ID: 412503
Sample Name:
W9YDH79i8G.exe
Cookbook: default.jbs
Time: 18:32:56
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

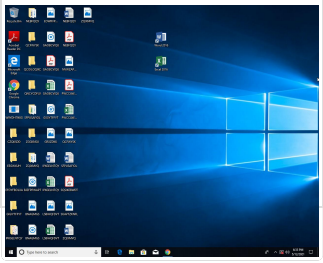
Analysis Report W9YDH79i8G.exe

Overview

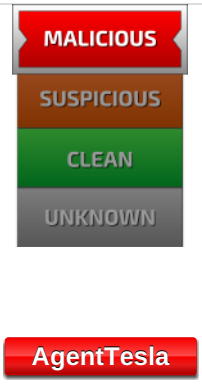
General Information

Sample Name:	W9YDH79i8G.exe
Analysis ID:	412503
MD5:	cdebc3e47db1db..
SHA1:	ceee8ff397069a6..
SHA256:	0fa77ee6af812f5…
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

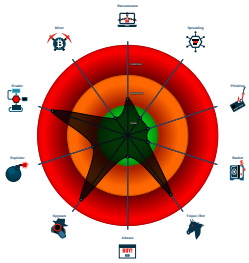


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Contains functionality to register a lo…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- W9YDH79i8G.exe (PID: 5656 cmdline: 'C:\Users\user\Desktop\W9YDH79i8G.exe' MD5: CDEBC3E47DB1DBEAC624DD329C1A9AE1)
  - schtasks.exe (PID: 6168 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\KcsiIHD' /XML 'C:\Users\user\AppData\Local\Temp\tmp4276.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - W9YDH79i8G.exe (PID: 6232 cmdline: C:\Users\user\Desktop\W9YDH79i8G.exe MD5: CDEBC3E47DB1DBEAC624DD329C1A9AE1)
  - W9YDH79i8G.exe (PID: 6248 cmdline: C:\Users\user\Desktop\W9YDH79i8G.exe MD5: CDEBC3E47DB1DBEAC624DD329C1A9AE1)
  - W9YDH79i8G.exe (PID: 6280 cmdline: C:\Users\user\Desktop\W9YDH79i8G.exe MD5: CDEBC3E47DB1DBEAC624DD329C1A9AE1)
  - W9YDH79i8G.exe (PID: 6316 cmdline: C:\Users\user\Desktop\W9YDH79i8G.exe MD5: CDEBC3E47DB1DBEAC624DD329C1A9AE1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "shekhar@ocl-india.icu@Mexico1.,mail.privateemail.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.252742797.000000000334000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.254574303.00000000042F9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.254574303.00000000042F9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000002.497630354.000000000325 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.497630354.000000000325 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 10 entries				

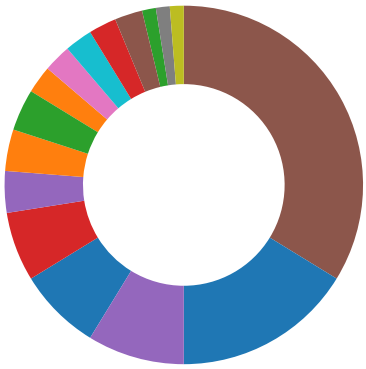
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.W9YDH79i8G.exe.4428d80.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.W9YDH79i8G.exe.4428d80.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.W9YDH79i8G.exe.4428d80.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.W9YDH79i8G.exe.4428d80.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.2.W9YDH79i8G.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 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 dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected 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

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

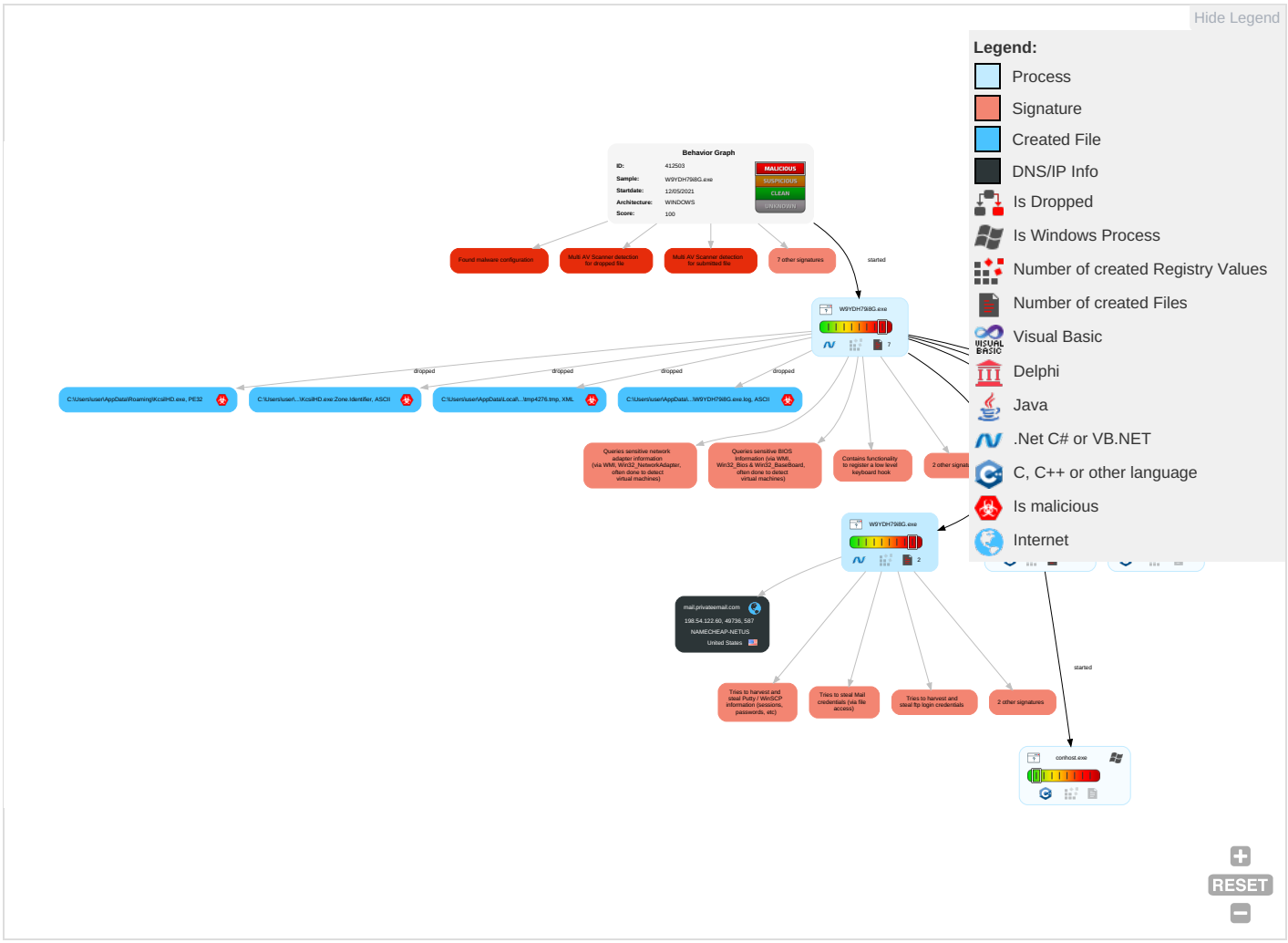
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
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	Input Capture 2 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commanc and Contr
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 Used 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	Applicatior Layer Prot

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
W9YDH79i8G.exe	35%	Virustotal		Browse
W9YDH79i8G.exe	40%	ReversingLabs	Win32.Trojan.AgentTesla	
W9YDH79i8G.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\KcsilHD.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\KcsilHD.exe	40%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.W9YDH79i8G.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://HVIItO.com	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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://3yctoQGYo4sp.com	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	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://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

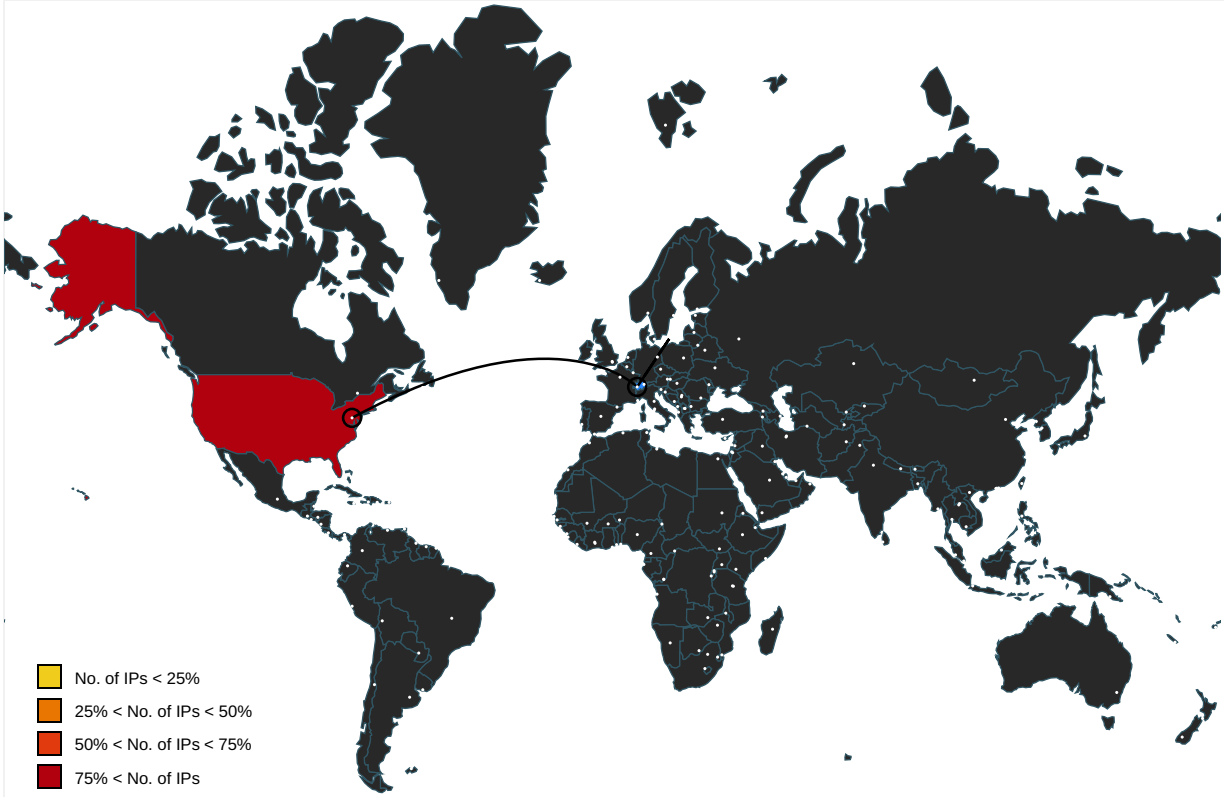
Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.privateemail.com	198.54.122.60	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	W9YDH79i8G.exe, 00000007.00000002.497963649.0000000003314000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	W9YDH79i8G.exe, 00000007.00000002.497630354.0000000003251000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://HVIItO.com	W9YDH79i8G.exe, 00000007.00000002.497630354.0000000003251000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	W9YDH79i8G.exe, 00000007.00000002.497630354.0000000003251000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	W9YDH79i8G.exe, 00000007.00000002.497963649.0000000003314000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://3yctoQGYo4sp.com	W9YDH79i8G.exe, 00000007.00000002.497762134.00000000032B3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	W9YDH79i8G.exe, 00000007.00000002.497963649.0000000003314000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.privateemail.com	W9YDH79i8G.exe, 00000007.00000002.497963649.0000000003314000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	W9YDH79i8G.exe, 00000007.00000002.497630354.0000000003251000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	W9YDH79i8G.exe, 00000000.00000002.252742797.0000000003334000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	W9YDH79i8G.exe, 00000000.00000002.254886399.0000000004412000.00000004.00000001.sdmp, W9YDH79i8G.exe, 00000007.00000002.494321847.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	W9YDH79i8G.exe, 00000000.00000002.252742797.0000000003334000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.122.60	mail.privateemail.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412503
Start date:	12.05.2021
Start time:	18:32:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	W9YDH79i8G.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:	32

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@12/4@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.5% (good quality ratio 5.5%) • Quality average: 68.3% • Quality standard deviation: 33.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 20.82.210.154, 168.61.161.212, 104.43.139.144, 92.122.145.220, 52.147.198.201, 104.43.193.48, 184.30.24.56, 20.82.209.183, 92.122.213.247, 92.122.213.194, 13.107.4.50, 2.20.143.16, 2.20.142.209, 20.50.102.62, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, Edge-Prod-FRA.env.au.au-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, elasticShed.au.au-msedge.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, afdap.au.au-msedge.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, au.au-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:33:47	API Interceptor	716x Sleep call for process: W9YDH79i8G.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.122.60	Ko4zQgTBHv.exe	Get hash	malicious	Browse	
	wed.doc	Get hash	malicious	Browse	
	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.43091.10004.exe	Get hash	malicious	Browse	
	6e5c05e1_by_Libranalysis.exe	Get hash	malicious	Browse	
	RFQ Plasma cutting machine.doc	Get hash	malicious	Browse	
	337840b9_by_Libranalysis.exe	Get hash	malicious	Browse	
	vy38Kw9qRh.exe	Get hash	malicious	Browse	
	ePj6KfzLBxh4vbe.exe	Get hash	malicious	Browse	
	zkXpISzeo3.exe	Get hash	malicious	Browse	
	yl9KgwwOXDZoGMw.exe	Get hash	malicious	Browse	
	8DL3LHg4SB6Q7z2.exe	Get hash	malicious	Browse	
	01217a79_by_Libranalysis.exe	Get hash	malicious	Browse	
	5iRqi4LmLF.exe	Get hash	malicious	Browse	
	6f37L7HNqo.exe	Get hash	malicious	Browse	
	IqRG5ZzYOH.exe	Get hash	malicious	Browse	
	PO 4302003683.doc	Get hash	malicious	Browse	
	Tender Overview 10052021.doc	Get hash	malicious	Browse	
	ORDER 10.05.doc	Get hash	malicious	Browse	
	purchase request.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.privateemail.com	Ko4zQgTBHv.exe	Get hash	malicious	Browse	• 198.54.122.60
	wed.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.Packed2.43091.10004.exe	Get hash	malicious	Browse	• 198.54.122.60
	6e5c05e1_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	RFQ Plasma cutting machine.doc	Get hash	malicious	Browse	• 198.54.122.60
	337840b9_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	vy38Kw9qRh.exe	Get hash	malicious	Browse	• 198.54.122.60
	ePj6KfzLBxh4vbe.exe	Get hash	malicious	Browse	• 198.54.122.60
	zkXpISzeo3.exe	Get hash	malicious	Browse	• 198.54.122.60
	yl9KgwwOXDZoGMw.exe	Get hash	malicious	Browse	• 198.54.122.60
	8DL3LHg4SB6Q7z2.exe	Get hash	malicious	Browse	• 198.54.122.60
	01217a79_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	5iRqi4LmLF.exe	Get hash	malicious	Browse	• 198.54.122.60
	6f37L7HNqo.exe	Get hash	malicious	Browse	• 198.54.122.60
	IqRG5ZzYOH.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO 4302003683.doc	Get hash	malicious	Browse	• 198.54.122.60
	Tender Overview 10052021.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER 10.05.doc	Get hash	malicious	Browse	• 198.54.122.60
	purchase request.doc	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	Ko4zQgTBHv.exe	Get hash	malicious	Browse	• 198.54.122.60
	Purchase Order.exe	Get hash	malicious	Browse	• 198.54.126.165
	wed.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.Packed2.43091.10004.exe	Get hash	malicious	Browse	• 198.54.122.60
	6e5c05e1_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	RFQ Plasma cutting machine.doc	Get hash	malicious	Browse	• 198.54.122.60
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 198.54.117.216
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 162.255.11 9.164
	00098765123POIIU.exe	Get hash	malicious	Browse	• 199.192.23.253
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 185.61.154.27
	2021_May_Quotation_pdf.exe	Get hash	malicious	Browse	• 198.54.115.133
	337840b9_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	Citvonvhciktufwvyzyhistnewdjgsoqdr.exe	Get hash	malicious	Browse	• 198.54.117.212
	Updated Order list -804333.exe	Get hash	malicious	Browse	• 198.54.115.56
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	BELLOW FABRICATION Dwg.exe	Get hash	malicious	Browse	• 199.188.200.15
	file.exe	Get hash	malicious	Browse	• 198.54.115.133
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 162.0.233.152
	vy38Kw9qRh.exe	Get hash	malicious	Browse	• 198.54.122.60

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\KcsilHD.exe	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\W9YDH79i8G.exe.log	
Process:	C:\Users\user\Desktop\W9YDH79i8G.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, 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..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp4276.tmp	
Process:	C:\Users\user\Desktop\W9YDH79i8G.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.167020690421923

C:\Users\user\AppData\Local\Temp\tmp4276.tmp	
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBUtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3U
MD5:	AF08A3DA8E0E3155FF47F61E57B341B6
SHA1:	5348054A4725F8F5E7605998FFE8F700D1765F54
SHA-256:	42D91FCF4B78A320EB132A20C82AD4D51EE2FEC556E836D41473BB1AAEF5DB6A
SHA-512:	5EA07A7C08C1515CB655F2C21572F82F63F1065A27C7E8C9B5BEC29C4D1CDE2D99D2CDF432E2158EC89BC1F191BBB294F0B3C6DC0CD417F91E54CC29B29EEB5
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>.. <StartWhenAv

C:\Users\user\AppData\Roaming\KcsilHD.exe	
Process:	C:\Users\user\Desktop\W9YDH79i8G.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	846336
Entropy (8bit):	7.9780435401207574
Encrypted:	false
SSDEEP:	24576:imn4+yPg0Ip0DImJyhjDDRPm7C56SOyFhLlSb2:irZP5IaHkR+7C5iyFhLl0
MD5:	CDEBC3E47DB1DBEAC624DD329C1A9AE1
SHA1:	CEEE8FF397069A606B3BBEF0D54A4175A1DE9A0E
SHA-256:	0FA77EE6AF812F5513BF0AE73A02143A4ED3A037E884AECCC57576F460A9EA57
SHA-512:	A6397B1517BD85F13395B874188BB93D46C2E77DA9C054DC1F762441BA292D6CD54F9711CAE28A513B8AB58E4111C376724400E7A424AA12822D90032B38648A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 40%
Joe Sandbox View:	• Filename: ORDER CONFIRMATION.doc, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....J.... .....@.. .....@..... .@.....O.....p..... ..... ..H.....text...X.... ..... ..`.rsrc...p.....@..@.reloc..... . .....@..B.....H.....@A...R...../.....i.....(....*.0.....(.....o....o.....,..(....(.....s....o ...(.....(!.....,L....s"....o#...($.....U...(..... (.....(.....io%...&....,..o&.....+.....U...(.....*.....L.3.....0..Q.....(.....,A.(!...,..+....,.('.....((...s).....(....o*.....,..o&.....*.....3..B.....0..!.....u.....,...t....Q..+....+..*....0.. @.....r...p.(.....(.....i...(+....(....-.~,..

C:\Users\user\AppData\Roaming\KcsilHD.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\W9YDH79i8G.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**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9780435401207574

General

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:	W9YDH79i8G.exe
File size:	846336
MD5:	cdebc3e47db1dbeac624dd329c1a9ae1
SHA1:	ceee8ff397069a606b3bbef0d54a4175a1de9a0e
SHA256:	0fa77ee6af812f5513bf0ae73a02143a4ed3a037e884aeccc57576f460a9ea57
SHA512:	a6397b1517bd85f13395b874188bb93d46c2e77da9c054dc1f762441ba292d6cd54f9711cae28a513b8ab58e4111c376724400e7a424aa12822d90032b38648a
SSDEEP:	24576:imn4+yPg0Ip0DImJyhjDDRPm7C56SOyFhLlSb2:irZP5IaHkR+7C5iyFhLl0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....J.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4cfd4a
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:	0x609AF3E2 [Tue May 11 21:15:14 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
inc ebp
dec edi
push eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0xcfcf8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd0000	0x670	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd2000	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	0xcdd58	0xcde00	False	0.982190630692	data	7.98266183828	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd0000	0x670	0x800	False	0.345703125	data	3.55057718956	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd0090	0x3e0	data		
RT_MANIFEST	0xd0480	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

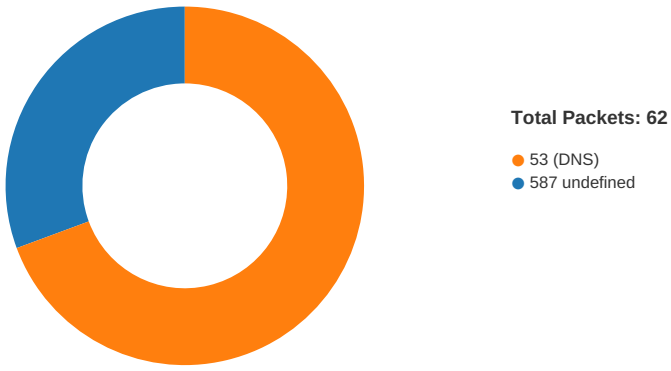
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Barret 2017 - 2021
Assembly Version	1.0.0.0
InternalName	AsyncCausalityTracer.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	Settings for TCP connections
ProductName	Framework - TCP Protocol
ProductVersion	1.0.0.0
FileDescription	Framework - TCP Protocol
OriginalFilename	AsyncCausalityTracer.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:35:29.670989990 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:29.865370035 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:29.867326021 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:30.099402905 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:30.099864960 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:30.293721914 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:30.294054985 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:30.294796944 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:30.488758087 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:30.533360958 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:30.729345083 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:30.730861902 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:30.730899096 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:30.730920076 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:30.730942965 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:30.731009007 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:30.771229029 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:30.966413975 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:30.967308998 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:31.012789965 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:31.056408882 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:31.252953053 CEST	587	49736	198.54.122.60	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:35:31.252980947 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:31.262046099 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:31.455735922 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:31.456871033 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:31.457626104 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:31.652164936 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:31.654834032 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:31.655723095 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:31.849677086 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:31.852600098 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:31.853085041 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:32.047009945 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:32.086910963 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:32.087454081 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:32.281621933 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:32.282399893 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:32.287432909 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:32.287549973 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:32.287616968 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:32.287689924 CEST	49736	587	192.168.2.7	198.54.122.60
May 12, 2021 18:35:32.481466055 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:32.570746899 CEST	587	49736	198.54.122.60	192.168.2.7
May 12, 2021 18:35:32.622329950 CEST	49736	587	192.168.2.7	198.54.122.60

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:33:38.219392061 CEST	62452	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:38.278716087 CEST	53	62452	8.8.8.8	192.168.2.7
May 12, 2021 18:33:38.310179949 CEST	57820	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:38.372602940 CEST	53	57820	8.8.8.8	192.168.2.7
May 12, 2021 18:33:38.889776945 CEST	50848	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:38.938575029 CEST	53	50848	8.8.8.8	192.168.2.7
May 12, 2021 18:33:40.599807978 CEST	61242	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:40.652945042 CEST	53	61242	8.8.8.8	192.168.2.7
May 12, 2021 18:33:41.375370026 CEST	58562	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:41.435806990 CEST	53	58562	8.8.8.8	192.168.2.7
May 12, 2021 18:33:41.682656050 CEST	56590	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:41.733218908 CEST	53	56590	8.8.8.8	192.168.2.7
May 12, 2021 18:33:42.993810892 CEST	60501	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:43.054022074 CEST	53	60501	8.8.8.8	192.168.2.7
May 12, 2021 18:33:44.013274908 CEST	53775	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:44.065963984 CEST	53	53775	8.8.8.8	192.168.2.7
May 12, 2021 18:33:44.978102922 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:45.029982090 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 18:33:46.354953051 CEST	55411	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:46.405982971 CEST	53	55411	8.8.8.8	192.168.2.7
May 12, 2021 18:33:47.701719046 CEST	63668	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:47.750437021 CEST	53	63668	8.8.8.8	192.168.2.7
May 12, 2021 18:33:49.096115112 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:49.144995928 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 18:33:51.494324923 CEST	58739	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:51.546130896 CEST	53	58739	8.8.8.8	192.168.2.7
May 12, 2021 18:33:53.428333998 CEST	60338	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:53.478770018 CEST	53	60338	8.8.8.8	192.168.2.7
May 12, 2021 18:33:54.205084085 CEST	58717	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:54.253799915 CEST	53	58717	8.8.8.8	192.168.2.7
May 12, 2021 18:33:55.399101019 CEST	59762	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:55.450783968 CEST	53	59762	8.8.8.8	192.168.2.7
May 12, 2021 18:33:57.007155895 CEST	54329	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:57.056205988 CEST	53	54329	8.8.8.8	192.168.2.7
May 12, 2021 18:33:57.853051901 CEST	58052	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:57.904751062 CEST	53	58052	8.8.8.8	192.168.2.7
May 12, 2021 18:33:58.752854109 CEST	54008	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:33:58.801477909 CEST	53	54008	8.8.8.8	192.168.2.7
May 12, 2021 18:33:59.546153069 CEST	59451	53	192.168.2.7	8.8.8.8
May 12, 2021 18:33:59.594888926 CEST	53	59451	8.8.8.8	192.168.2.7
May 12, 2021 18:34:01.312114954 CEST	52914	53	192.168.2.7	8.8.8.8
May 12, 2021 18:34:01.360932112 CEST	53	52914	8.8.8.8	192.168.2.7
May 12, 2021 18:34:03.235868931 CEST	64569	53	192.168.2.7	8.8.8.8
May 12, 2021 18:34:03.297327995 CEST	53	64569	8.8.8.8	192.168.2.7
May 12, 2021 18:34:03.376880884 CEST	52816	53	192.168.2.7	8.8.8.8
May 12, 2021 18:34:03.425638914 CEST	53	52816	8.8.8.8	192.168.2.7
May 12, 2021 18:34:04.312475920 CEST	50781	53	192.168.2.7	8.8.8.8
May 12, 2021 18:34:04.361272097 CEST	53	50781	8.8.8.8	192.168.2.7
May 12, 2021 18:34:05.374078989 CEST	54230	53	192.168.2.7	8.8.8.8
May 12, 2021 18:34:05.422889948 CEST	53	54230	8.8.8.8	192.168.2.7
May 12, 2021 18:34:16.277774096 CEST	54911	53	192.168.2.7	8.8.8.8
May 12, 2021 18:34:16.346321106 CEST	53	54911	8.8.8.8	192.168.2.7
May 12, 2021 18:34:27.371154070 CEST	49958	53	192.168.2.7	8.8.8.8
May 12, 2021 18:34:27.430054903 CEST	53	49958	8.8.8.8	192.168.2.7
May 12, 2021 18:34:33.539928913 CEST	50860	53	192.168.2.7	8.8.8.8
May 12, 2021 18:34:33.588852882 CEST	53	50860	8.8.8.8	192.168.2.7
May 12, 2021 18:34:33.686065912 CEST	50452	53	192.168.2.7	8.8.8.8
May 12, 2021 18:34:33.743349075 CEST	53	50452	8.8.8.8	192.168.2.7
May 12, 2021 18:34:58.687050104 CEST	59730	53	192.168.2.7	8.8.8.8
May 12, 2021 18:34:58.746838093 CEST	53	59730	8.8.8.8	192.168.2.7
May 12, 2021 18:35:02.738291979 CEST	59310	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:02.801356077 CEST	53	59310	8.8.8.8	192.168.2.7
May 12, 2021 18:35:23.399950981 CEST	51919	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:23.548990965 CEST	53	51919	8.8.8.8	192.168.2.7
May 12, 2021 18:35:24.151328087 CEST	64296	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:24.210515976 CEST	53	64296	8.8.8.8	192.168.2.7
May 12, 2021 18:35:24.819634914 CEST	56680	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:24.876698017 CEST	53	56680	8.8.8.8	192.168.2.7
May 12, 2021 18:35:25.079459906 CEST	58820	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:25.157521963 CEST	53	58820	8.8.8.8	192.168.2.7
May 12, 2021 18:35:25.492592096 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:25.617566109 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 18:35:26.262207985 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:26.319638968 CEST	53	49247	8.8.8.8	192.168.2.7
May 12, 2021 18:35:26.979278088 CEST	52286	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:27.039125919 CEST	53	52286	8.8.8.8	192.168.2.7
May 12, 2021 18:35:27.696122885 CEST	56064	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:27.754156113 CEST	53	56064	8.8.8.8	192.168.2.7
May 12, 2021 18:35:28.996915102 CEST	63744	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:29.056936979 CEST	53	63744	8.8.8.8	192.168.2.7
May 12, 2021 18:35:29.559542894 CEST	61457	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:29.616543055 CEST	53	61457	8.8.8.8	192.168.2.7
May 12, 2021 18:35:30.227416992 CEST	58367	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:30.292738914 CEST	53	58367	8.8.8.8	192.168.2.7
May 12, 2021 18:35:30.789813042 CEST	60599	53	192.168.2.7	8.8.8.8
May 12, 2021 18:35:30.840092897 CEST	53	60599	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 18:35:29.559542894 CEST	192.168.2.7	8.8.8.8	0x264a	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:35:29.616543055 CEST	8.8.8.8	192.168.2.7	0x264a	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

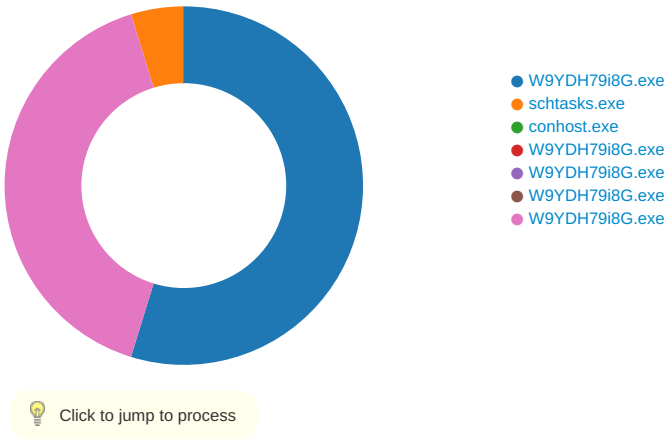
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 18:35:30.099402905 CEST	587	49736	198.54.122.60	192.168.2.7	220 PrivateEmail.com Mail Node
May 12, 2021 18:35:30.099864960 CEST	49736	587	192.168.2.7	198.54.122.60	EHLO 899552
May 12, 2021 18:35:30.294054985 CEST	587	49736	198.54.122.60	192.168.2.7	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
May 12, 2021 18:35:30.294796944 CEST	49736	587	192.168.2.7	198.54.122.60	STARTTLS
May 12, 2021 18:35:30.488758087 CEST	587	49736	198.54.122.60	192.168.2.7	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: W9YDH79i8G.exe PID: 5656 Parent PID: 5776

General

Start time:	18:33:45
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\W9YDH79i8G.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\W9YDH79i8G.exe'
Imagebase:	0xf00000
File size:	846336 bytes
MD5 hash:	CDEBC3E47DB1DBEAC624DD329C1A9AE1
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: 00000000.00000002.252742797.0000000003334000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.254574303.00000000042F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.254574303.00000000042F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.254886399.0000000004412000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.254886399.0000000004412000.00000004.00000001.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	6D3BCF06	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	6D3BCF06	unknown
C:\Users\user\AppData\Roaming\KcsilHD.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	6C20DD66	CopyFileW
C:\Users\user\AppData\Roaming\KcsilHD.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C20DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4276.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\W9YDH79i8G.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6CC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4276.tmp	success or wait	1	6C206A95	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\KcsilHD.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 e2 f3 9a 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 de 0c 00 00 0a 00 00 00 00 00 00 4a fd 0c 00 00 20 00 00 00 00 0d 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 40 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....P.............J.... ....@.. ....@ ....@................	success or wait	4	6C20DD66	CopyFileW
C:\Users\user\AppData\Roaming\KcsilHD.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	6C20DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4276.tmp	unknown	1656	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 66 72 6f 6e 74 64 65 73 6b 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	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	6C201B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\W9YDH79i8G.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	6D6CC907	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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	ReadFile

Analysis Process: schtasks.exe PID: 6168 Parent PID: 5656

General

Start time:	18:33:51
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\KcsilHD' /XML 'C:\Users\user\AppData\Local\Temp\tmp4276.tmp'
Imagebase:	0xb80000
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\tmp4276.tmp	unknown	2	success or wait	1	B8AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4276.tmp	unknown	1657	success or wait	1	B8ABD9	ReadFile

Analysis Process: conhost.exe PID: 6188 Parent PID: 6168

General

Start time:	18:33:52
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: W9YDH79i8G.exe PID: 6232 Parent PID: 5656

General

Start time:	18:33:53
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\W9YDH79i8G.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\W9YDH79i8G.exe
Imagebase:	0x240000
File size:	846336 bytes
MD5 hash:	CDEBC3E47DB1DBEAC624DD329C1A9AE1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: W9YDH79i8G.exe PID: 6248 Parent PID: 5656

General

Start time:	18:33:54
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\W9YDH79i8G.exe
Wow64 process (32bit):	false

Commandline:	C:\Users\user\Desktop\W9YDH79i8G.exe
Imagebase:	0x320000
File size:	846336 bytes
MD5 hash:	CDEBC3E47DB1DBEAC624DD329C1A9AE1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: W9YDH79i8G.exe PID: 6280 Parent PID: 5656

General

Start time:	18:33:54
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\W9YDH79i8G.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\W9YDH79i8G.exe
Imagebase:	0x140000
File size:	846336 bytes
MD5 hash:	CDEBC3E47DB1DBEAC624DD329C1A9AE1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: W9YDH79i8G.exe PID: 6316 Parent PID: 5656

General

Start time:	18:33:55
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\W9YDH79i8G.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\W9YDH79i8G.exe
Imagebase:	0xf20000
File size:	846336 bytes
MD5 hash:	CDEBC3E47DB1DBEAC624DD329C1A9AE1
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: 00000007.00000002.497630354.0000000003251000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.497630354.0000000003251000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.494321847.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.494321847.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.497673320.0000000003286000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.497762134.00000000032B3000.00000004.00000001.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	6D3BCF06	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	6D3BCF06	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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C201B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C201B4F	ReadFile

Disassembly

Code Analysis