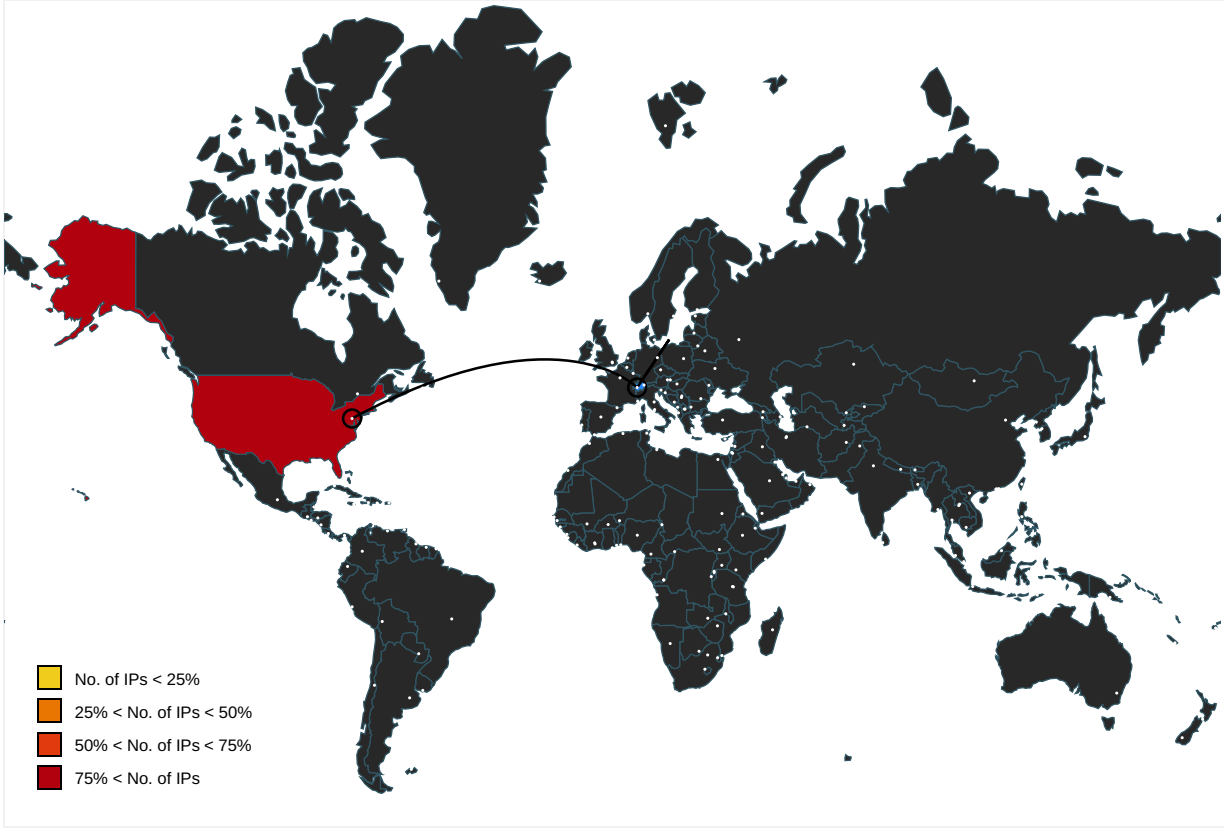
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	BILL-OOO566876.exe, 00000002.00000002.476024928.0000000002E51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	BILL-OOO566876.exe, 00000000.00000002.225516202.000000000054C0000.00000002.00000001.sdmp	false		high
http://www.fonts.comno	BILL-OOO566876.exe, 00000000.00000003.202973628.00000000053EB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/murrty/ychanex/releases/latest	BILL-OOO566876.exe, 00000000.00000002.221101600.0000000002F11000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	BILL-OOO566876.exe, 00000000.00000002.225516202.000000000054C0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	BILL-OOO566876.exe, 00000000.00000002.225516202.000000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.420chan.org/	BILL-OOO566876.exe, 00000000.00000002.221101600.0000000002F11000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	BILL-OOO566876.exe, 00000000.00000002.225516202.000000000054C0000.00000002.00000001.sdmp	false		high
http://hBlbMr.com	BILL-OOO566876.exe, 00000002.00000002.476024928.0000000002E51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	BILL-OOO566876.exe, 00000000.00000002.225516202.000000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://8chan.moe/	BILL-OOO566876.exe, 00000000.00000002.221101600.0000000002F11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false		high
http://YdPNTdHEQXue9T.orgl;	BILL-OOO566876.exe, 00000002.00000002.476441058.0000000002EFC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.goodfont.co.kr	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	BILL-OOO566876.exe, 00000000.00000003.206256359.00000000053D9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com)	BILL-OOO566876.exe, 00000000.00000003.206174068.00000000053D7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com	BILL-OOO566876.exe, 00000000.00000003.202808276.00000000053EB000.00000004.00000001.sdmp, BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	BILL-OOO566876.exe, 00000000.00000003.211731693.000000000540D000.00000004.00000001.sdmp, BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/murrty/ychanex	BILL-OOO566876.exe, 00000000.00000002.221101600.0000000002F11000.00000004.00000001.sdmp	false		high
http://https://github.com/	BILL-OOO566876.exe, 00000000.00000002.221101600.0000000002F11000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comx	BILL-OOO566876.exe, 00000000.00000003.202973628.00000000053EB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	BILL-OOO566876.exe, 00000000.00000002.222165033.0000000003F36000.00000004.00000001.sdmp, BILL-OOO566876.exe, 00000002.00000002.469525382.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com=	BILL-OOO566876.exe, 00000000.00000003.218522176.00000000053D0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	BILL-OOO566876.exe, 00000000.00000003.218522176.00000000053D0000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	BILL-OOO566876.exe, 00000002.00000002.476024928.0000000002E51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comx	BILL-OOO566876.exe, 00000000.00000003.204324110.00000000053EB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://8kun.top/	BILL-OOO566876.exe, 00000000.00000002.221101600.0000000002F11000.00000004.00000001.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	BILL-OOO566876.exe, 00000002.00000002.476024928.0000000002E51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comY	BILL-OOO566876.exe, 00000000.00000003.206174068.00000000053D7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comu	BILL-OOO566876.exe, 00000000.00000003.206256359.00000000053D9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	BILL-OOO566876.exe, 00000000.00000003.218522176.00000000053D0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmld	BILL-OOO566876.exe, 00000000.00000003.208525319.000000000540D000.00000004.00000001.sdmp	false		high
http://en.w	BILL-OOO566876.exe, 00000000.00000003.203328834.00000000053D7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://raw.githubusercontent.com/	BILL-OOO566876.exe, 00000000.00000002.221101600.0000000002F11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp, BILL-OOO566876.exe, 00000000.00000003.208195250.000000000540D000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	BILL-OOO566876.exe, 00000000.00000003.208525319.000000000540D000.00000004.00000001.sdmp	false		high
http://https://a.4cdn.org/	BILL-OOO566876.exe, 00000000.00000002.221101600.0000000002F11000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	BILL-OOO566876.exe, 00000000.00000002.225516202.00000000054C0000.00000002.00000001.sdmp	false		high
http://https://github.com/murrty/YChanEx/	BILL-OOO566876.exe, 00000000.00000002.221101600.0000000002F11000.00000004.00000001.sdmp	false		high
http://YdPNTdHEQXue9T.org	BILL-OOO566876.exe, 00000002.00000002.476441058.0000000002EFC000.00000004.00000001.sdmp, BILL-OOO566876.exe, 00000002.00000002.476845028.0000000002F88000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.github.com/repos/	BILL-OOO566876.exe, 00000000.00000002.221101600.0000000002F11000.00000004.00000001.sdmp	false		high
http://www.tiro.comc	BILL-OOO566876.exe, 00000000.00000003.203388064.00000000053EB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.225	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385473
Start date:	12.04.2021
Start time:	15:16:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BILL-OOO566876.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 11.9% (good quality ratio 6.6%) • Quality average: 32.2% • Quality standard deviation: 36.5%
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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 204.79.197.200, 13.107.21.200, 52.147.198.201, 20.50.102.62, 184.30.24.56, 92.122.213.194, 92.122.213.247, 13.88.21.125, 205.185.216.42, 205.185.216.10, 20.54.26.129, 13.64.90.137 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:17:11	API Interceptor	969x Sleep call for process: BILL-OOO566876.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.225	ORDER 9387383900.xlsx	Get hash	malicious	Browse	
	usd 420232.exe	Get hash	malicious	Browse	
	P037725600.exe	Get hash	malicious	Browse	
	VAT INVOICE.exe	Get hash	malicious	Browse	
	New Order PO#121012020_____PDF_____.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	swift Copy.xls.exe	Get hash	malicious	Browse	
	AD1-2001028L.exe	Get hash	malicious	Browse	
	AD1-2001028L (2).exe	Get hash	malicious	Browse	
	#U7f8e#U91d1#U532f#U738728.84 (USD 40,257+5% #U7a05.exe	Get hash	malicious	Browse	
	balance payment.exe	Get hash	malicious	Browse	
	Image0001.exe	Get hash	malicious	Browse	
	money.exe	Get hash	malicious	Browse	
	new order.doc	Get hash	malicious	Browse	
	New Enquiry.MORROCCO.exe	Get hash	malicious	Browse	
	Purchase Order #07916813.exe	Get hash	malicious	Browse	
	QUOTATION 03-28-2021.exe	Get hash	malicious	Browse	
	PURCHASE ORDER COPY.exe	Get hash	malicious	Browse	
	credit notification.exe	Get hash	malicious	Browse	
	PURCHASE ORDER COPY.exe	Get hash	malicious	Browse	
	Ref_0866_0817.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	SecuriteInfo.com.Scr.Malcodegdn30.29716.exe	Get hash	malicious	Browse	• 208.91.198.143
	ORDER 9387383900.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Payment Advice Note from 02.04.2021 to 608761.exe	Get hash	malicious	Browse	• 208.91.199.223
	e0xd7qhFaMk3Dpx.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAGO FACTURA V-8680.exe	Get hash	malicious	Browse	• 208.91.198.143
	usd 420232.exe	Get hash	malicious	Browse	• 208.91.199.225
	P037725600.exe	Get hash	malicious	Browse	• 208.91.199.225
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW ORDER.exe	Get hash	malicious	Browse	• 208.91.198.143
	TRANSFERENCIA AL EXTERIOR U810295.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAYMENT SWIFT COPY MT103.exe	Get hash	malicious	Browse	• 208.91.198.143
	UPDATED SOA.exe	Get hash	malicious	Browse	• 208.91.199.224
	BANK PAYMENT.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	IMG_00000000001.PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	New Order PO#121012020_____PDF_____.exe	Get hash	malicious	Browse	• 208.91.198.143
	swift Copy.xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 208.91.199.224

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	SecuriteInfo.com.Scr.Malcodegdn30.29716.exe	Get hash	malicious	Browse	• 208.91.198.143
	commercial invoice & packing list doc.exe	Get hash	malicious	Browse	• 43.225.55.205
	ORDER 9387383900.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Payment Advice Note from 02.04.2021 to 608761.exe	Get hash	malicious	Browse	• 208.91.199.223
	Dubai REGA 2021UAE.exe	Get hash	malicious	Browse	• 208.91.199.135
	e0xd7qhFaMk3Dpx.exe	Get hash	malicious	Browse	• 208.91.198.143
	Dridex.xls	Get hash	malicious	Browse	• 208.91.199.159
	documents-351331057.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	documents-351331057.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	DUBAI UAEGH092021.exe	Get hash	malicious	Browse	• 208.91.199.135
	PAGO FACTURA V-8680.exe	Get hash	malicious	Browse	• 208.91.198.143
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	usd 420232.exe	Get hash	malicious	Browse	• 208.91.199.225
	P037725600.exe	Get hash	malicious	Browse	• 208.91.199.225
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	NEW ORDER.exe	Get hash	malicious	Browse	• 208.91.198.143
	TRANSFERENCIA AL EXTERIOR U810295.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAYMENT SWIFT COPY MT103.exe	Get hash	malicious	Browse	• 208.91.198.143

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\BILL-OOO566876.exe.log	
Process:	C:\Users\user\Desktop\BILL-OOO566876.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6241220288435505
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:	BILL-OOO566876.exe
File size:	893952
MD5:	1c84862e5b015bcecf6a194d17172dcf
SHA1:	a3e0a0bda2cdef94089a6012bd025113f9fbead9
SHA256:	ea29689e038f2a801066054f8ae2e3e3884127e8ac897f5467055250ce2b42f9
SHA512:	786b1e6f5c283b33bb55e252355346af43715b81f926cb035c9935ba031958e21413e2bd54fa7c8fc198b725043131a3abf39adc418d03a72a9d3afd9d42bdc
SSDEEP:	12288:g/m/1Vjriddyflf5T716samRCChXNNAdUbuTSYScJ/cfCTpc7kg5M7Cdb/G/uxFB:AaSyB5T716rmRCQB6T5/hT5kb/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....0..... .....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

General	
Entrypoint:	0x4db91e
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:	0x60731BE9 [Sun Apr 11 15:55:21 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdb8c4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xdc000	0x5c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xde000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd9924	0xd9a00	False	0.765819078475	data	7.62974179137	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xdc000	0x5c0	0x600	False	0.428385416667	data	4.12173224524	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xde000	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	0xdc0a0	0x330	data		
RT_MANIFEST	0xdc3d0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

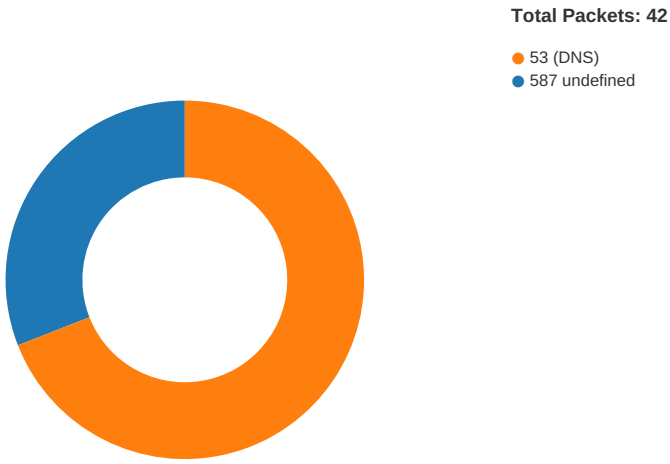
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Microsoft 2018
Assembly Version	1.0.0.0
InternalName	mWu.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	ASCIIArt
ProductVersion	1.0.0.0
FileDescription	ASCIIArt
OriginalFilename	mWu.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:18:42.176328897 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:42.352276087 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:42.352453947 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:42.875756979 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:42.876359940 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:43.050717115 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:43.050755024 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:43.052225113 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:43.228472948 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:43.229031086 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:43.407139063 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:43.407423019 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:43.585530043 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:43.585781097 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:43.771244049 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:43.771477938 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:43.946533918 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:43.960316896 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:43.960429907 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:43.960508108 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:43.960582018 CEST	49739	587	192.168.2.3	208.91.199.225
Apr 12, 2021 15:18:44.134759903 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:44.134810925 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:44.231465101 CEST	587	49739	208.91.199.225	192.168.2.3
Apr 12, 2021 15:18:44.280231953 CEST	49739	587	192.168.2.3	208.91.199.225

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:16:57.626996040 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:16:57.676660061 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 12, 2021 15:16:57.950560093 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:16:58.002713919 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 15:16:59.123594046 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:16:59.172378063 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:00.325143099 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:00.382375002 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:10.669775009 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:10.718667030 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:11.884468079 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:11.935942888 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:12.807837009 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:12.859298944 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:16.975037098 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:17.026108980 CEST	53	58361	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:17:22.659409046 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:22.708585978 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:28.712503910 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:28.770036936 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:29.946908951 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:29.998414993 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:33.402914047 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:33.451730013 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:34.819503069 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:34.881642103 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:45.875643015 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:45.934130907 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:50.349664927 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:50.401159048 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:51.484985113 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:51.536576033 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:53.174205065 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:53.205549002 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:53.222877026 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:53.264185905 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:54.363640070 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:54.420811892 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:55.627034903 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:55.675615072 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:56.907742977 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:56.956568956 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 15:17:58.024431944 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:17:58.073045015 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 15:18:03.563596010 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:18:03.631918907 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 15:18:09.803677082 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:18:09.855288029 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 15:18:13.240446091 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:18:13.297455072 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 15:18:29.325659990 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:18:29.374316931 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 15:18:41.811301947 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:18:42.129463911 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 15:18:44.853279114 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:18:44.901916027 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 15:18:47.035443068 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:18:47.092525959 CEST	53	56579	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:18:41.811301947 CEST	192.168.2.3	8.8.8.8	0x51eb	Standard query (0)	smtp.syntrnomh.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:18:42.129463911 CEST	8.8.8.8	192.168.2.3	0x51eb	No error (0)	smtp.syntrnomh.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:18:42.129463911 CEST	8.8.8.8	192.168.2.3	0x51eb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Apr 12, 2021 15:18:42.129463911 CEST	8.8.8.8	192.168.2.3	0x51eb	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Apr 12, 2021 15:18:42.129463911 CEST	8.8.8.8	192.168.2.3	0x51eb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Apr 12, 2021 15:18:42.129463911 CEST	8.8.8.8	192.168.2.3	0x51eb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

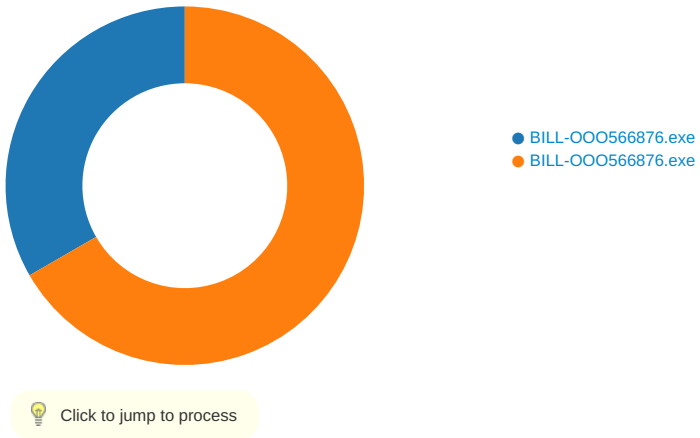
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 15:18:42.875756979 CEST	587	49739	208.91.199.225	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Apr 12, 2021 15:18:42.876359940 CEST	49739	587	192.168.2.3	208.91.199.225	EHLO 134349
Apr 12, 2021 15:18:43.050755024 CEST	587	49739	208.91.199.225	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Apr 12, 2021 15:18:43.052225113 CEST	49739	587	192.168.2.3	208.91.199.225	AUTH login cmFpbmllLndhbmdAc3ludHJub21oLmNvbQ==
Apr 12, 2021 15:18:43.228472948 CEST	587	49739	208.91.199.225	192.168.2.3	334 UGFzc3dvcmQ6
Apr 12, 2021 15:18:43.407139063 CEST	587	49739	208.91.199.225	192.168.2.3	235 2.7.0 Authentication successful
Apr 12, 2021 15:18:43.407423019 CEST	49739	587	192.168.2.3	208.91.199.225	MAIL FROM:<rainie.wang@syntrnomh.com>
Apr 12, 2021 15:18:43.585530043 CEST	587	49739	208.91.199.225	192.168.2.3	250 2.1.0 Ok
Apr 12, 2021 15:18:43.585781097 CEST	49739	587	192.168.2.3	208.91.199.225	RCPT TO:<rainie.wang@syntrnomh.com>
Apr 12, 2021 15:18:43.771244049 CEST	587	49739	208.91.199.225	192.168.2.3	250 2.1.5 Ok
Apr 12, 2021 15:18:43.771477938 CEST	49739	587	192.168.2.3	208.91.199.225	DATA
Apr 12, 2021 15:18:43.946533918 CEST	587	49739	208.91.199.225	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Apr 12, 2021 15:18:43.960582018 CEST	49739	587	192.168.2.3	208.91.199.225	.
Apr 12, 2021 15:18:44.231465101 CEST	587	49739	208.91.199.225	192.168.2.3	250 2.0.0 Ok: queued as A9165781F07

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: BILL-OOO566876.exe PID: 1308 Parent PID: 5652

General

Start time:	15:17:04
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\BILL-OOO566876.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BILL-OOO566876.exe'
Imagebase:	0x7e0000
File size:	893952 bytes
MD5 hash:	1C84862E5B015BCECF6A194D17172DCF
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: 00000000.00000002.222165033.0000000003F36000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\BILL-OOO566876.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\BILL-OOO566876.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

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

Analysis Process: BILL-OOO566876.exe PID: 1156 Parent PID: 1308

General

Start time:	15:17:12
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\BILL-OOO566876.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x630000
File size:	893952 bytes
MD5 hash:	1C84862E5B015BCECF6A194D17172DCF
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: 00000002.00000002.476024928.0000000002E51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.476024928.0000000002E51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.469525382.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Read

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	58E1183	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	58E1183	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	58E1183	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	58E1183	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	58E1183	ReadFile

Disassembly

Code Analysis