ID: 358326
Sample Name: 4019223246.exe
Cookbook: default.jbs
Time: 12:15:28
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

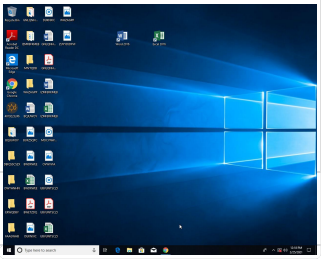
Analysis Report 4019223246.exe

Overview

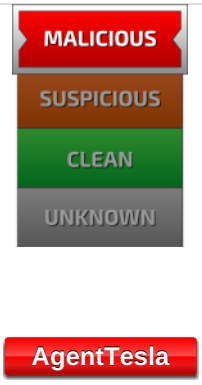
General Information

Sample Name:	4019223246.exe
Analysis ID:	358326
MD5:	87e6882bcebf482.
SHA1:	fa6df79dd667fcb…
SHA256:	369d92b64ee7b4..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

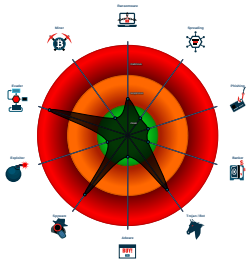


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- Found evasive API chain (trying to d…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- 4019223246.exe (PID: 7056 cmdline: 'C:\Users\user\Desktop\4019223246.exe' MD5: 87E6882BCEBF4823AFB4303AAC3628B1)
  - schtasks.exe (PID: 5708 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\WZXjvtGBEKK' /XML 'C:\Users\user\AppData\Local\Temp\tmp35E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 4019223246.exe (PID: 6104 cmdline: C:\Users\user\Desktop\4019223246.exe MD5: 87E6882BCEBF4823AFB4303AAC3628B1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "systems@krenterprisesindia.comparida@1971@us2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.913312856.0000000002ED4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.658750521.0000000002C95000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.914172803.0000000003E21000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.914560852.0000000004FE0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.913196902.0000000002E21000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 8 entries				

Unpacked PEs

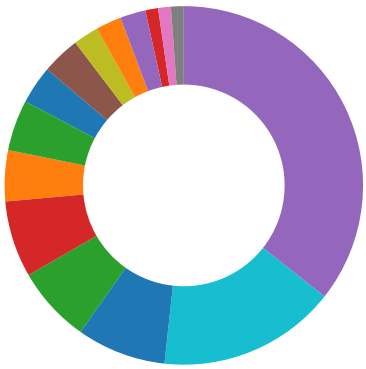
Source	Rule	Description	Author	Strings
4.2.4019223246.exe.25e301e.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.4019223246.exe.3e23258.8.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.4019223246.exe.3e24140.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.4019223246.exe.25e2136.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.3.4019223246.exe.be4648.0.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

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

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

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

Binary contains paths to debug symbols

System Summary:

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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)

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:

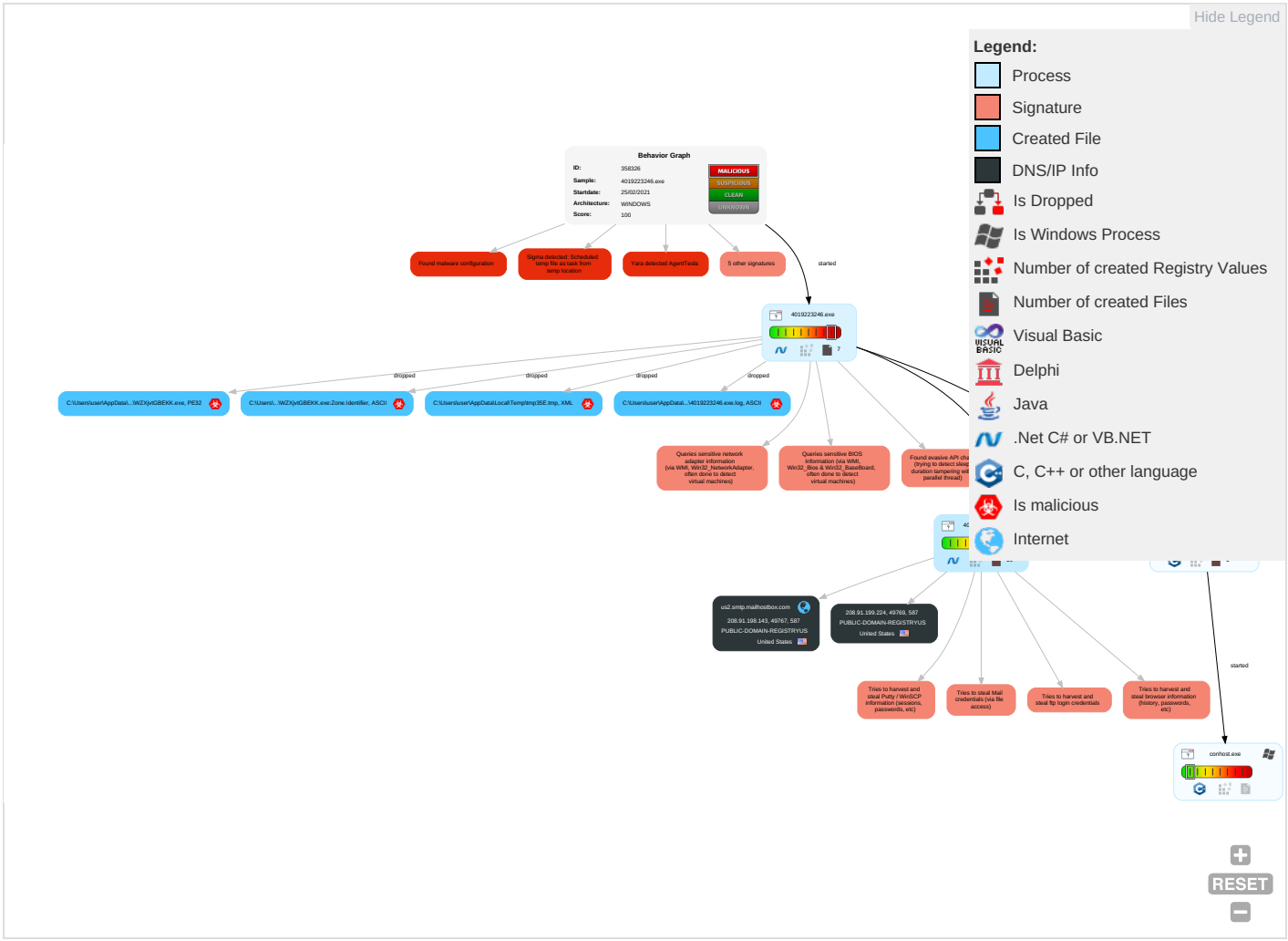
Yara detected AgentTesla

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	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 2 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Security Software Discovery 2 5 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 3	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	Process Injection 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

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
4019223246.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WZXjvtGBEKK.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WZXjvtGBEKK.exe	9%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://wg3NmRd1lkGGL4Op.org	0%	Avira URL Cloud	safe	
http://wg3NmRd1lkGGL4Op.orghb	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%tordir%%ha	0%	URL Reputation	safe	
http://qpQMsG.com	0%	Avira URL Cloud	safe	

Domains and IPs

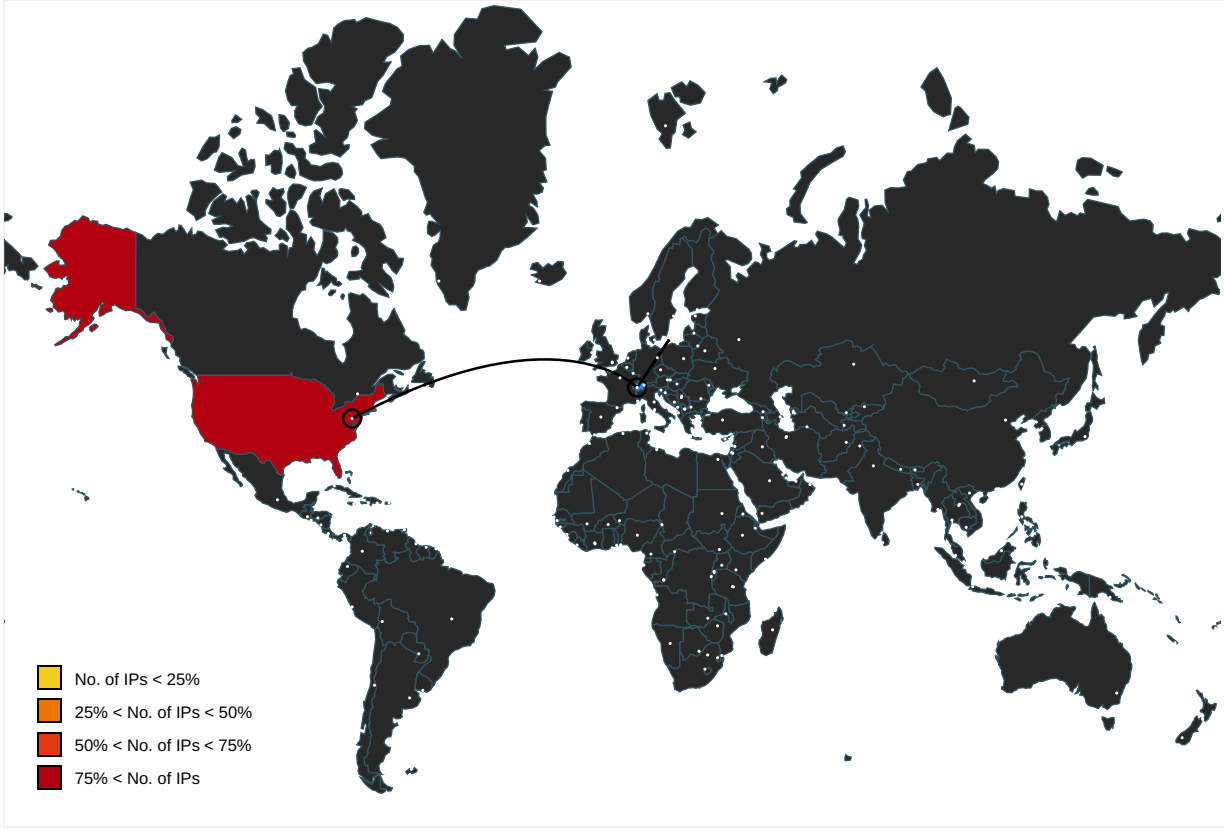
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.143	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	4019223246.exe, 00000004.00000002.913196902.0000000002E21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	4019223246.exe, 00000004.00000002.913196902.0000000002E21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://wg3NmRd1lkGGL4Op.org	4019223246.exe, 00000004.00000002.913312856.0000000002ED4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://wg3NmRd1lkGGL4Op.orghb	4019223246.exe, 00000004.00000002.913312856.0000000002ED4000.00000004.00000001.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	4019223246.exe, 00000004.00000002.913196902.0000000002E21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	4019223246.exe, 00000001.00000002.658704693.0000000002C41000.00000004.00000001.sdmp	false		high
http://qpQMsG.com	4019223246.exe, 00000004.00000002.913196902.0000000002E21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	4019223246.exe, 00000001.00000002.658750521.0000000002C95000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358326
Start date:	25.02.2021
Start time:	12:15:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4019223246.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:	20
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@6/6@2/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.7% (good quality ratio 2.4%) • Quality average: 68.5% • Quality standard deviation: 33.2%
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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 23.211.6.115, 168.61.161.212, 13.64.90.137, 13.88.21.125, 51.11.168.160, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 205.185.216.10, 205.185.216.42, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
12:16:17	API Interceptor	917x Sleep call for process: 4019223246.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	Swift.jpg.exe	Get hash	malicious	Browse	
	1344-21-03-00079 Q N QUEUE.exe	Get hash	malicious	Browse	
	JKG Eximcon Pvt. Ltd P.O.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Mal.Generic-S.15142.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ffkjg5CVrO.exe	Get hash	malicious	Browse	
	7Lf8J7h7os.exe	Get hash	malicious	Browse	
	Shipping Details_PDF.exe	Get hash	malicious	Browse	
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis249E62CF9BAE.exe	Get hash	malicious	Browse	
	inquiry.doc	Get hash	malicious	Browse	
	BL COPY.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.ArtemisF31D2F976320.exe	Get hash	malicious	Browse	
	Proforma Invoice February.exe	Get hash	malicious	Browse	
	133663INV.exe	Get hash	malicious	Browse	
	ConsoleStream.exe	Get hash	malicious	Browse	
	qUq5Aepd3g.exe	Get hash	malicious	Browse	
	GM610izIhl.exe	Get hash	malicious	Browse	
	IMG-09-02-2021-OWA001-pdf.exe	Get hash	malicious	Browse	
208.91.199.224	INVOICE-2101-0006N.exe	Get hash	malicious	Browse	
	HcHimkU72e.exe	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	
	AWB & Shipping Document.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.6572.1879.exe	Get hash	malicious	Browse	
	PAYMENT INVOICE-9876543456789.exe	Get hash	malicious	Browse	
	inquiry.doc	Get hash	malicious	Browse	
	SecuriteInfo.com.CAP_HookExKeylogger.31203.exe	Get hash	malicious	Browse	
	SWIFT COPY 27078.exe	Get hash	malicious	Browse	
	PO 000102.xlsx	Get hash	malicious	Browse	
	Pro.invoice-0656.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.ArtemisF31D2F976320.exe	Get hash	malicious	Browse	
	COMMERCIAL INVOICE BILL OF LADING ETC DOCX..exe	Get hash	malicious	Browse	
	PO-41000055885.exe	Get hash	malicious	Browse	
	Swift Mensaje 093763.exe	Get hash	malicious	Browse	
	xbZkF2dYZz.exe	Get hash	malicious	Browse	
	chrome.exe	Get hash	malicious	Browse	
	statement and proforma invoice.xlsx	Get hash	malicious	Browse	
	GM610izIhl.exe	Get hash	malicious	Browse	
	dheivF8q0m.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Swift.jpg.exe	Get hash	malicious	Browse	• 208.91.198.143
	INVOICE-2101-0006N.exe	Get hash	malicious	Browse	• 208.91.199.224
	1344-21-03-00079 Q N QUEUE.exe	Get hash	malicious	Browse	• 208.91.198.143
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 208.91.199.225
	HcHimkU72e.exe	Get hash	malicious	Browse	• 208.91.199.224
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	• 208.91.199.225
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 208.91.199.224
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 208.91.198.143
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	AOBO MOULD QUOTATION -1752002.exe	Get hash	malicious	Browse	• 208.91.199.225
	JKG Eximcon Pvt. Ltd P.O.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Mal.Generic-S.15142.exe	Get hash	malicious	Browse	• 208.91.198.143
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.Packed2.42850.3598.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.Inject4.6572.1879.exe	Get hash	malicious	Browse	• 208.91.199.224
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 208.91.199.225
	ffkjg5CVrO.exe	Get hash	malicious	Browse	• 208.91.198.143
	7Lf8J7h7os.exe	Get hash	malicious	Browse	• 208.91.199.223
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	YKRAB010B_KHE_Preminary Packing List.xlsx.exe	Get hash	malicious	Browse	• 208.91.199.225

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	data.xls	Get hash	malicious	Browse	• 5.100.152.162
	Swift.jpg.exe	Get hash	malicious	Browse	• 208.91.198.143
	Claim-920537744-02082021.xls	Get hash	malicious	Browse	• 119.18.58.55
	Claim-920537744-02082021.xls	Get hash	malicious	Browse	• 119.18.58.55
	INVOICE-2101-0006N.exe	Get hash	malicious	Browse	• 208.91.199.224
	logs.php.dll	Get hash	malicious	Browse	• 116.206.105.72
	1344-21-03-00079 Q N QUEUE.exe	Get hash	malicious	Browse	• 208.91.198.143
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 208.91.199.225
	HcHimkU72e.exe	Get hash	malicious	Browse	• 208.91.199.224
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	• 208.91.199.225
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 208.91.199.224
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	Document14371.xls	Get hash	malicious	Browse	• 103.50.162.157
	Document14371.xls	Get hash	malicious	Browse	• 103.50.162.157
	AOBO MOULD QUOTATION -1752002.exe	Get hash	malicious	Browse	• 208.91.199.223
	JKG Eximcon Pvt. Ltd P.O.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Mal.Generic-S.15142.exe	Get hash	malicious	Browse	• 208.91.198.143
	smartandfinalTicket#51347303511505986.htm	Get hash	malicious	Browse	• 208.91.198.178
	f4b1bde3-706a-40d2-8ace-693803810b6f.exe	Get hash	malicious	Browse	• 103.53.43.36
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 208.91.199.223
PUBLIC-DOMAIN-REGISTRYUS	data.xls	Get hash	malicious	Browse	• 5.100.152.162
	Swift.jpg.exe	Get hash	malicious	Browse	• 208.91.198.143
	Claim-920537744-02082021.xls	Get hash	malicious	Browse	• 119.18.58.55
	Claim-920537744-02082021.xls	Get hash	malicious	Browse	• 119.18.58.55
	INVOICE-2101-0006N.exe	Get hash	malicious	Browse	• 208.91.199.224
	logs.php.dll	Get hash	malicious	Browse	• 116.206.105.72
	1344-21-03-00079 Q N QUEUE.exe	Get hash	malicious	Browse	• 208.91.198.143
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 208.91.199.225
	HcHimkU72e.exe	Get hash	malicious	Browse	• 208.91.199.224
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	• 208.91.199.225
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 208.91.199.224
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	Document14371.xls	Get hash	malicious	Browse	• 103.50.162.157
	Document14371.xls	Get hash	malicious	Browse	• 103.50.162.157
	AOBO MOULD QUOTATION -1752002.exe	Get hash	malicious	Browse	• 208.91.199.223
	JKG Eximcon Pvt. Ltd P.O.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Mal.Generic-S.15142.exe	Get hash	malicious	Browse	• 208.91.198.143
	smartandfinalTicket#51347303511505986.htm	Get hash	malicious	Browse	• 208.91.198.178
	f4b1bde3-706a-40d2-8ace-693803810b6f.exe	Get hash	malicious	Browse	• 103.53.43.36
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4019223246.exe.log

Process:	C:\Users\user\Desktop\4019223246.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4019223246.exe.log	
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp35E.tmp	
Process:	C:\Users\user\Desktop\4019223246.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.1910277324869165
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGAYtn:cbhK79lNQR/rydbz9l3YODOLNdq3G
MD5:	0436449A8A29D6DDCE3A32F0AFEC9F86
SHA1:	1BA25B0B13158E49344283743E476A5583B7110D
SHA-256:	274CF49E1C8DB4264092964FF5D604E47F20D0F93C5E4C62E4B728EBB8843506
SHA-512:	5DEFAA4B15AD8D4A7BCD2710381B82E9EFC68FC97BB1897BC96B3E4D3DE0227E57A98925D384B9182944C8738657C68533AB40B7CE01992E6094F9DDE91AC60
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\WZXjvtGBEKK.exe	
Process:	C:\Users\user\Desktop\4019223246.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	981504
Entropy (8bit):	7.118177937126348
Encrypted:	false
SSDEEP:	24576:CVsJT2fy3BWYR+nwvQILyPB+A+9JqWqi7jDB:ouB0wvngN+Dqg7
MD5:	87E6882BCEBF4823AFB4303AAC3628B1
SHA1:	FA6DF79DD667FCBB97C6FFBF947EE356512B292D
SHA-256:	369D92B64EE7B40F1679B98499E6D2B3470F9D477A8C35256508AE5715516194
SHA-512:	87F490512C0984C98EEDFAF34D97CF8FD7018A4ACE412DF73D61B1274034BCD87BC5B69956125687816AD77CF57951CA656608987233A79858BA0361A1F6890E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 9%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....r7`.....P.....T..... .....@.. .....`.....@.....K.....R.....@..... ....H.....text...$.... ....`.rsrc....R.....R.....@..@.reloc.....@.....@..B.....H.....8C...~.....8.....0..#.....+.&...(....(.....(.....o....*.....0..#.....+.&..8.....8.....+e..Ta.+...Pa...VXE.....@...M...]....T(.....+...QXE...'...;...D...R...a...j...s.....+..R(.....+.....&.U(.....+.8y.....(.....P(.....8e.....8\.....&...8N.....(.....8?.....86.....8-.....(....+.(....8.....8.....8.....(....+..8.....8....*..0.....+.&...+>..Sa.+...Oa8{.....VX

C:\Users\user\AppData\Roaming\WZXjvtGBEKK.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\4019223246.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621

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

C:\Users\user\AppData\Roaming\o20cyjeo.lhs\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\4019223246.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Windows\assembly\Desktop.ini	
Process:	C:\Users\user\Desktop\4019223246.exe
File Type:	Windows desktop.ini, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.2735028737400205
Encrypted:	false
SSDEEP:	6:a1eZBXVNYTF0NwoScUbtSgyAXIWv7v5PMKq:UeZBFNYTswUq1r5zq
MD5:	F7F759A5CD40BC52172E83486B6DE404
SHA1:	D74930F354A56CFD03DC91AA96D8AE9657B1EE54
SHA-256:	A709C2551B8818D7849D31A65446DC2F8C4CCA2DCBBC5385604286F49CFDAF1C
SHA-512:	A50B7826BFE72506019E4B1148A214C71C6F4743C09E809EF15CD0E0223F3078B683D203200910B07B5E1E34B94F0FE516AC53527311E2943654BFCEADE53298
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	; ==++==..; ..; Copyright (c) Microsoft Corporation. All rights reserved...; ..; ==--==..[.ShellClassInfo]..CLSID={1D2680C9-0E2A-469d-B787-065558BC7D43}..ConfirmFileOp=1..InfoTip=Contains application stability information...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.118177937126348
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	4019223246.exe

General

File size:	981504
MD5:	87e6882bcebf4823afb4303aac3628b1
SHA1:	fa6df79dd667fcbb97c6ffbf947ee356512b292d
SHA256:	369d92b64ee7b40f1679b98499e6d2b3470f9d477a8c352 56508ae5715516194
SHA512:	87f490512c0984c98eedfaf34d97cf8fd7018a4ace412df7 3d61b1274034bcd87bc5b69956125687816ad77cf57951 ca656608987233a79858ba0361a1f6890e
SSDEEP:	24576:CVsJT2fy3BWYR+nwvQILyPB+A+9JqWqi7jDB: ouB0wvngN+Dqg7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.... r7`.....P.....T..... .....@.. .....`..... ...@.....

File Icon

Icon Hash:	e0dad4adc4d2d870

Static PE Info

General

Entrypoint:	0x4ec21e
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:	0x603772F4 [Thu Feb 25 09:50:44 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 [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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xec1d0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xee000	0x5200	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf4000	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	0xea224	0xea400	False	0.631924526414	data	7.13411382713	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xee000	0x5200	0x5200	False	0.189738948171	data	4.23787907322	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf4000	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	0xee100	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xf2338	0x14	data		
RT_VERSION	0xf235c	0x350	data		
RT_MANIFEST	0xf26bc	0xb15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

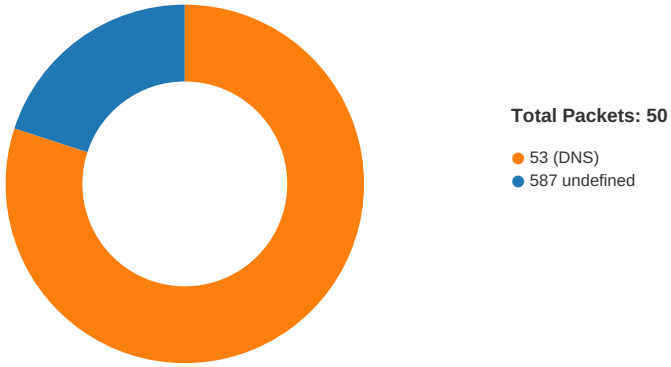
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	3.0.0.0

Description	Data
InternalName	ObjectIDGenerator.exe
FileVersion	3.0.0.0
CompanyName	KTV
LegalTrademarks	
Comments	
ProductName	KTVManagement
ProductVersion	3.0.0.0
FileDescription	KTVManagement
OriginalFilename	ObjectIDGenerator.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:17:51.331866026 CET	49767	587	192.168.2.4	208.91.198.143
Feb 25, 2021 12:17:51.509077072 CET	587	49767	208.91.198.143	192.168.2.4
Feb 25, 2021 12:17:51.509422064 CET	49767	587	192.168.2.4	208.91.198.143
Feb 25, 2021 12:17:51.700047016 CET	49767	587	192.168.2.4	208.91.198.143
Feb 25, 2021 12:17:51.875421047 CET	587	49767	208.91.198.143	192.168.2.4
Feb 25, 2021 12:17:52.132086992 CET	587	49767	208.91.198.143	192.168.2.4
Feb 25, 2021 12:17:52.133080959 CET	587	49767	208.91.198.143	192.168.2.4
Feb 25, 2021 12:17:52.133245945 CET	49767	587	192.168.2.4	208.91.198.143
Feb 25, 2021 12:17:52.136126041 CET	49767	587	192.168.2.4	208.91.198.143
Feb 25, 2021 12:17:52.172266960 CET	49769	587	192.168.2.4	208.91.199.224
Feb 25, 2021 12:17:52.347788095 CET	587	49769	208.91.199.224	192.168.2.4
Feb 25, 2021 12:17:52.347913027 CET	49769	587	192.168.2.4	208.91.199.224
Feb 25, 2021 12:17:52.556086063 CET	49769	587	192.168.2.4	208.91.199.224
Feb 25, 2021 12:17:52.732153893 CET	587	49769	208.91.199.224	192.168.2.4
Feb 25, 2021 12:17:52.903023958 CET	587	49769	208.91.199.224	192.168.2.4
Feb 25, 2021 12:17:52.903078079 CET	587	49769	208.91.199.224	192.168.2.4
Feb 25, 2021 12:17:52.903177977 CET	49769	587	192.168.2.4	208.91.199.224
Feb 25, 2021 12:17:52.903203964 CET	49769	587	192.168.2.4	208.91.199.224

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:16:08.954318047 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:09.016263008 CET	53	54531	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:09.560831070 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:09.628031015 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:09.943583012 CET	58028	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:16:09.992244005 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:10.898617983 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:10.948581934 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:11.871423006 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:11.920135975 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:13.275801897 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:13.327435017 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:14.433896065 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:14.495963097 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:17.263098001 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:17.316633940 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:21.227560043 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:21.276355982 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:22.460968971 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:22.521953106 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:25.565582037 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:25.615742922 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:26.567420006 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:26.619057894 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:27.530153036 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:27.578783035 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:28.491105080 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:28.539812088 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:29.634676933 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:29.683394909 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:30.969171047 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:31.034598112 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:32.470849037 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:32.519582987 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:34.405419111 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:34.457778931 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:35.373509884 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:35.422241926 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:39.010205030 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:39.063091993 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:44.146946907 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:44.210143089 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 12:16:59.515502930 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:16:59.578229904 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:00.533399105 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:00.591711044 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:01.171139956 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:01.229161024 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:01.658354998 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:01.672601938 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:01.715528011 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:01.743844986 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:02.226500988 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:02.275459051 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:02.812575102 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:02.874855042 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:03.473861933 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:03.531816006 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:03.868362904 CET	56448	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:03.917093992 CET	53	56448	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:04.346051931 CET	59172	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:04.395165920 CET	53	59172	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:05.323928118 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:05.385248899 CET	53	62420	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:06.007525921 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:06.066492081 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:14.653417110 CET	50183	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:14.704200983 CET	53	50183	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:14.856503963 CET	61531	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:17:14.932482958 CET	53	61531	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:17.254736900 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:17.315517902 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:51.249157906 CET	59794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:51.313503027 CET	53	59794	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:51.505810976 CET	55916	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:51.555139065 CET	53	55916	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:52.108124971 CET	52752	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:52.169742107 CET	53	52752	8.8.8.8	192.168.2.4
Feb 25, 2021 12:17:53.187391996 CET	60542	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:17:53.247427940 CET	53	60542	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 12:17:51.249157906 CET	192.168.2.4	8.8.8.8	0x224b	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Feb 25, 2021 12:17:52.108124971 CET	192.168.2.4	8.8.8.8	0x286d	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 12:17:51.313503027 CET	8.8.8.8	192.168.2.4	0x224b	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Feb 25, 2021 12:17:51.313503027 CET	8.8.8.8	192.168.2.4	0x224b	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Feb 25, 2021 12:17:51.313503027 CET	8.8.8.8	192.168.2.4	0x224b	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Feb 25, 2021 12:17:51.313503027 CET	8.8.8.8	192.168.2.4	0x224b	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Feb 25, 2021 12:17:52.169742107 CET	8.8.8.8	192.168.2.4	0x286d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Feb 25, 2021 12:17:52.169742107 CET	8.8.8.8	192.168.2.4	0x286d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Feb 25, 2021 12:17:52.169742107 CET	8.8.8.8	192.168.2.4	0x286d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Feb 25, 2021 12:17:52.169742107 CET	8.8.8.8	192.168.2.4	0x286d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

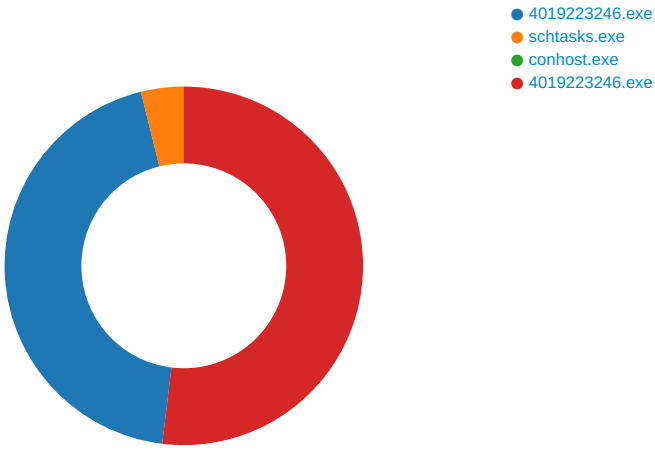
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 12:17:52.132086992 CET	587	49767	208.91.198.143	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Feb 25, 2021 12:17:52.903023958 CET	587	49769	208.91.199.224	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 4019223246.exe PID: 7056 Parent PID: 6020

General

Start time:	12:16:15
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\4019223246.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\4019223246.exe'
Imagebase:	0x850000
File size:	981504 bytes
MD5 hash:	87E6882BCEBF4823AFB4303AAC3628B1
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: 00000001.00000002.658750521.0000000002C95000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.658704693.0000000002C41000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WZXjvtGBEKK.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	6C1DDD66	CopyFileW
C:\Users\user\AppData\Roaming\WZXjvtGBEKK.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C1DDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp35E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C1D7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4019223246.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp35E.tmp	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WZXjvtGBEKK.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 f4 72 37 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 a4 0e 00 00 54 00 00 00 00 00 00 1e c2 0e 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 60 0f 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....r7`.......... ....P......T........... ........@.. .......................` ....@................	success or wait	4	6C1DDD66	CopyFileW
C:\Users\user\AppData\Roaming\WZXjvtGBEKK.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	6C1DDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp35E.tmp	unknown	1644	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 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4019223246.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: schtasks.exe PID: 5708 Parent PID: 7056

General

Start time:	12:16:19
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\WZXjvtGBEKK' /XML 'C:\Users\user\AppData\Local\Temp\tmp35E.tmp'
Imagebase:	0x970000
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\tmp35E.tmp	unknown	2	success or wait	1	97AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp35E.tmp	unknown	1645	success or wait	1	97ABD9	ReadFile

Analysis Process: conhost.exe PID: 3436 Parent PID: 5708

General

Start time:	12:16:19
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 4019223246.exe PID: 6104 Parent PID: 7056

General

Start time:	12:16:20
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\4019223246.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\4019223246.exe
Imagebase:	0x460000
File size:	981504 bytes
MD5 hash:	87E6882BCEBF4823AFB4303AAC3628B1
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: 00000004.00000002.913312856.0000000002ED4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.914172803.0000000003E21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.914560852.0000000004FE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.913196902.0000000002E21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.913196902.0000000002E21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.657508762.0000000000BE4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.912388878.00000000025A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.912715120.00000000029F0000.00000004.00000001.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	722760AC	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	722760AC	unknown
C:\Windows\assembly	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72521BEF	unknown
C:\Windows\assembly\Desktop.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72521BEF	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	722760AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming\o20cyjeo.lhs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	56637C1	CreateDirectoryW
C:\Users\user\AppData\Roaming\o20cyjeo.lhs\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	56637C1	CreateDirectoryW
C:\Users\user\AppData\Roaming\o20cyjeo.lhs\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	56637C1	CreateDirectoryW
C:\Users\user\AppData\Roaming\o20cyjeo.lhs\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	5663884	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\o20cyjeo.lhs\Chrome\Default\Cookies	success or wait	1	566393E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\assembly\Desktop.ini	unknown	227	3b 20 3d 3d 2b 2b 3d 3d 0d 0a 3b 20 0d 0a 3b 20 20 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 3b 20 0d 0a 3b 20 3d 3d 2d 2d 3d 3d 0d 0a 5b 2e 53 68 65 6c 6c 43 6c 61 73 73 49 6e 66 6f 5d 0d 0a 43 4c 53 49 44 3d 7b 31 44 32 36 38 30 43 39 2d 30 45 32 41 2d 34 36 39 64 2d 42 37 38 37 2d 30 36 35 35 35 38 42 43 37 44 34 33 7d 0d 0a 43 6f 6e 66 69 72 6d 46 69 6c 65 4f 70 3d 31 0d 0a 49 6e 66 6f 54 69 70 3d 43 6f 6e 74 61 69 6e 73 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 73 74 61 62 69 6c 69 74 79 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 0d 0a	; ==++==..; ..; Copyright (c) Microsoft Corporation. All rights reserved...; ..; ==--==.. [.ShellClassInfo]..CLSID={1D2680C9-0E2A-469d-B787-065558BC7D43}..ConfirmFileOp=1..InfoTip=Contains application stability information...	success or wait	1	72521BEF	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\o20cyjeo.lhs\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	5663884	CopyFileW

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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5661633	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\dc6ff561-03ad-4f47-bfdf-3f554e3ff9ba	unknown	4096	success or wait	1	5661633	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5661633	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5661633	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5661633	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5661633	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5661633	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5661633	ReadFile
C:\Users\user\AppData\Roaming\o20cyjeo.lhs\Chrome\Default\Cookies	unknown	16384	success or wait	2	5661633	ReadFile

Disassembly

Code Analysis