ID: 383916
Sample Name:
TRENWATR.EXE
Cookbook: default.jbs
Time: 12:22:43
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

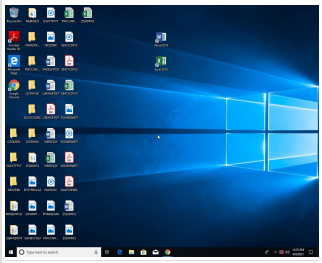
Analysis Report TRENWATR.EXE

Overview

General Information

Sample Name:	TRENWATR.EXE
Analysis ID:	383916
MD5:	4c8c4125a16387..
SHA1:	a550ec500bfa00f..
SHA256:	5aaae83a4b166e..
Tags:	AgentTesla EXE
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

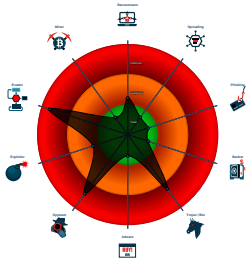
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Moves itself to temp directory
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- TRENWATR.EXE (PID: 1048 cmdline: 'C:\Users\user\Desktop\TRENWATR.EXE' MD5: 4C8C4125A16387F16558E841A704C718)
  - TRENWATR.EXE (PID: 3336 cmdline: C:\Users\user\Desktop\TRENWATR.EXE MD5: 4C8C4125A16387F16558E841A704C718)
- outlook.exe (PID: 6696 cmdline: 'C:\Users\user\AppData\Roaming\outlook\outlook.exe' MD5: 4C8C4125A16387F16558E841A704C718)
  - outlook.exe (PID: 6944 cmdline: C:\Users\user\AppData\Roaming\outlook\outlook.exe MD5: 4C8C4125A16387F16558E841A704C718)
- outlook.exe (PID: 6904 cmdline: 'C:\Users\user\AppData\Roaming\outlook\outlook.exe' MD5: 4C8C4125A16387F16558E841A704C718)
  - outlook.exe (PID: 7012 cmdline: C:\Users\user\AppData\Roaming\outlook\outlook.exe MD5: 4C8C4125A16387F16558E841A704C718)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "datastore1840@yandex.comopjis0123smtp.yandex.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.360720856.0000000002EE0000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.495941887.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.375859880.0000000000429C000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000016.00000002.496146481.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000015.00000002.377800877.000000000290 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 25 entries				

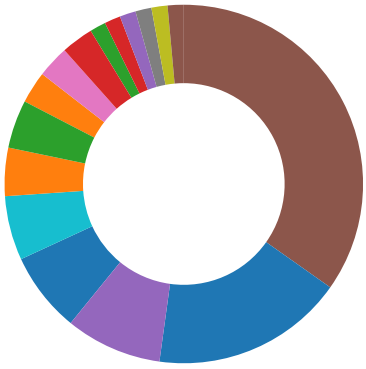
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.TRENWATR.EXE.3ff53d8.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
20.2.outlook.exe.44d1fe8.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.outlook.exe.40d1fe8.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
21.2.outlook.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.outlook.exe.3fa53d8.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Moves itself to temp directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

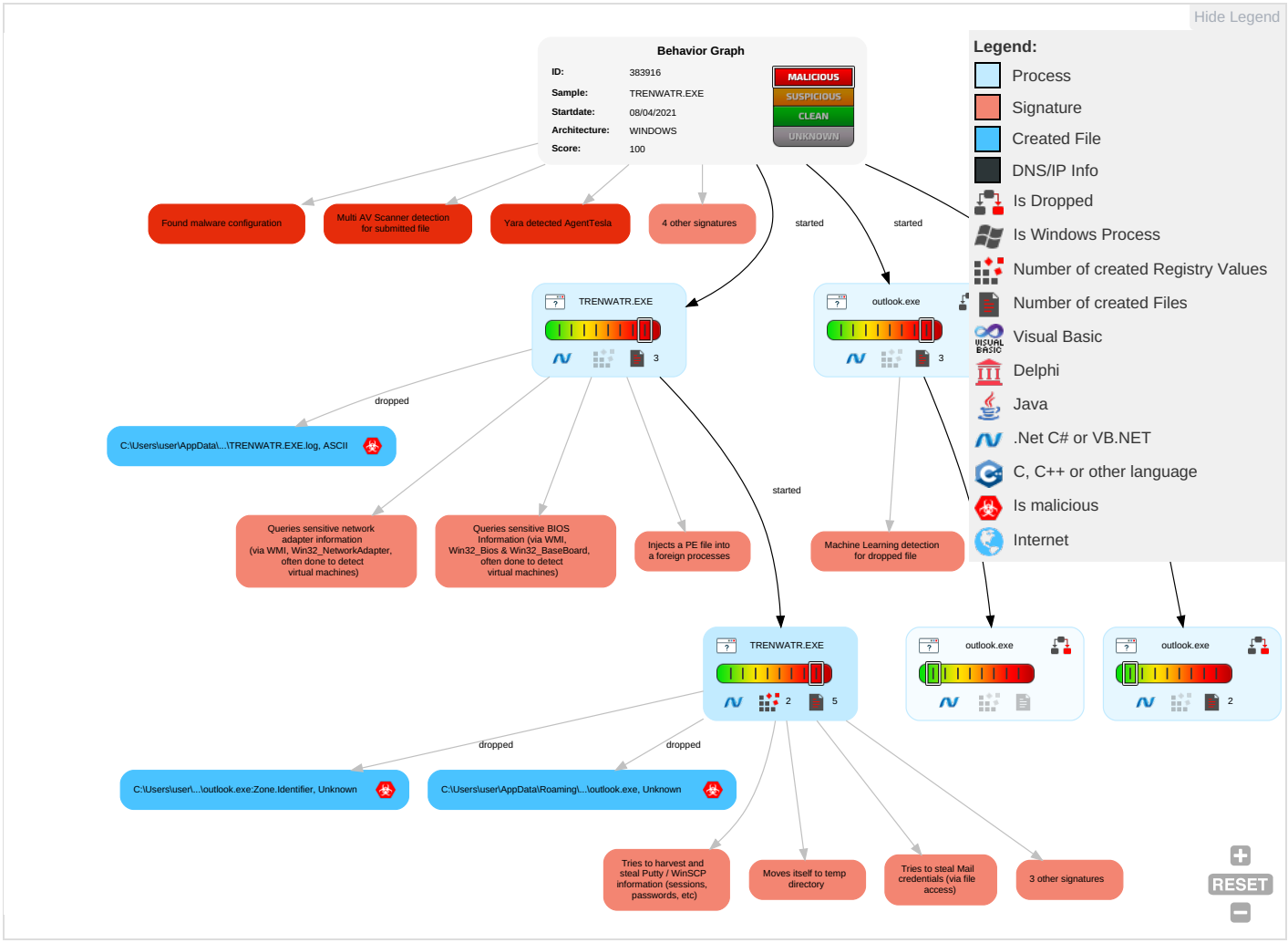
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Masquerading 1 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	Input Capture 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Credentials in Registry 1	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Steganograph
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

Copyright Joe Security LLC 2021

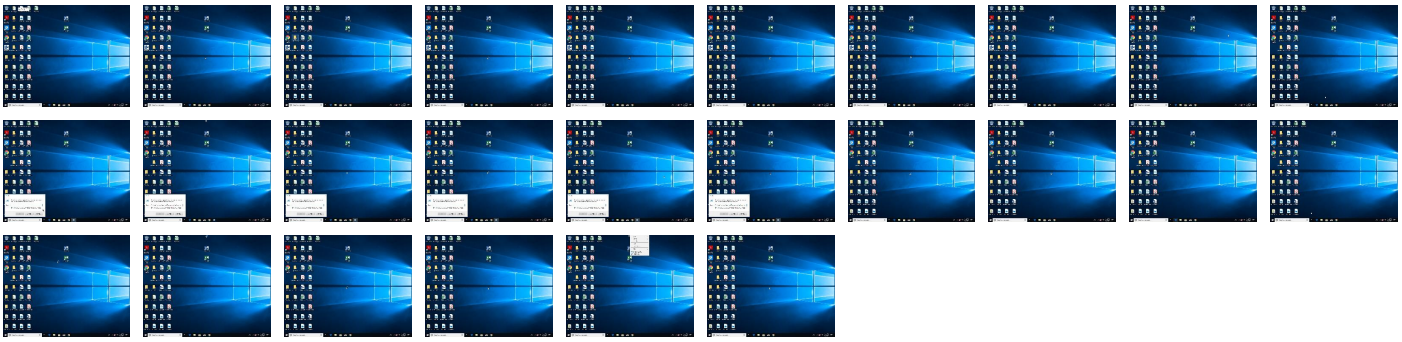
Behavior Graph



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
TRENWATR.EXE	16%	Virustotal		Browse
TRENWATR.EXE	15%	ReversingLabs	Win32.Trojan.Wacatac	
TRENWATR.EXE	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\outlook\outlook.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.2.outlook.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.2.outlook.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.TRENWATR.EXE.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comB.TTFG	0%	Avira URL Cloud	safe	
http://www.carterandcone.comes	0%	URL Reputation	safe	
http://www.carterandcone.comes	0%	URL Reputation	safe	
http://www.carterandcone.comes	0%	URL Reputation	safe	
http://www.carterandcone.comes	0%	URL Reputation	safe	
http://www.founder.com.cn/cn$RZ	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netL.TTFOq	0%	Avira URL Cloud	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.carterandcone.comMic	0%	Avira URL Cloud	safe	
http://www.typography.netor	0%	Avira URL Cloud	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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.galapagosdesign.com/xM	0%	Avira URL Cloud	safe	
http://www.tiro.com#gO	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	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.carterandcone.comtig	0%	Avira URL Cloud	safe	
http://JaIZBT.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.carterandcone.compe	0%	Avira URL Cloud	safe	
http://www.carterandcone.comperN	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://www.carterandcone.comY	0%	Avira URL Cloud	safe	
http://www.typography.netliqueFq	0%	Avira URL Cloud	safe	
http://www.carterandcone.comi	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.sandoll.co.kra-d&u	0%	Avira URL Cloud	safe	
http://www.carterandcone.comrh	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comelpLm	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krony	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.tiro.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmhi	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	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/cnq	0%	Avira URL Cloud	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.carterandcone.comD	0%	Avira URL Cloud	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.typography.netcreen	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.htmlzi	0%	Avira URL Cloud	safe	
http://www.carterandcone.com8	0%	Avira URL Cloud	safe	
http://www.carterandcone.comits	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmtr-tr	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	TRENWATR.EXE, 00000005.00000002.506281676.0000000002E81000.00000004.00000001.sdmp, outlook.exe, 00000015.00000002.377800877.0000000002901000.00000004.00000001.sdmp, outlook.exe, 00000016.00000002.503516708.0000000002E61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comB.TTFG	TRENWATR.EXE, 00000000.00000002.259515653.0000000001717000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comes	TRENWATR.EXE, 00000000.00000003.238587043.0000000005F3B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dist.nuget.org/win-x86-commandline/latest/nuget.exe	outlook.exe, outlook.exe, 0000 0014.00000002.370585135.000000 0000EB2000.00000002.00020000.sdmp, outlook.exe, 00000015.00000002.3762 95024.00000000005B2000.0000000 2.00020000.sdmp, outlook.exe, 00000016.00000000.368954462.00 00000000AB2000.00000002.000200 00.sdmp, TRENWATR.EXE	false		high
http://www.fontbureau.com/designers0c.	TRENWATR.EXE, 00000000.0000000 3.242105483.0000000005F47000.0 0000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	outlook.exe, 00000012.00000002 .360749670.0000000002EE9000.00 000004.00000001.sdmp, outlook.exe, 00000014.00000002.3747003 47.00000000032EB000.00000004.0 0000001.sdmp	false		high
http://www.fontbureau.com/designers	outlook.exe, 00000014.00000002 .381519178.00000000063D0000.00 000002.00000001.sdmp	false		high
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	TRENWATR.EXE, 00000000.0000000 2.259862651.0000000002F34000.0 0000004.00000001.sdmp, outlook.exe, 00000012.00000002.360720856.000000 0002EE0000.00000004.00000001.sdmp, outlook.exe, 00000014.00000002.3746 65884.00000000032E4000.0000000 4.00000001.sdmp	false		high
http://www.founder.com.cn/cn$RZ	TRENWATR.EXE, 00000000.0000000 3.237832318.0000000005F53000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	TRENWATR.EXE, 00000000.0000000 3.234896317.0000000005F3B000.0 0000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.000000 0005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.3815 19178.00000000063D0000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netL.TTFOq	TRENWATR.EXE, 00000000.0000000 3.236015819.0000000005F3B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://repository.certum.pl/ca.cer09	TRENWATR.EXE, 00000005.0000000 2.518819386.0000000006660000.0 0000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	TRENWATR.EXE, 00000000.0000000 2.266888357.0000000007132000.0 0000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.000000 0005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.3815 19178.00000000063D0000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comMic	TRENWATR.EXE, 00000000.0000000 3.238427690.0000000005F3B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netor	TRENWATR.EXE, 00000000.0000000 3.236231153.0000000005F3B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	TRENWATR.EXE, 00000000.0000000 2.266888357.0000000007132000.0 0000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.000000 0005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.3815 19178.00000000063D0000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	TRENWATR.EXE, 00000000.0000000 3.239865090.0000000005F44000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Spegeli/Pokemon-Go-Rocket-API/archive/master.zip	outlook.exe, outlook.exe, 0000 0015.00000002.376295024.000000 00005B2000.00000002.00020000.sdmp, outlook.exe, 00000016.00000000.3689 54462.0000000000AB2000.0000000 2.00020000.sdmp, TRENWATR.EXE	false		high
http://www.galapagosdesign.com/xM	TRENWATR.EXE, 00000000.0000000 3.244974147.0000000005F47000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com#gO	TRENWATR.EXE, 00000000.00000003.237954503.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	TRENWATR.EXE, 00000000.00000002.259743735.0000000002EE1000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.360749670.0000000002EE9000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.360529730.0000000002E91000.00000004.00000001.sdmp, outlook.exe, 00000014.00000002.374700347.000000032EB000.00000004.00000001.sdmp, outlook.exe, 00000014.00000002.374363731.0000000003291000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	TRENWATR.EXE, 00000000.00000002.260543683.0000000003EEC000.00000004.00000001.sdmp, TRENWATR.EXE, 00000005.00000002.495941887.0000000000402000.00000040.00000001.sdmp, outlook.exe, 00000012.00000002.361897576.0000000003E9C000.00000004.00000001.sdmp, outlook.exe, 00000014.00000002.375859880.00000000429C000.00000004.00000001.sdmp, outlook.exe, 00000015.00000002.376120241.0000000000402000.00000040.00000001.sdmp, outlook.exe, 00000016.00000002.496146481.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certum.pl/CPS0	TRENWATR.EXE, 00000005.00000002.518819386.0000000006660000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comtig	TRENWATR.EXE, 00000000.00000003.238427690.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://JaIZBT.com	outlook.exe, 00000016.00000002.503516708.0000000002E61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/	TRENWATR.EXE, 00000000.00000003.244974147.0000000005F47000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.compe	TRENWATR.EXE, 00000000.00000003.238427690.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comperN	TRENWATR.EXE, 00000000.00000003.238427690.0000000005F3B000.00000004.00000001.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	TRENWATR.EXE, 00000005.00000002.506281676.0000000002E81000.00000004.00000001.sdmp, outlook.exe, 00000015.00000002.377800877.0000000002901000.00000004.00000001.sdmp, outlook.exe, 00000016.00000002.503516708.0000000002E61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.certum.pl/ctnca.crl0k	TRENWATR.EXE, 00000005.00000002.518819386.0000000006660000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comY	TRENWATR.EXE, 00000000.00000003.238558968.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/d-haxton/HaxtonBot/archive/master.zip	outlook.exe, outlook.exe, 0000 0014.00000002.370585135.000000 0000EB2000.00000002.00020000.sdmp, outlook.exe, 00000015.00000002.3762 95024.00000000005B2000.0000000 2.00020000.sdmp, outlook.exe, 00000016.00000000.368954462.00 00000000AB2000.00000002.000200 00.sdmp, TRENWATR.EXE	false		high
http://www.fontbureau.com/designers/frere-jones.htmlX	TRENWATR.EXE, 00000000.0000000 3.242301739.0000000005F47000.0 0000004.00000001.sdmp	false		high
http://www.typography.netliqueFq	TRENWATR.EXE, 00000000.0000000 3.236231153.0000000005F3B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comi	TRENWATR.EXE, 00000000.0000000 3.238558968.0000000005F3B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://smtp.yandex.com	TRENWATR.EXE, 00000005.0000000 2.513816109.0000000003135000.0 0000004.00000001.sdmp	false		high
http://www.carterandcone.coml	TRENWATR.EXE, 00000000.0000000 2.266888357.0000000007132000.0 0000004.00000001.sdmp, TRENWAT R.EXE, 00000000.00000003.23855 8968.0000000005F3B000.00000004 .00000001.sdmp, outlook.exe, 0 0000012.00000002.366183325.000 0000005E70000.00000002.0000000 1.sdmp, outlook.exe, 00000014. 00000002.381519178.00000000063 D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	TRENWATR.EXE, 00000000.0000000 3.237913831.0000000005F3B000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	TRENWATR.EXE, 00000000.0000000 2.266888357.0000000007132000.0 0000004.00000001.sdmp, TRENWAT R.EXE, 00000000.00000003.24250 3896.0000000005F47000.00000004 .00000001.sdmp, outlook.exe, 0 0000012.00000002.366183325.000 0000005E70000.00000002.0000000 1.sdmp, outlook.exe, 00000014. 00000002.381519178.00000000063 D0000.00000002.00000001.sdmp	false		high
http://crls.yandex.net/certum/ycasha2.crl0-	TRENWATR.EXE, 00000005.0000000 2.518819386.0000000006660000.0 0000004.00000001.sdmp	false		high
http://www.sandoll.co.kra-d&u	TRENWATR.EXE, 00000000.0000000 3.237176182.0000000005F3B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comrh	TRENWATR.EXE, 00000000.0000000 3.238264721.0000000005F3B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	TRENWATR.EXE, 00000000.0000000 2.266888357.0000000007132000.0 0000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.000000 0005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.3815 19178.00000000063D0000.0000000 2.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	TRENWATR.EXE, 00000000.0000000 2.266888357.0000000007132000.0 0000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.000000 0005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.3815 19178.00000000063D0000.0000000 2.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	TRENWATR.EXE, 00000000.0000000 2.266888357.0000000007132000.0 0000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.000000 0005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.3815 19178.00000000063D0000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comelpLm	TRENWATR.EXE, 00000000.0000000 3.238264721.0000000005F3B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false		high
http://yandex.crl.certum.pl/ycasha2.crl0q	TRENWATR.EXE, 00000005.00000002.518819386.0000000006660000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers&c	TRENWATR.EXE, 00000000.00000003.248532139.0000000005F47000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.krony	TRENWATR.EXE, 00000000.00000003.237176182.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmhi	TRENWATR.EXE, 00000000.00000003.245675829.0000000005F47000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersZ	TRENWATR.EXE, 00000000.00000003.241695306.0000000005F47000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	TRENWATR.EXE, 00000000.00000003.238558968.0000000005F3B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://subca.ocsp-certum.com0.	TRENWATR.EXE, 00000005.00000002.518819386.0000000006660000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnq	TRENWATR.EXE, 00000000.00000003.237832318.0000000005F53000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, TRENWATR.EXE, 00000000.00000003.236572064.0000000005F3B000.00000004.00000001.sdmp, TRENWATR.EXE, 00000000.00000003.235975296.0000000005F3B000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comD	TRENWATR.EXE, 00000000.00000003.238427690.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comC	TRENWATR.EXE, 00000000.00000003.238427690.0000000005F3B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.net	TRENWATR.EXE, 00000000.00000003.236231153.0000000005F3B000.00000004.00000001.sdmp, TRENWATR.EXE, 00000000.00000003.236015819.0000000005F3B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netcreen	TRENWATR.EXE, 00000000.00000003.236231153.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.htmlzi	TRENWATR.EXE, 00000000.00000003.240042629.0000000005F47000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com8	TRENWATR.EXE, 00000000.00000003.238291911.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comits	TRENWATR.EXE, 00000000.00000003.238558968.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmtr-tr	TRENWATR.EXE, 00000000.00000003.248272029.0000000005F47000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	TRENWATR.EXE, 00000005.00000002.518819386.0000000006660000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	outlook.exe, 00000016.00000002.503516708.0000000002E61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.carterandcone.comV	TRENWATR.EXE, 00000000.00000003.238264721.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	TRENWATR.EXE, 00000000.00000003.237176182.0000000005F3B000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comsign	TRENWATR.EXE, 00000000.00000003.238427690.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comd	TRENWATR.EXE, 00000000.00000003.234896317.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ycasha2.cer0	TRENWATR.EXE, 00000005.00000002.518819386.0000000006660000.00000004.00000001.sdmp	false		high
http://www.carterandcone.compef	TRENWATR.EXE, 00000000.00000003.238558968.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	outlook.exe, 00000016.00000002.503516708.0000000002E61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ctnca.cer09	TRENWATR.EXE, 00000005.00000002.518819386.0000000006660000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.comx	TRENWATR.EXE, 00000000.00000003.234896317.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlt	TRENWATR.EXE, 00000000.00000003.242859092.0000000005F47000.00000004.00000001.sdmp	false		high
http://https://www.certum.pl/CPS0	TRENWATR.EXE, 00000005.00000002.518819386.0000000006660000.00000004.00000001.sdmp	false		high
http://www.fontbureau.coma	TRENWATR.EXE, 00000000.00000002.259515653.0000000001717000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comto	TRENWATR.EXE, 00000000.00000003.238427690.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%$	TRENWATR.EXE, 00000005.00000002.506281676.0000000002E81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://yandex.ocsp-responder.com03	TRENWATR.EXE, 00000005.00000002.518819386.0000000006660000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	TRENWATR.EXE, 00000000.00000003.237832318.0000000005F53000.00000004.00000001.sdmp, TRENWATR.EXE, 00000000.00000003.237698757.0000000005F47000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	TRENWATR.EXE, 00000000.00000003.242859092.0000000005F47000.00000004.00000001.sdmp	false		high
http://www.monotype.	TRENWATR.EXE, 00000000.00000003.241477321.0000000005F47000.00000004.00000001.sdmp, TRENWATR.EXE, 00000000.00000003.241231274.0000000005F47000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comT	TRENWATR.EXE, 00000000.00000003.237977092.0000000005F3B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	TRENWATR.EXE, 00000000.00000002.259515653.0000000001717000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	TRENWATR.EXE, 00000000.00000002.266888357.0000000007132000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.366183325.0000000005E70000.00000002.00000001.sdmp, outlook.exe, 00000014.00000002.381519178.00000000063D0000.00000002.00000001.sdmp	false		high
http://crl.certum.pl/ca.crl0h	TRENWATR.EXE, 00000005.00000002.518819386.0000000006660000.00000004.00000001.sdmp	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383916
Start date:	08.04.2021
Start time:	12:22:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TRENWATR.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@9/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 34.8% • Quality standard deviation: 38.7%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .EXE
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:23:44	API Interceptor	682x Sleep call for process: TRENWATR.EXE modified
12:24:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run outlook C:\Users\user\AppData\Roaming\outlook\outlook.exe
12:24:22	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run outlook C:\Users\user\AppData\Roaming\outlook\outlook.exe
12:24:29	API Interceptor	235x Sleep call for process: outlook.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TRENWATR.EXE.log	
Process:	C:\Users\user\Desktop\TRENWATR.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\outlook.exe.log	
Process:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\outlook.exe.log	
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\outlook\outlook.exe	
Process:	C:\Users\user\Desktop\TRENWATR.EXE
File Type:	Unknown
Category:	dropped
Size (bytes):	937984
Entropy (8bit):	7.076855806946785
Encrypted:	false
SSDEEP:	12288:/SAIIK2eESC92/+WjfrGiEMCYPXVK0UC8cHpM+liUCDqOHxVMqIK1eES:/QlVd2/+WLCRM3/VK0rAUCDLHxKqII
MD5:	4C8C4125A16387F16558E841A704C718
SHA1:	A550EC500BFA00F45AC799B9E5F4868A30892E23
SHA-256:	5AAAE83A4B166E0CB4A3A5841C6B92C39C66B2C8DABBE9E304C7865237C9AD5B
SHA-512:	11519CDC8EAFD3CC39FA3AE0A335B6FA53725B77176C73FAED4999733D36C20DE9DDDDE572D027E71619A2B47CE0615C28A4A7022126ACDCDD9CD5F89D60ECF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....n`.....P..R.....p... .....@.. ..... ..@.....p..O..... ..... ..H.....text....P... ...R..... ..`.rsrc.....T.....@..@.rel oc.....N.....@..B.....p.....H.....?..XH.....0.....(....(.....(.....o!....*.....("......(#.....($.....(%.....(&....*N..(.. ..ol...('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<..... ..~.....(3.....!r...p.....(4...o5...s6.....~.....+..*.0.....

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.076855806946785

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	TRENWATR.EXE
File size:	937984
MD5:	4c8c4125a16387f16558e841a704c718
SHA1:	a550ec500bfa00f45ac799b9e5f4868a30892e23
SHA256:	5aaae83a4b166e0cb4a3a5841c6b92c39c66b2c8dabbe9e304c7865237c9ad5b
SHA512:	11519cdc8eafd3cc39fa3ae0a335b6fa53725b77176c73faed4999733d36c20de9dddde572d027e71619a2b47ce0615c28a4a7022126acdcdd9cd5f89d60e2cf
SSDEEP:	12288:/SAIIK2eESC92/+WjfrGiEMCYPXVK0UC8cHpM+liUCDqOHxVMqIK1eES:/QIVd2/+WLCRM3/VK0rAUCDLHxKqII
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....n`.....P..R.....p... .....@.. .....@.....

File Icon

Icon Hash:	0e07030d0d030750

Static PE Info

General

Entrypoint:	0x4a70ea
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:	0x606EC4F6 [Thu Apr 8 08:55:18 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

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

Copyright Joe Security LLC 2021

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa7098	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x3f884	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe8000	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	0xa50f0	0xa5200	False	0.788516926098	data	7.54897918265	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x3f884	0x3fa00	False	0.266258134823	data	5.24868308892	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa8310	0x10828	data		
RT_ICON	0xb8b38	0x6f5a	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xbfa94	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xd02bc	0x94a8	data		
RT_ICON	0xd9764	0x5488	data		
RT_ICON	0xdebec	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 15794175, next used block 4294902528		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe2e14	0x25a8	data		
RT_ICON	0xe53bc	0x10a8	data		
RT_ICON	0xe6464	0x988	data		
RT_ICON	0xe6dec	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xe7254	0x14	data		
RT_GROUP_ICON	0xe7268	0x92	data		
RT_VERSION	0xe72fc	0x39a	data		
RT_MANIFEST	0xe7698	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 2016 Computer City
Assembly Version	1.12.0.2
InternalName	EnumSByteTypeInfo.exe
FileVersion	1.12.0.2
CompanyName	Computer City
LegalTrademarks	
Comments	
ProductName	UnmanagedAccessor
ProductVersion	1.12.0.2
FileDescription	UnmanagedAccessor
OriginalFilename	EnumSByteTypeInfo.exe

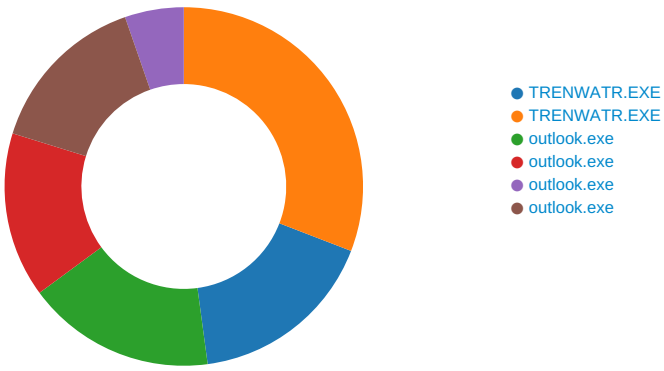
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: TRENWATR.EXE PID: 1048 Parent PID: 5768

General

Start time:	12:23:35
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\TRENWATR.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TRENWATR.EXE'
Imagebase:	0xab0000
File size:	937984 bytes
MD5 hash:	4C8C4125A16387F16558E841A704C718
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: 00000000.00000002.260543683.0000000003EEC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.261068565.00000000040F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.259862651.0000000002F34000.00000004.00000001.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	6D59CF06	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	6D59CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TRENWATR.EXE.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8AC78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\TRENWATR.EXE.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D8AC907	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	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D575705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D57CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3E1B4F	ReadFile

Analysis Process: TRENWATR.EXE PID: 3336 Parent PID: 1048

General

Start time:	12:23:46
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\TRENWATR.EXE
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\TRENWATR.EXE
Imagebase:	0x980000
File size:	937984 bytes
MD5 hash:	4C8C4125A16387F16558E841A704C718
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: 00000005.00000002.495941887.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.513517765.00000000030FF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.506281676.0000000002E81000.00000004.00000001.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	6D59CF06	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	6D59CF06	unknown
C:\Users\user\AppData\Roaming\outlook	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C3EBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\outlook\outlook.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	6C3EDD66	CopyFileW
C:\Users\user\AppData\Roaming\outlook\outlook.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C3EDD66	CopyFileW

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\outlook\outlook.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 f6 c4 6e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 52 0a 00 00 fc 03 00 00 00 00 00 ea 70 0a 00 00 20 00 00 00 80 0a 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 a0 0e 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.....n`.......... ....P..R...........p... ....@.. ....@................	success or wait	4	6C3EDD66	CopyFileW
C:\Users\user\AppData\Roaming\outlook\outlook.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	6C3EDD66	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	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D575705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D57CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C3E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\235aac83-7b0d-4912-a586-3c6fcc481456	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C3E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C3E1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	outlook	unicode	C:\Users\user\AppData\Roaming\outlook\outlook.exe	success or wait	1	6C3E646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	outlook	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C3EDE2E	RegSetValueExW

Analysis Process: outlook.exe PID: 6696 Parent PID: 3292

General

Start time:	12:24:23
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\outlook\outlook.exe'
Imagebase:	0x920000
File size:	937984 bytes
MD5 hash:	4C8C4125A16387F16558E841A704C718
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: 00000012.00000002.360720856.0000000002EE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.363998493.00000000040A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.361897576.0000000003E9C000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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 | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D59CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D59CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\outlook.exe.log	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D8AC78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\outlook.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D8AC907	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	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D575705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D57CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3E1B4F	ReadFile

Analysis Process: outlook.exe PID: 6904 Parent PID: 3292

General

Start time:	12:24:31
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\outlook\outlook.exe'
Imagebase:	0xeb0000
File size:	937984 bytes
MD5 hash:	4C8C4125A16387F16558E841A704C718
Has elevated privileges:	true

Copyright Joe Security LLC 2021

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.375859880.000000000429C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.374665884.00000000032E4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.376980132.00000000044A9000.00000004.00000001.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 | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D59CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D59CF06	unknown

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	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D575705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D57CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3E1B4F	ReadFile

Analysis Process: outlook.exe PID: 6944 Parent PID: 6696

General

Start time:	12:24:32
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Imagebase:	0x5b0000
File size:	937984 bytes
MD5 hash:	4C8C4125A16387F16558E841A704C718
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.377800877.0000000002901000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.377800877.0000000002901000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.376120241.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

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	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D575705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D57CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4D03DE	ReadFile

Analysis Process: outlook.exe PID: 7012 Parent PID: 6904

General

Start time:	12:24:38
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Imagebase:	0xab0000
File size:	937984 bytes
MD5 hash:	4C8C4125A16387F16558E841A704C718
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: 00000016.00000002.496146481.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000002.503516708.0000000002E61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.503516708.0000000002E61000.00000004.00000001.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 | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D59CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D59CF06	unknown

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	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D575705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D57CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3E1B4F	ReadFile

Disassembly

Code Analysis