ID: 433199
Sample Name: PO #R58490.exe
Cookbook: default.jbs
Time: 12:47:22
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

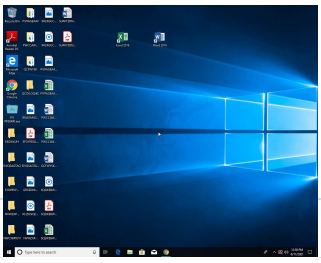
Analysis Report PO #R58490.exe

Overview

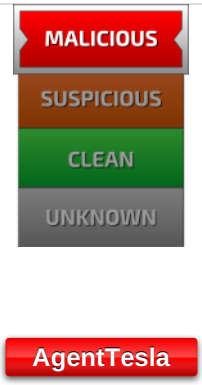
General Information

Sample Name:	PO #R58490.exe
Analysis ID:	433199
MD5:	5cff42958cd317e..
SHA1:	dec2ad475f2989f..
SHA256:	8636a1af1afb3fa...
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

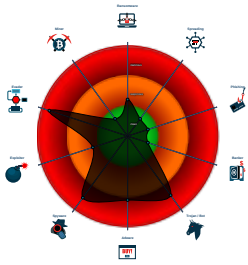


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains method ...
- .NET source code contains very larg...
- Installs a global keyboard hook
- Machine Learning detection for samp...
- Modifies the hosts file
- Queries sensitive BIOS Information ...
- Queries sensitive network adapter in...

Classification



Process Tree

- **System is w10x64**
- PO #R58490.exe (PID: 5396 cmdline: 'C:\Users\user\Desktop\PO #R58490.exe' MD5: 5CFF42958CD317E239D575732F7F9114)
  - PO #R58490.exe (PID: 4724 cmdline: C:\Users\user\Desktop\PO #R58490.exe MD5: 5CFF42958CD317E239D575732F7F9114)
  - PO #R58490.exe (PID: 3840 cmdline: C:\Users\user\Desktop\PO #R58490.exe MD5: 5CFF42958CD317E239D575732F7F9114)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "mmardones@cavilum.cl",
  "Password": "Cavilum4313",
  "Host": "mail.cavilum.cl"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.211277551.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.211277551.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000002.469305003.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.469305003.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.214163603.0000000003BB9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 7 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.PO #R58490.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.PO #R58490.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.PO #R58490.exe.3c75d68.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.PO #R58490.exe.3c75d68.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.0.PO #R58490.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

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:

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

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:

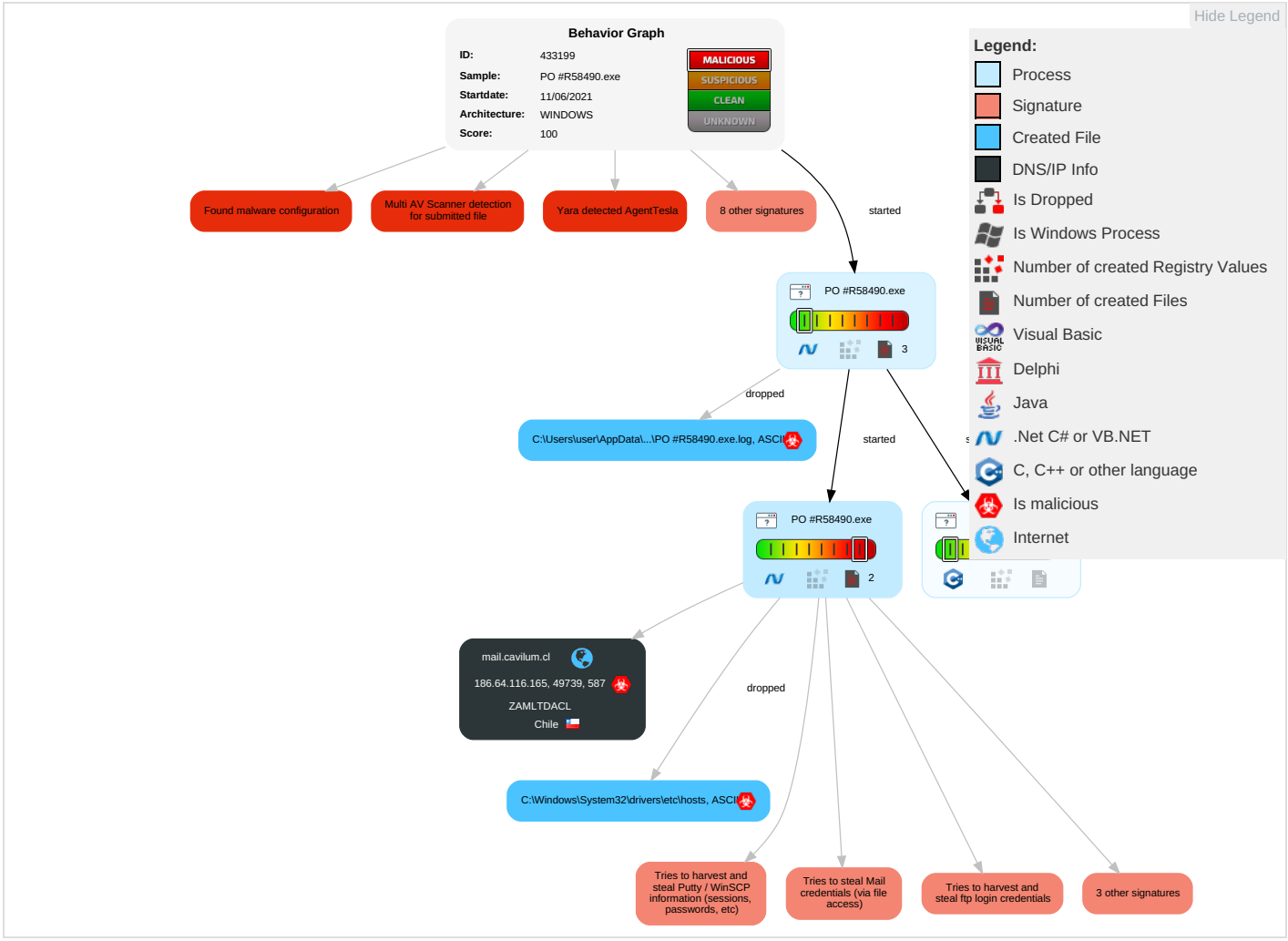
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Security Software Discovery 2 1 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)	Obfuscated Files or Information 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System 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	Process Injection 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

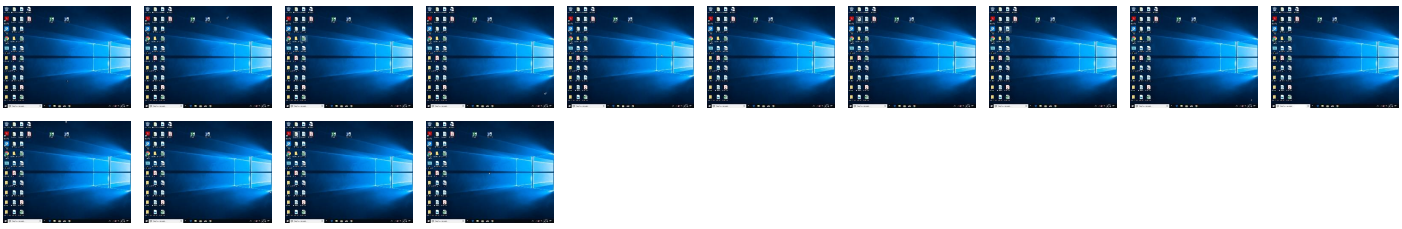
Behavior Graph



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
PO #R58490.exe	31%	Virustotal		Browse
PO #R58490.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PO #R58490.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.PO #R58490.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.PO #R58490.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.cavilum.cl	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://api.ipify.org%x	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://mail.cavilum.cl	0%	Virustotal		Browse
http://mail.cavilum.cl	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://xUGEzQ.com	0%	Avira URL Cloud	safe	
http://https://49Z9TKhGLJ3VymNKQj.org	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	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	
http://https://api.ipify.org%GETMozilla/5.0	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://r3.i.lencr.org/0#	0%	URL Reputation	safe	
http://r3.i.lencr.org/0#	0%	URL Reputation	safe	
http://r3.i.lencr.org/0#	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.cavilum.cl	186.64.116.165	true	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
186.64.116.165	mail.cavilum.cl	Chile		52368	ZAMLTDACL	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433199
Start date:	11.06.2021
Start time:	12:47:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO #R58490.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:	26
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.adwa.spyw.evad.winEXE@5/2@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.7% (good quality ratio 1.1%) • Quality average: 52.5% • Quality standard deviation: 44.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:48:12	API Interceptor	813x Sleep call for process: PO #R58490.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
186.64.116.165	Cotizaci#U00f3n.exe	Get hash	malicious	Browse	
	Confirmaci#U00f3n de env#U00edo.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order.exe	Get hash	malicious	Browse	
	Order #6762.exe	Get hash	malicious	Browse	
	Urgent Quote.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	6VIB0nWd6H.exe	Get hash	malicious	Browse	
	67ONSqP4Cl.exe	Get hash	malicious	Browse	
	dKWw5dCC4L.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.cavilum.cl	Cotizaci#U00f3n.exe	Get hash	malicious	Browse	• 186.64.116.165
	Confirmaci#U00f3n de env#U00edo.exe	Get hash	malicious	Browse	• 186.64.116.165
	Purchase Order.exe	Get hash	malicious	Browse	• 186.64.116.165
	Order #6762.exe	Get hash	malicious	Browse	• 186.64.116.165
	Urgent Quote.exe	Get hash	malicious	Browse	• 186.64.116.165
	Quotation.exe	Get hash	malicious	Browse	• 186.64.116.165
	6VIB0nWd6H.exe	Get hash	malicious	Browse	• 186.64.116.165
	67ONSqP4Cl.exe	Get hash	malicious	Browse	• 186.64.116.165
	dKWw5dCC4L.exe	Get hash	malicious	Browse	• 186.64.116.165

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ZAMLTDACL	Cotizaci#U00f3n.exe	Get hash	malicious	Browse	• 186.64.116.165
	Confirmaci#U00f3n de env#U00edo.exe	Get hash	malicious	Browse	• 186.64.116.165
	Purchase Order.exe	Get hash	malicious	Browse	• 186.64.116.165
	Order #6762.exe	Get hash	malicious	Browse	• 186.64.116.165
	Urgent Quote.exe	Get hash	malicious	Browse	• 186.64.116.165
	Quotation.exe	Get hash	malicious	Browse	• 186.64.116.165
	#Ud83d#Udd7b Missed Playback Recording.wav - 1424 592794.htm	Get hash	malicious	Browse	• 186.64.116.45
	Sales_Receipt 5576.xls	Get hash	malicious	Browse	• 186.64.118.235
	OUTSTANDING_INVOICE_Statement_077117.xlsm	Get hash	malicious	Browse	• 186.64.116.95
	file.doc	Get hash	malicious	Browse	• 186.64.118.225
	Ordine -159-pdf.exe	Get hash	malicious	Browse	• 186.64.118.215
	Rep_#_475.xlsm	Get hash	malicious	Browse	• 186.64.116.135
	Subconract 504.xlsm	Get hash	malicious	Browse	• 186.64.116.135
	Webinar.exe	Get hash	malicious	Browse	• 186.64.118.125
	QC-Telecom.exe	Get hash	malicious	Browse	• 186.64.118.125
	Io8ic2291n.doc	Get hash	malicious	Browse	• 190.114.254.163
	k5K4BcM1b5.exe	Get hash	malicious	Browse	• 186.64.118.110
	0QKsIlEBln.exe	Get hash	malicious	Browse	• 186.64.118.110
	KuPBIsrqbO.exe	Get hash	malicious	Browse	• 186.64.118.110
	1D1PBttduH.exe	Get hash	malicious	Browse	• 186.64.118.110

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO #R58490.exe.log

Process:	C:\Users\user\Desktop\PO #R58490.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\PO #R58490.exe.log	
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:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\Desktop\PO #R58490.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.516884488799235
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	PO #R58490.exe
File size:	966656
MD5:	5cff42958cd317e239d575732f7f9114
SHA1:	dec2ad475f2989f5096e02e00b45b265dd10c8c0
SHA256:	8636a1af1afb3fa83c218cbc4a18f37782b835d4ab8b27148d6f99cb849453a3
SHA512:	43cde418b8aa6d0626eb861e980bdeab3b82f472ac56b1e5aaa43f676e7203ecedd1f48813168f82a08aec7665e1fd04fb59586ea32b1679188a572a70c3b11c
SSDEEP:	12288:j4ZHNvC3A163SoAPBsFHDEp4rcVyfab52ZM4e/ZUdtb:jKHNvGAoxFHDEMY92NeBUdt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....2... ...@....@.. .....@.....@.....

File Icon

Icon Hash:	8c8caa8e9692aa00

Static PE Info

General

Entrypoint:	0x4c32fe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C28A90 [Thu Jun 10 21:56:32 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc1304	0xc1400	False	0.897549371362	data	7.85720013511	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xc4000	0x1e8	0x200	False	0.861328125	data	6.62101963076	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x2a380	0x2a400	False	0.12430658284	data	4.17130427114	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf2000	0xc	0x200	False	0.041015625	data	0.0776331623432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 12:49:56.910500050 CEST	192.168.2.3	8.8.8.8	0x8c7	Standard query (0)	mail.cavilum.cl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 12:49:57.063219070 CEST	8.8.8.8	192.168.2.3	0x8c7	No error (0)	mail.cavilum.cl		186.64.116.165	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 12:49:57.825237989 CEST	587	49739	186.64.116.165	192.168.2.3	220-blue125.dnsmisitio.net ESMTP Exim 4.93 #2 Fri, 11 Jun 2021 06:49:57 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 11, 2021 12:49:57.826041937 CEST	49739	587	192.168.2.3	186.64.116.165	EHLO 980108
Jun 11, 2021 12:49:58.092140913 CEST	587	49739	186.64.116.165	192.168.2.3	250-blue125.dnsmisitio.net Hello 980108 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 11, 2021 12:49:58.092753887 CEST	49739	587	192.168.2.3	186.64.116.165	STARTTLS
Jun 11, 2021 12:49:58.362252951 CEST	587	49739	186.64.116.165	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PO #R58490.exe PID: 5396 Parent PID: 5796

General

Start time:	12:48:10
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\PO #R58490.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO #R58490.exe'
Imagebase:	0x830000
File size:	966656 bytes
MD5 hash:	5CFF42958CD317E239D575732F7F9114
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: 00000001.00000002.214163603.0000000003BB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.214163603.0000000003BB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.213317019.0000000002BEF000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: PO #R58490.exe PID: 4724 Parent PID: 5396

General

Start time:	12:48:14
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\PO #R58490.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PO #R58490.exe
Imagebase:	0x2c0000
File size:	966656 bytes
MD5 hash:	5CFF42958CD317E239D575732F7F9114
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO #R58490.exe PID: 3840 Parent PID: 5396

General

Start time:	12:48:15
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\PO #R58490.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO #R58490.exe
Imagebase:	0x640000
File size:	966656 bytes
MD5 hash:	5CFF42958CD317E239D575732F7F9114
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.211277551.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.211277551.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.469305003.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.469305003.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.474545404.0000000002AE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis

