ID: 339079
Sample Name: Statement of Account.exe
Cookbook: default.jbs
Time: 13:16:08
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

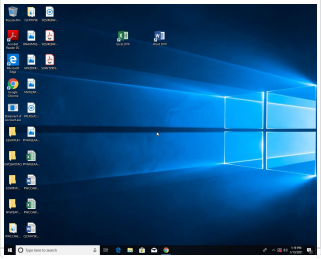
Analysis Report Statement of Account.exe

Overview

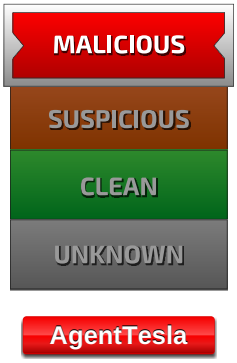
General Information

Sample Name:	Statement of Account.exe
Analysis ID:	339079
MD5:	8d7144cdca415d..
SHA1:	7a37f9f07287088..
SHA256:	fa769a960a22d4c.
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

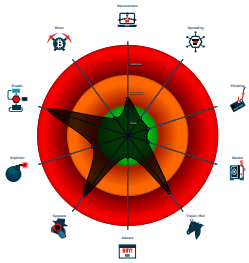


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: MSBuild connects …
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- Statement of Account.exe (PID: 3980 cmdline: 'C:\Users\user\Desktop\Statement of Account.exe' MD5: 8D7144CDCA415DBDF39548D460A8866B)
  - schtasks.exe (PID: 4640 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eRwRffX' /XML 'C:\Users\user\AppData\Local\Temp\tmpBACF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 5456 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "yJr2pyY5i7vE9",
  "URL: ": "http://cV9LNZgDQeR7CK6z.org",
  "To: ": "sales2@chestronic.com",
  "ByHost: ": "mail.chestronic.com:587",
  "Password: ": "d4aqvGyl40aQf",
  "From: ": "sales2@chestronic.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.230197757.0000000003B5F000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.570956453.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.227700296.0000000002B0 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

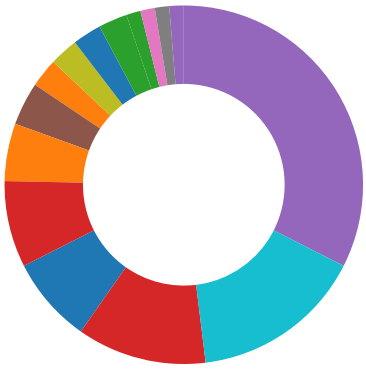
Sigma Overview

System Summary:

Sigma detected: MSBuild connects to smtp port

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- 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

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Writes to foreign memory regions

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:

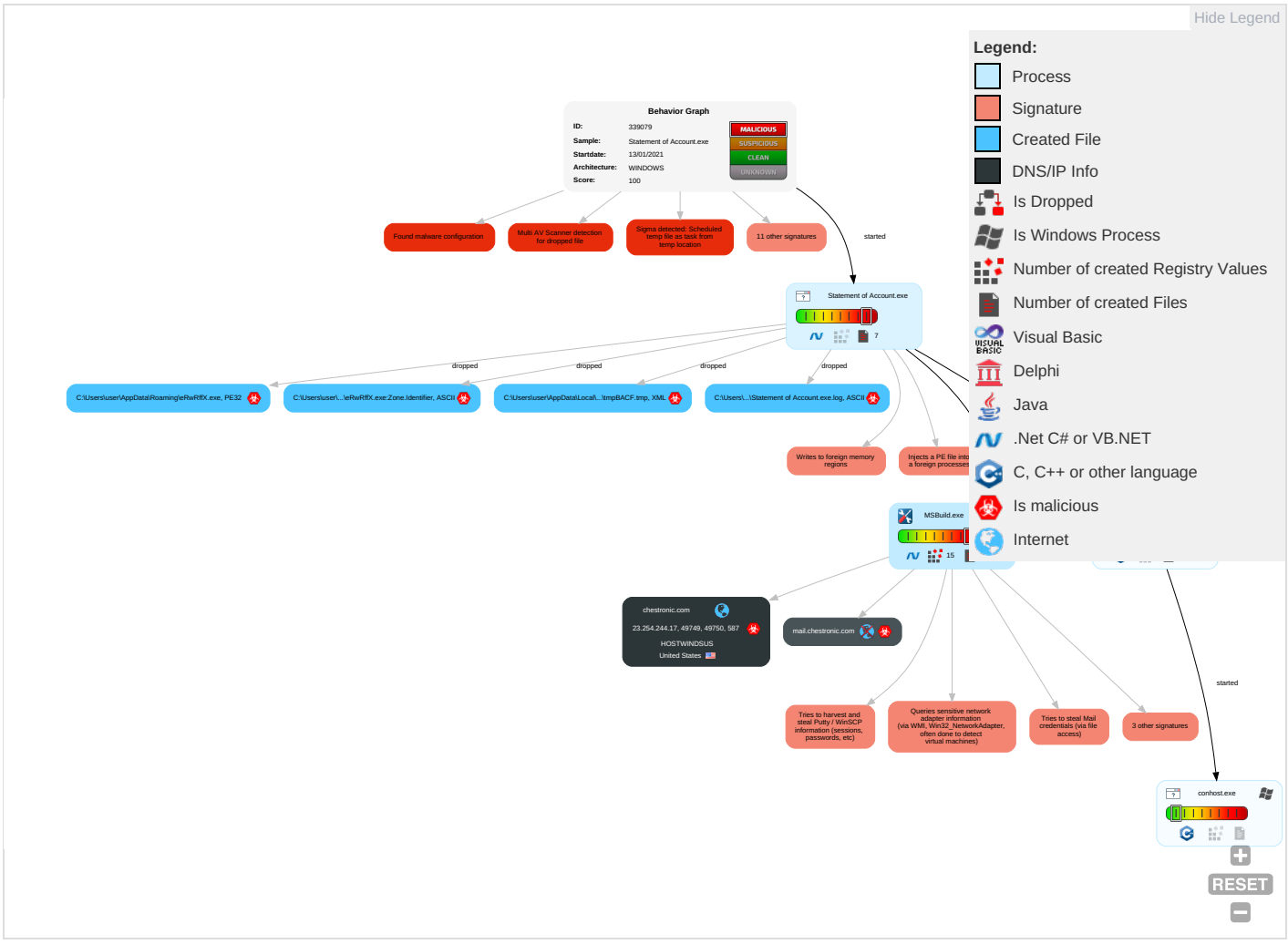
Yara detected AgentTesla

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	Process Injection 2 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	Encrypted Channel 1 2
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 2	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
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	Multiband Communicatio

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Us 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	Application La Protocol

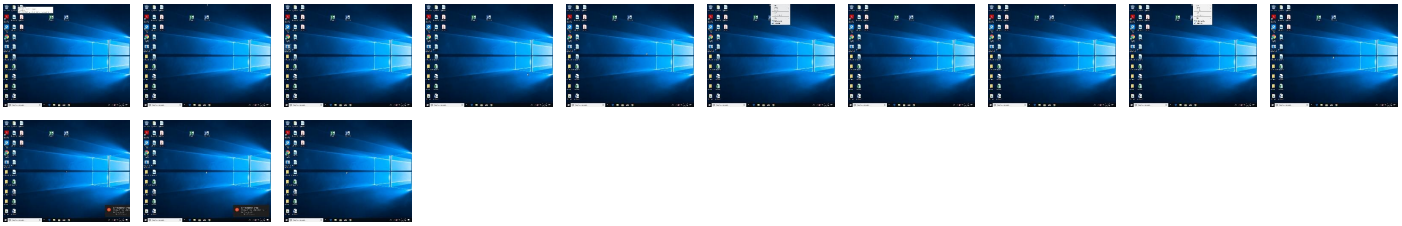
Behavior Graph



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
Statement of Account.exe	25%	Virustotal		Browse
Statement of Account.exe	11%	ReversingLabs	Win32.Trojan.Wacatac	
Statement of Account.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eRwRffX.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\eRwRffX.exe	11%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://sjSmfS.com	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://chestronic.com	0%	Avira URL Cloud	safe	
http://cV9LNZgDQeR7CK6z.org	0%	Avira URL Cloud	safe	
http://mail.chestronic.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chestronic.com	23.254.244.17	true	true		unknown
mail.chestronic.com	unknown	unknown	true		unknown

Contacted URLs

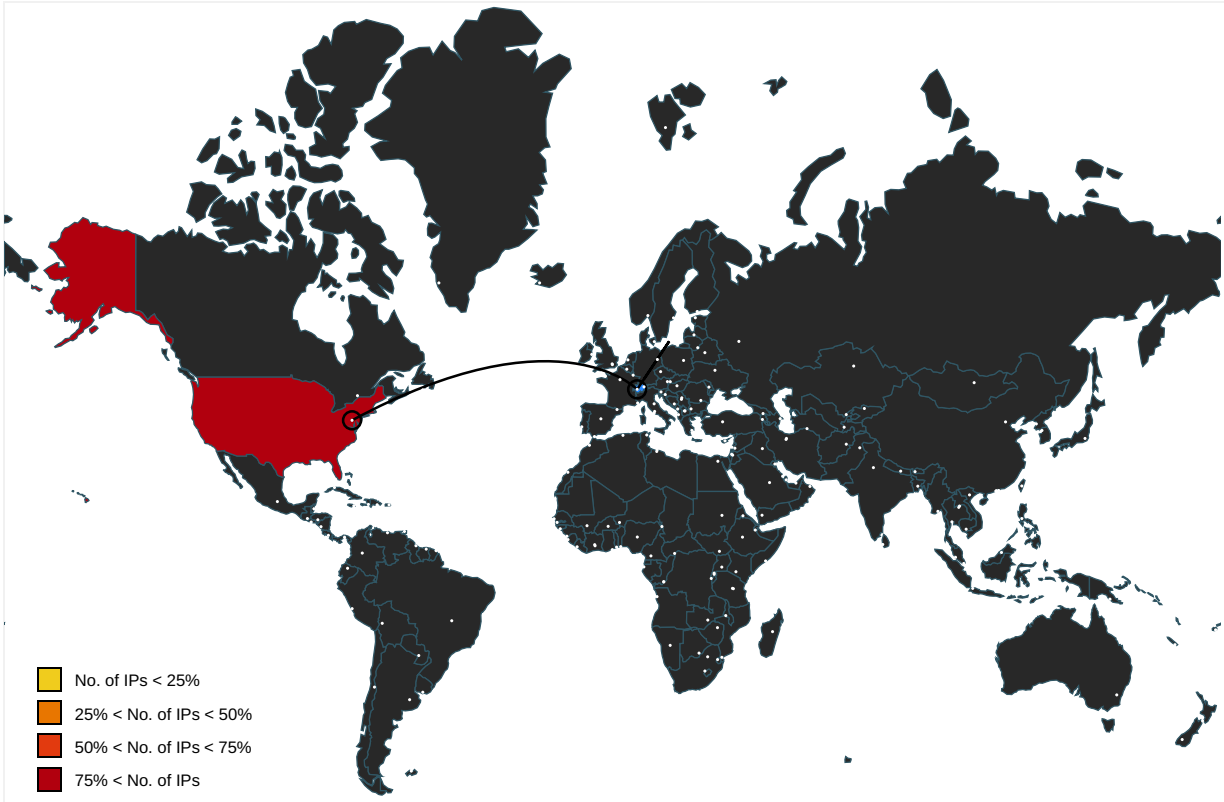
Name	Malicious	Antivirus Detection	Reputation
http://cV9LNZgDQeR7CK6z.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	MSBuild.exe, 00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	MSBuild.exe, 00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org	MSBuild.exe, 00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	MSBuild.exe, 00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	MSBuild.exe, 00000003.00000002.578757614.00000000036D8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sjSmfS.com	MSBuild.exe, 00000003.00000002.575561117.0000000003401000.00000004.00000001.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	MSBuild.exe, 00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	Statement of Account.exe, 00000000.00000002.230197757.0000000003B5F000.00000004.00000001.sdmp, MSBuild.exe, 00000003.00000002.570956453.0000000000402000.00000040.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://chestronic.com	MSBuild.exe, 00000003.00000002.578692738.00000000036D2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.chestronic.com	MSBuild.exe, 00000003.00000002.578692738.00000000036D2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Statement of Account.exe, 00000000.00000002.227700296.0000000002B01000.00000004.00000001.sdmp, MSBuild.exe, 00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	MSBuild.exe, 00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Statement of Account.exe, 00000000.00000002.230197757.0000000003B5F000.00000004.00000001.sdmp, MSBuild.exe, 00000003.00000002.570956453.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	MSBuild.exe, 00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.254.244.17	unknown	United States		54290	HOSTWINDSUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339079
Start date:	13.01.2021
Start time:	13:16:08

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Statement of Account.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:	33
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:	Failed
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, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 13.88.21.125, 51.104.139.180, 23.210.248.85, 92.122.213.194, 92.122.213.247, 20.54.26.129, 93.184.221.240, 51.103.5.186, 51.11.168.160, 40.88.32.150, 168.61.161.212, 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, par02p.wns.notify.windows.com.akadns.net, skypedataprdcoleus15.cloudapp.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, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:17:06	API Interceptor	1x Sleep call for process: Statement of Account.exe modified
13:17:22	API Interceptor	1109x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.254.244.17	4600031748.exe	Get hash	malicious	Browse	
	4600031748.exe	Get hash	malicious	Browse	
	scan copy-001.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	Transfer Form.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Transfer Form.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	PO.423pdf.exe	Get hash	malicious	Browse	
	PO.423pdf.exe	Get hash	malicious	Browse	
	032021CITAR.exe	Get hash	malicious	Browse	
	AGROMAR#U00a0PROFORMA.exe	Get hash	malicious	Browse	
	AGROMAR#U00a0PROFORMA.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	Hydraulex.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTWINDSUS	4600031748.exe	Get hash	malicious	Browse	• 23.254.244.17
	1gEpBw4A95.exe	Get hash	malicious	Browse	• 23.254.224.2
	4600031748.exe	Get hash	malicious	Browse	• 23.254.244.17
	scan copy-001.exe	Get hash	malicious	Browse	• 23.254.244.17
	SOA.exe	Get hash	malicious	Browse	• 23.254.244.17
	Z8363664.doc	Get hash	malicious	Browse	• 104.168.154.203
	Transfer Form.exe	Get hash	malicious	Browse	• 23.254.244.17
	Transfer Form.exe	Get hash	malicious	Browse	• 23.254.244.17
	jfuoevj.exe	Get hash	malicious	Browse	• 192.119.111.137
	SOA.exe	Get hash	malicious	Browse	• 23.254.244.17
	SOA.exe	Get hash	malicious	Browse	• 23.254.244.17
	zsmcirs.exe	Get hash	malicious	Browse	• 192.119.111.137
	REP er0005147.doc	Get hash	malicious	Browse	• 104.168.154.203
	PO.423pdf.exe	Get hash	malicious	Browse	• 23.254.244.17
	PO.423pdf.exe	Get hash	malicious	Browse	• 23.254.244.17
	032021CITAR.exe	Get hash	malicious	Browse	• 23.254.244.17
	http://chr-cssnf.ga/?login=do	Get hash	malicious	Browse	• 104.168.136.235
	utr63q.vbs	Get hash	malicious	Browse	• 104.168.204.195
	NaTdOM3rA7.exe	Get hash	malicious	Browse	• 198.44.97.180
	k8Jw01YX3c.exe	Get hash	malicious	Browse	• 192.119.110.12

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Statement of Account.exe.log	
Process:	C:\Users\user\Desktop\Statement of Account.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Statement of Account.exe.log	
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\tmpBACF.tmp	
Process:	C:\Users\user\Desktop\Statement of Account.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.186147810066712
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBltn:cbh47TlNQ//rydbz9I3YODOLNdq3Z
MD5:	007C0FA4B0C756852145C60F6E025A6D
SHA1:	AD817895DFBD7C83F762C14C328DB07FDAF66301
SHA-256:	CB6D3D6C38C318AFE9F3E4A9565132F3A7DB86BA8F1978A873A596B1A62E6649
SHA-512:	C7AE152687F473E84F10122C7615794D59AE258ADCC4D2B209760FF86189EEDD7AF55EDE3856648BA80D3779EAD772DD6A2606FEB50B457C80311AE9F8DBBC1
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\eRwRffX.exe	
Process:	C:\Users\user\Desktop\Statement of Account.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	827392
Entropy (8bit):	7.28144235904361
Encrypted:	false
SSDEEP:	12288:cRQgp43cnZDfBQjFX9rfFHzM3bRwjLYPBoER6Ddm:A4sZLBQjd3zM3aYpo3Jm
MD5:	8D7144CDCA415DBDF39548D460A8866B
SHA1:	7A37F9F07287088112354370 69FB74579548F758
SHA-256:	FA769A960A22D4CE289DA152E5535FA6F9E610D8796AEB907BACF3157C1270B5
SHA-512:	955AE6FCD4BD5F77A5EA376FBBF7827315BAF73BDFCEFB5F519944398DCB700EA9F22218176624D89F0FD523FF34DCCCCAD4139E1C8E6142D1F295E0F67498
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 11%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P..... .....@.. ..... .@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....<X.....(....*&..(....*.s .....s!.....s".....s#.....s$.....*...0.....~....o%....+..*.0.....~....o&. ...+..*.0.....~....o'....+..*.0.....~....o(....+..*.0.....~....o)....+..*&..(*....*...0..<.....~.....(+.....,!r...p.....(,...o-...s.....~.....+..*.0.....~.....+..*".....*.0.....(....r=..p ~....o/....+..*...0..<.....~.....(+.....,!rG..p.....(,

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

C:\Users\user\AppData\Roaming\eRwRffX.exe:Zone.Identifier	
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\sh0vu41c.d1k\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.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..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.28144235904361
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Statement of Account.exe
File size:	827392
MD5:	8d7144cdca415dbdf39548d460a8866b
SHA1:	7a37f9f07287088112354 37d69fb74579548f758
SHA256:	fa769a960a22d4ce289da152e5535fa6f9e610d8796aeb907bacf3157c1270b5
SHA512:	955ae6fcd4bd5f77a5ea376fbbf7827315baf73bdfcefb5f519944398dcb700ea9f22218176624d89f0fd523ff34dcccc ad4139e1c8e6142d1f295e0f67498f0
SSDEEP:	12288:cRQgp43cnZDfBQjFX9rfFHzM3bRwjLYPBoER6Ddm:A4sZLBQjd3zM3aYpo3Jm
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... _.....P..... .....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4cb40e
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:	0x5FFEB9F0 [Wed Jan 13 09:14:24 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcb3bc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xcc000	0x5cc	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xce000	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	0xc9414	0xc9600	False	0.691340782123	data	7.28753546565	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xcc000	0x5cc	0x600	False	0.419270833333	data	4.11955969192	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xcc090	0x33c	data		
RT_MANIFEST	0xcc3dc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

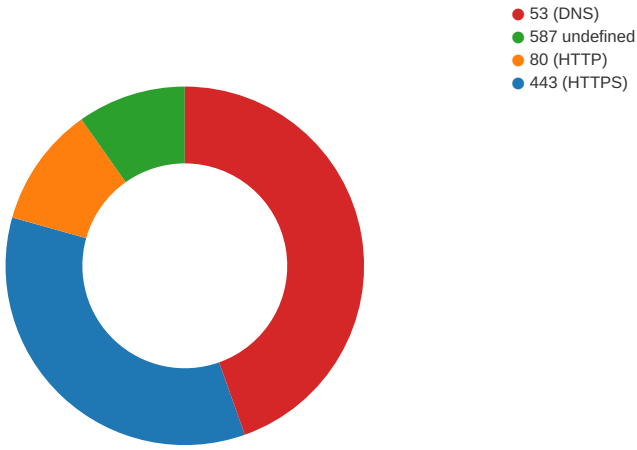
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2011
Assembly Version	1.0.0.0
InternalName	SessionInfo.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	FileReplacement
ProductVersion	1.0.0.0
FileDescription	FileReplacement
OriginalFilename	SessionInfo.exe

Network Behavior

Network Port Distribution

Total Packets: 92



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:17:22.329139948 CET	49693	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.332210064 CET	49693	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.344530106 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.392551899 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.406025887 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.406214952 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.406900883 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.424411058 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.470793009 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.470844984 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.470884085 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.470906973 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.470921040 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.471004009 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.475728989 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.536870003 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.536914110 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.536952019 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.536983967 CET	49693	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.537019968 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.537056923 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.537074089 CET	49693	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.537096024 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.537137032 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.537151098 CET	49693	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.537184000 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.537223101 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.537247896 CET	49693	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.537739038 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.538515091 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.538587093 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.600013971 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.600058079 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.747093916 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.747150898 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.747188091 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.747246027 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.747263908 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.747303009 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.747317076 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.747339964 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.747378111 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.747387886 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.747414112 CET	443	49714	20.190.129.2	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:17:22.747459888 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:17:22.747476101 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.759885073 CET	49693	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:22.822376966 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:17:43.929927111 CET	80	49680	93.184.220.29	192.168.2.3
Jan 13, 2021 13:17:43.930327892 CET	49680	80	192.168.2.3	93.184.220.29
Jan 13, 2021 13:17:44.043482065 CET	49683	80	192.168.2.3	93.184.220.29
Jan 13, 2021 13:17:44.083384037 CET	80	49683	93.184.220.29	192.168.2.3
Jan 13, 2021 13:17:44.083514929 CET	49683	80	192.168.2.3	93.184.220.29
Jan 13, 2021 13:17:44.590485096 CET	49689	80	192.168.2.3	84.53.167.113
Jan 13, 2021 13:17:44.590569973 CET	49688	443	192.168.2.3	2.17.179.193
Jan 13, 2021 13:17:44.630980015 CET	80	49689	84.53.167.113	192.168.2.3
Jan 13, 2021 13:17:44.631040096 CET	443	49688	2.17.179.193	192.168.2.3
Jan 13, 2021 13:17:44.631072998 CET	443	49688	2.17.179.193	192.168.2.3
Jan 13, 2021 13:17:44.631072998 CET	49689	80	192.168.2.3	84.53.167.113
Jan 13, 2021 13:17:44.631131887 CET	49688	443	192.168.2.3	2.17.179.193
Jan 13, 2021 13:17:44.631175041 CET	49688	443	192.168.2.3	2.17.179.193
Jan 13, 2021 13:17:46.267443895 CET	49696	443	192.168.2.3	23.210.249.50
Jan 13, 2021 13:17:46.267637014 CET	49697	80	192.168.2.3	93.184.220.29
Jan 13, 2021 13:17:46.280858040 CET	80	49692	93.184.220.29	192.168.2.3
Jan 13, 2021 13:17:46.281016111 CET	49692	80	192.168.2.3	93.184.220.29
Jan 13, 2021 13:17:48.646560907 CET	49707	443	192.168.2.3	204.79.197.200
Jan 13, 2021 13:17:48.646626949 CET	49708	443	192.168.2.3	204.79.197.200
Jan 13, 2021 13:18:33.203876019 CET	49680	80	192.168.2.3	93.184.220.29
Jan 13, 2021 13:18:33.203952074 CET	49698	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:18:33.235389948 CET	49693	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:18:33.235456944 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:18:33.244103909 CET	80	49680	93.184.220.29	192.168.2.3
Jan 13, 2021 13:18:33.244350910 CET	49680	80	192.168.2.3	93.184.220.29
Jan 13, 2021 13:18:33.265650988 CET	443	49698	20.190.129.2	192.168.2.3
Jan 13, 2021 13:18:33.265834093 CET	49698	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:18:33.295329094 CET	443	49693	20.190.129.2	192.168.2.3
Jan 13, 2021 13:18:33.295591116 CET	49693	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:18:33.296845913 CET	443	49714	20.190.129.2	192.168.2.3
Jan 13, 2021 13:18:33.297058105 CET	49714	443	192.168.2.3	20.190.129.2
Jan 13, 2021 13:18:47.720607042 CET	80	49692	93.184.220.29	192.168.2.3
Jan 13, 2021 13:18:47.720715046 CET	49692	80	192.168.2.3	93.184.220.29
Jan 13, 2021 13:18:49.084397078 CET	49749	587	192.168.2.3	23.254.244.17
Jan 13, 2021 13:18:49.261193991 CET	587	49749	23.254.244.17	192.168.2.3
Jan 13, 2021 13:18:49.261331081 CET	49749	587	192.168.2.3	23.254.244.17
Jan 13, 2021 13:18:49.629069090 CET	587	49749	23.254.244.17	192.168.2.3
Jan 13, 2021 13:18:49.629375935 CET	49749	587	192.168.2.3	23.254.244.17
Jan 13, 2021 13:18:49.800765991 CET	587	49749	23.254.244.17	192.168.2.3
Jan 13, 2021 13:18:49.801074982 CET	49749	587	192.168.2.3	23.254.244.17
Jan 13, 2021 13:18:49.978652954 CET	587	49749	23.254.244.17	192.168.2.3
Jan 13, 2021 13:18:50.032744884 CET	49749	587	192.168.2.3	23.254.244.17
Jan 13, 2021 13:18:50.041479111 CET	49749	587	192.168.2.3	23.254.244.17
Jan 13, 2021 13:18:50.226382017 CET	587	49749	23.254.244.17	192.168.2.3
Jan 13, 2021 13:18:50.226447105 CET	587	49749	23.254.244.17	192.168.2.3
Jan 13, 2021 13:18:50.226488113 CET	587	49749	23.254.244.17	192.168.2.3
Jan 13, 2021 13:18:50.226519108 CET	587	49749	23.254.244.17	192.168.2.3
Jan 13, 2021 13:18:50.226517916 CET	49749	587	192.168.2.3	23.254.244.17
Jan 13, 2021 13:18:50.226571083 CET	49749	587	192.168.2.3	23.254.244.17
Jan 13, 2021 13:18:50.230479956 CET	587	49749	23.254.244.17	192.168.2.3
Jan 13, 2021 13:18:50.259190083 CET	49749	587	192.168.2.3	23.254.244.17
Jan 13, 2021 13:18:50.433252096 CET	587	49749	23.254.244.17	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:17:15.235147953 CET	60152	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:15.283096075 CET	53	60152	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:17.794472933 CET	57544	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:17.851032972 CET	53	57544	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:17:21.795707941 CET	55984	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:21.846538067 CET	53	55984	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:23.372314930 CET	64185	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:23.420351982 CET	53	64185	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:25.096415997 CET	65110	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:25.144617081 CET	53	65110	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:25.713126898 CET	58361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:25.769495964 CET	53	58361	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:26.364336967 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:26.415071964 CET	53	63492	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:29.223328114 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:29.284353018 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:36.062458992 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:36.113209963 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:38.070696115 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:38.118870974 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:39.373505116 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:39.424463034 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:39.559889078 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:39.624552011 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:40.635224104 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:40.683197975 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:41.903990984 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:41.952049971 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:44.475142002 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:44.531775951 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:45.342811108 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:45.434134007 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:47.258168936 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:47.306293964 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:50.283185005 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:50.339901924 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:52.749754906 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:52.800834894 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:57.024214983 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:57.072196007 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 13:17:57.860409975 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:17:57.908476114 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:22.762449980 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:22.810399055 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:23.612066984 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:23.660207987 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:24.486335039 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:24.537156105 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:24.968077898 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:25.042423010 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:25.404375076 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:25.452408075 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:26.290127039 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:26.338430882 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:48.603116035 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:48.785650015 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:48.798002005 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:48.829895020 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:48.877932072 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:48.983237982 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:53.368350983 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:53.424547911 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 13:18:53.433990955 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:18:53.495500088 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 13:19:42.402489901 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:19:42.459256887 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 13:19:43.190722942 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:19:43.249910116 CET	53	52123	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:19:44.091826916 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:19:44.144438028 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 13:19:44.714895010 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:19:44.763113976 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 13:19:45.374547005 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:19:45.431186914 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 13:19:46.206428051 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:19:46.264622927 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 13:19:46.855021954 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:19:46.902925968 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 13:19:48.015754938 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:19:48.066567898 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 13:19:48.738970041 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 13:19:48.786906004 CET	53	55708	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 13:18:48.603116035 CET	192.168.2.3	8.8.8.8	0xabe6	Standard query (0)	mail.chestronic.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:18:48.798002005 CET	192.168.2.3	8.8.8.8	0xf37	Standard query (0)	mail.chestronic.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:18:53.368350983 CET	192.168.2.3	8.8.8.8	0x924d	Standard query (0)	mail.chestronic.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:18:53.433990955 CET	192.168.2.3	8.8.8.8	0x1b24	Standard query (0)	mail.chestronic.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 13:18:48.785650015 CET	8.8.8.8	192.168.2.3	0xabe6	No error (0)	mail.chestronic.com	chestronic.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:18:48.785650015 CET	8.8.8.8	192.168.2.3	0xabe6	No error (0)	chestronic.com		23.254.244.17	A (IP address)	IN (0x0001)
Jan 13, 2021 13:18:48.983237982 CET	8.8.8.8	192.168.2.3	0xf37	No error (0)	mail.chestronic.com	chestronic.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:18:48.983237982 CET	8.8.8.8	192.168.2.3	0xf37	No error (0)	chestronic.com		23.254.244.17	A (IP address)	IN (0x0001)
Jan 13, 2021 13:18:53.424547911 CET	8.8.8.8	192.168.2.3	0x924d	No error (0)	mail.chestronic.com	chestronic.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:18:53.424547911 CET	8.8.8.8	192.168.2.3	0x924d	No error (0)	chestronic.com		23.254.244.17	A (IP address)	IN (0x0001)
Jan 13, 2021 13:18:53.495500088 CET	8.8.8.8	192.168.2.3	0x1b24	No error (0)	mail.chestronic.com	chestronic.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:18:53.495500088 CET	8.8.8.8	192.168.2.3	0x1b24	No error (0)	chestronic.com		23.254.244.17	A (IP address)	IN (0x0001)

SMTP Packets

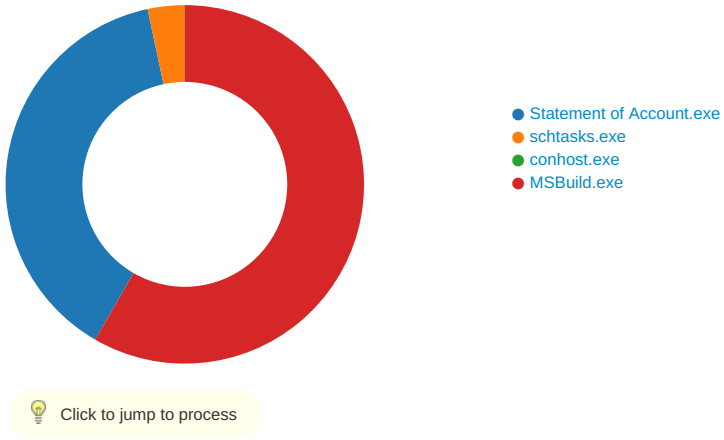
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 13:18:49.629069090 CET	587	49749	23.254.244.17	192.168.2.3	220-dal-shared-36.hostwindsdns.com ESMTP Exim 4.93 #2 Wed, 13 Jan 2021 04:18:49 -0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 13, 2021 13:18:49.629375935 CET	49749	587	192.168.2.3	23.254.244.17	EHLO 124406
Jan 13, 2021 13:18:49.800765991 CET	587	49749	23.254.244.17	192.168.2.3	250-dal-shared-36.hostwindsdns.com Hello 124406 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Jan 13, 2021 13:18:49.801074982 CET	49749	587	192.168.2.3	23.254.244.17	STARTTLS
Jan 13, 2021 13:18:49.978652954 CET	587	49749	23.254.244.17	192.168.2.3	220 TLS go ahead

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 13:18:53.852014065 CET	587	49750	23.254.244.17	192.168.2.3	220-dal-shared-36.hostwindsdns.com ESMTP Exim 4.93 #2 Wed, 13 Jan 2021 04:18:53 -0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 13, 2021 13:18:53.852494001 CET	49750	587	192.168.2.3	23.254.244.17	EHLO 124406
Jan 13, 2021 13:18:54.028196096 CET	587	49750	23.254.244.17	192.168.2.3	250-dal-shared-36.hostwindsdns.com Hello 124406 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Jan 13, 2021 13:18:54.028923035 CET	49750	587	192.168.2.3	23.254.244.17	STARTTLS
Jan 13, 2021 13:18:54.207133055 CET	587	49750	23.254.244.17	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Statement of Account.exe PID: 3980 Parent PID: 5596

General

Start time:	13:17:00
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Statement of Account.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Statement of Account.exe'
Imagebase:	0x5e0000
File size:	827392 bytes
MD5 hash:	8D7144CDCA415DBDF39548D460A8866B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.230197757.0000000003B5F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.227700296.0000000002B01000.00000004.00000001.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	6DEECF06	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	6DEECF06	unknown
C:\Users\user\AppData\Roaming\eRwRffX.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	6CD3DD66	CopyFileW
C:\Users\user\AppData\Roaming\eRwRffX.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD3DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpBACF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD37038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Statement of Account.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBACF.tmp	success or wait	1	6CD36A95	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\eRwRffX.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 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 f0 b9 fe 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 96 0c 00 00 08 00 00 00 00 00 00 0e b4 0c 00 00 20 00 00 00 c0 0c 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 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	6CD3DD66	CopyFileW
C:\Users\user\AppData\Roaming\eRwRffX.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	6CD3DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpBACF.tmp	unknown	1640	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.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	6CD31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Statement of Account.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	6E1FC907	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: schtasks.exe PID: 4640 Parent PID: 3980

General

Start time:	13:17:07
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eRwRffX' /XML 'C:\Users\user\AppData\Local\Temp\tmpBACF.tmp'
Imagebase:	0x330000
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\tmpBACF.tmp	unknown	2	success or wait	1	33AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBACF.tmp	unknown	1641	success or wait	1	33ABD9	ReadFile

Analysis Process: conhost.exe PID: 4272 Parent PID: 4640

General

Start time:	13:17:07
Start date:	13/01/2021
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: MSBuild.exe PID: 5456 Parent PID: 3980

General

Start time:	13:17:08
Start date:	13/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0x7ff7488e0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.575561117.0000000003401000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.570956453.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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	6DEECF06	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	6DEECF06	unknown
C:\Users\user\AppData\Roaming\sh0vu41c.d1k	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\sh0vu41c.d1k\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	6CD3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\sh0vu41c.d1k\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	6CD3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\sh0vu41c.d1k\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	6CD3DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sh0vu41c.d1k\Chrome\Default\Cookies	success or wait	1	6CD36A95	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\sh0vu41c.d1k\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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CD3DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6DECCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6DEC5705	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d39db4d7-5fed-4bb0-9238-1671503b50f4	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Roaming\sh0vu41c.d1k\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CD31B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis