ID: 532821
Sample Name:
PO4567328901.exe
Cookbook: default.jbs
Time: 18:20:30
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

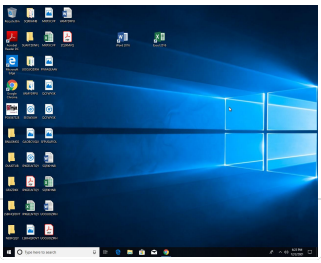
Windows Analysis Report PO4567328901.exe

Overview

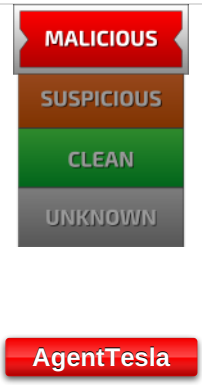
General Information

Sample Name:	PO4567328901.exe
Analysis ID:	532821
MD5:	0346606c84796f9.
SHA1:	4fbae6bc6fe32fa…
SHA256:	9c0608f3b43dc52..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection

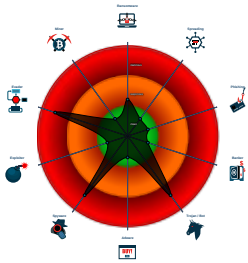


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- .NET source code contains very larg…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- PO4567328901.exe (PID: 7068 cmdline: "C:\Users\user\Desktop\PO4567328901.exe" MD5: 0346606C84796F9A92803E29DAECAD72)
  - PO4567328901.exe (PID: 4180 cmdline: {path} MD5: 0346606C84796F9A92803E29DAECAD72)
  - PO4567328901.exe (PID: 6124 cmdline: {path} MD5: 0346606C84796F9A92803E29DAECAD72)
  - PO4567328901.exe (PID: 3184 cmdline: {path} MD5: 0346606C84796F9A92803E29DAECAD72)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "zspamming@modularelect.com",
  "Password": "successman12@",
  "Host": "mail.modularelect.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.703382608.00000000035F9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.703382608.00000000035F9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000000.692121481.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.692121481.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000000.693283829.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.PO4567328901.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.0.PO4567328901.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PO4567328901.exe.37766d8.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO4567328901.exe.37766d8.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.0.PO4567328901.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

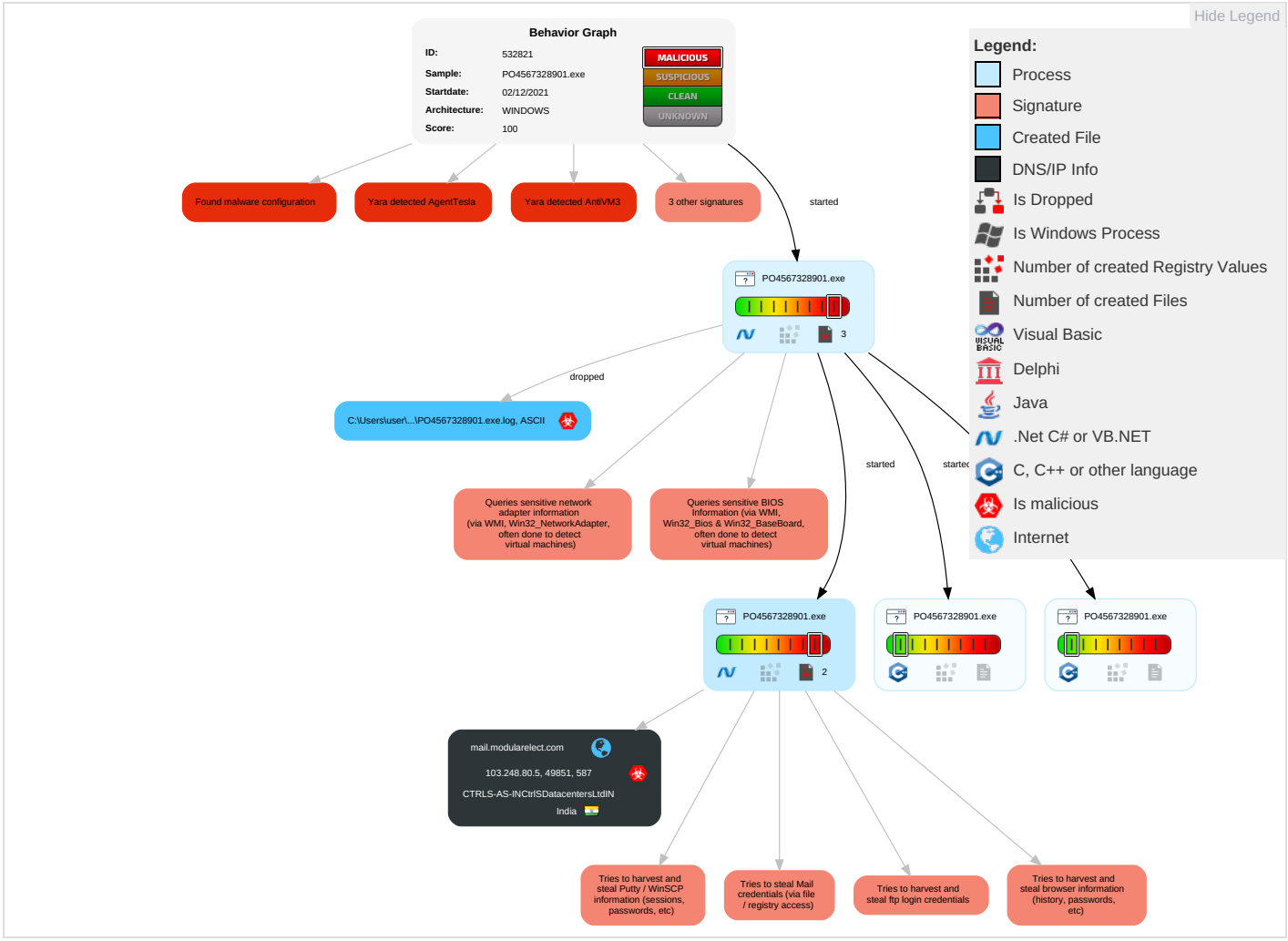
Remote Access Functionality:

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	Path Interception	Process Injection 1 2	Masquerading 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	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1
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	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 1 1
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	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 4	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	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

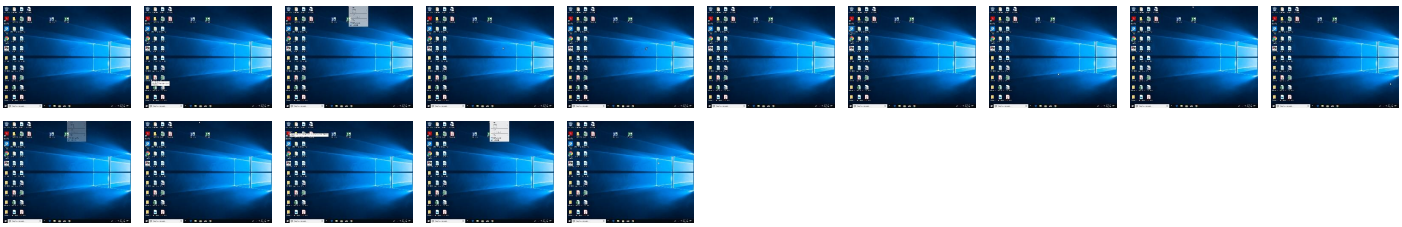
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO4567328901.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.PO4567328901.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.PO4567328901.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.2.PO4567328901.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.PO4567328901.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.PO4567328901.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.PO4567328901.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://mail.modularelect.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://pdvOKN.com	0%	Avira URL Cloud	safe	
http://https://ngLbihuDlAdBVmL.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.modularelect.com	103.248.80.5	true	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.248.80.5	mail.modularelect.com	India		18229	CTRLS-AS-INCtrlSDatacentersLtdIN	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532821
Start date:	02.12.2021
Start time:	18:20:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO4567328901.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:	18
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@7/1@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.2% (good quality ratio 0.8%) • Quality average: 43.2% • Quality standard deviation: 33.1%
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
18:21:32	API Interceptor	691x Sleep call for process: PO4567328901.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.248.80.5	PO#67890345201.exe	Get hash	malicious	Browse	
	New order.exe	Get hash	malicious	Browse	
	1089765423012021_inquiry.exe	Get hash	malicious	Browse	
	PO2018975601.exe	Get hash	malicious	Browse	
	Payment details.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	PO8805545321.exe	Get hash	malicious	Browse	
	Swift.exe	Get hash	malicious	Browse	
	PO801445976.exe	Get hash	malicious	Browse	
	PO-101524309.exe	Get hash	malicious	Browse	
	PO110629.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.modularelect.com	PO#67890345201.exe	Get hash	malicious	Browse	• 103.248.80.5
	New order.exe	Get hash	malicious	Browse	• 103.248.80.5
	1089765423012021_inquiry.exe	Get hash	malicious	Browse	• 103.248.80.5
	PO2018975601.exe	Get hash	malicious	Browse	• 103.248.80.5
	MT103_SWIFT ADVICE.exe	Get hash	malicious	Browse	• 103.248.80.5
	Payment details.exe	Get hash	malicious	Browse	• 103.248.80.5

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase order.exe	Get hash	malicious	Browse	• 103.248.80.5
	SOA.exe	Get hash	malicious	Browse	• 103.248.80.5
	PO8805545321.exe	Get hash	malicious	Browse	• 103.248.80.5
	Swift.exe	Get hash	malicious	Browse	• 103.248.80.5
	PO801445976.exe	Get hash	malicious	Browse	• 103.248.80.5
	PO-101524309.exe	Get hash	malicious	Browse	• 103.248.80.5
	PO110629.exe	Get hash	malicious	Browse	• 103.248.80.5
	Purchase order.exe	Get hash	malicious	Browse	• 209.99.40.222
	PO#101873452021.exe	Get hash	malicious	Browse	• 209.99.40.222

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CTRLS-AS-INCtrlSDatacentersLtdIN	SecuriteInfo.com.Zum.Androm.1.23035.exe	Get hash	malicious	Browse	• 219.90.65.155
	PO#67890345201.exe	Get hash	malicious	Browse	• 103.248.80.5
	New order.exe	Get hash	malicious	Browse	• 103.248.80.5
	1089765423012021_inquiry.exe	Get hash	malicious	Browse	• 103.248.80.5
	Partial Shipment.exe	Get hash	malicious	Browse	• 219.90.65.155
	PO2018975601.exe	Get hash	malicious	Browse	• 103.248.80.5
	Payment details.exe	Get hash	malicious	Browse	• 103.248.80.5
	Purchase order.exe	Get hash	malicious	Browse	• 103.248.80.5
	SOA.exe	Get hash	malicious	Browse	• 103.248.80.5
	Confirm.16451.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	PO8805545321.exe	Get hash	malicious	Browse	• 103.248.80.5
	Swift.exe	Get hash	malicious	Browse	• 103.248.80.5
	arm7	Get hash	malicious	Browse	• 14.197.171.139
	BookingXConfirm-11401.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	06799.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	06799.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Rooms_requirement.7149.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Rooms_requirement.7149.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Rooms_requirement 17757.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Rooms_requirement 17757.xlsb	Get hash	malicious	Browse	• 103.117.180.99

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO4567328901.exe.log

Process:	C:\Users\user\Desktop\PO4567328901.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO4567328901.exe.log	
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.40179576148845
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:	PO4567328901.exe
File size:	615936
MD5:	0346606c84796f9a92803e29daecad72
SHA1:	4fbae6bc6fe32fa19088ea77969f1c6de354d18c
SHA256:	9c0608f3b43dc5252841b632ed93c76252e712464be27e8932e10c86f19a8f07
SHA512:	c54989f63f8629d7b3669614dd70ed6e9b6085988160617752f61737374e6c73632b13ed19a64dfd829a4a46f6facf76fed2fc192c0e133a07bb2701c384ae90
SSDEEP:	12288:3T+m3eYS8uhGwJvAvWx43TtOD4VHnymXlhGBGrq:QjGyAOx43hOEVHyQ1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...t.....P..f..... .....@.. .....@.....

File Icon

Icon Hash:	00130d31155d7e00

Static PE Info

General

Entrypoint:	0x48851e
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:	0xEB1F9274 [Sat Jan 1 10:07:48 2095 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	0x86524	0x86600	False	0.810913880814	data	7.62123130094	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0xfb20	0xfc00	False	0.272305927579	data	3.44750366842	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9a000	0xc	0x200	False	0.044921875	data	0.101910425663	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
Dec 2, 2021 18:23:24.428626060 CET	192.168.2.4	8.8.8.8	0x890b	Standard query (0)	mail.modularelect.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 18:23:24.448544979 CET	8.8.8.8	192.168.2.4	0x890b	No error (0)	mail.modularelect.com		103.248.80.5	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 18:23:25.797975063 CET	587	49851	103.248.80.5	192.168.2.4	220-bom15.balasai.com ESMTP Exim 4.94.2 #2 Thu, 02 Dec 2021 22:53:27 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Dec 2, 2021 18:23:25.798446894 CET	49851	587	192.168.2.4	103.248.80.5	EHLO 061544
Dec 2, 2021 18:23:25.942393064 CET	587	49851	103.248.80.5	192.168.2.4	250-bom15.balasai.com Hello 061544 [84.17.52.65] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Dec 2, 2021 18:23:25.942991018 CET	49851	587	192.168.2.4	103.248.80.5	STARTTLS
Dec 2, 2021 18:23:26.090584993 CET	587	49851	103.248.80.5	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PO4567328901.exe PID: 7068 Parent PID: 900

General

Start time:	18:21:26
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\PO4567328901.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO4567328901.exe"
Imagebase:	0x100000
File size:	615936 bytes
MD5 hash:	0346606C84796F9A92803E29DAECAD72
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: 00000000.00000002.703382608.00000000035F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.703382608.00000000035F9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: PO4567328901.exe PID: 4180 Parent PID: 7068

General

Start time:	18:21:36
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\PO4567328901.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x190000
File size:	615936 bytes
MD5 hash:	0346606C84796F9A92803E29DAECAD72
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO4567328901.exe PID: 6124 Parent PID: 7068

General

Start time:	18:21:37
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\PO4567328901.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x100000
File size:	615936 bytes
MD5 hash:	0346606C84796F9A92803E29DAECAD72
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO4567328901.exe PID: 3184 Parent PID: 7068

General

Start time:	18:21:39
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\PO4567328901.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x660000
File size:	615936 bytes
MD5 hash:	0346606C84796F9A92803E29DAECAD72
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: 00000006.00000000.692121481.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.692121481.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.693283829.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.693283829.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.931868286.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.931868286.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.691722265.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.691722265.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.692643912.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.692643912.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.933223406.0000000002A71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.933223406.0000000002A71000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis