ID: 358415
Sample Name: PO45678.exe
Cookbook: default.jbs
Time: 15:36:25
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report PO45678.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 4
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Compliance: 5
System Summary: 5
Hooking and other Techniques for Hiding and Protection: 5
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 14
General 14
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 17
Sections 17
Resources 17

Imports 17
Version Infos 17
Network Behavior 18
UDP Packets 18
DNS Queries 19
DNS Answers 19
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: PO45678.exe PID: 6392 Parent PID: 5704 20
General 20
File Activities 20
File Created 20
File Written 20
File Read 21
Registry Activities 22
Analysis Process: InstallUtil.exe PID: 6708 Parent PID: 6392 22
General 22
File Activities 22
File Created 22
File Read 23
Disassembly 23
Code Analysis 23

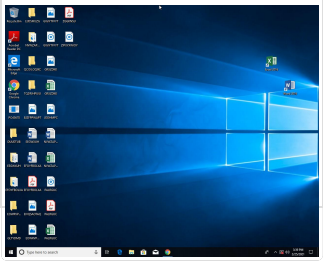
Analysis Report PO45678.exe

Overview

General Information

Sample Name:	PO45678.exe
Analysis ID:	358415
MD5:	0f3ca465173914c..
SHA1:	46dded33d12784..
SHA256:	400b1bf4c7139f7..
Tags:	exe Hostgator
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

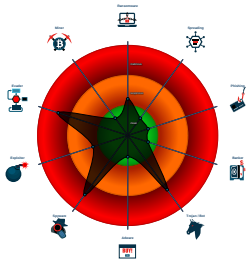
AgentTesla

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

Signatures

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

Classification



Startup

- **System is w10x64**
- PO45678.exe (PID: 6392 cmdline: 'C:\Users\user\Desktop\PO45678.exe' MD5: 0F3CA465173914C361362A754A6BF65E)
  - InstallUtil.exe (PID: 6708 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "box@alscotop.comgodisgreatmail.privateemail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.262870817.0000000003D1A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.494036078.0000000002F71000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.494036078.0000000002F71000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000004.00000002.490156222.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.263060829.0000000003E8B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 4 entries

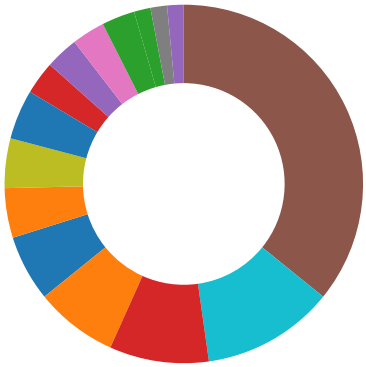
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PO45678.exe.3db3caa.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO45678.exe.3de9b8a.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO45678.exe.3e8b7da.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.InstallUtil.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO45678.exe.3e1fa5a.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

System Summary:

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

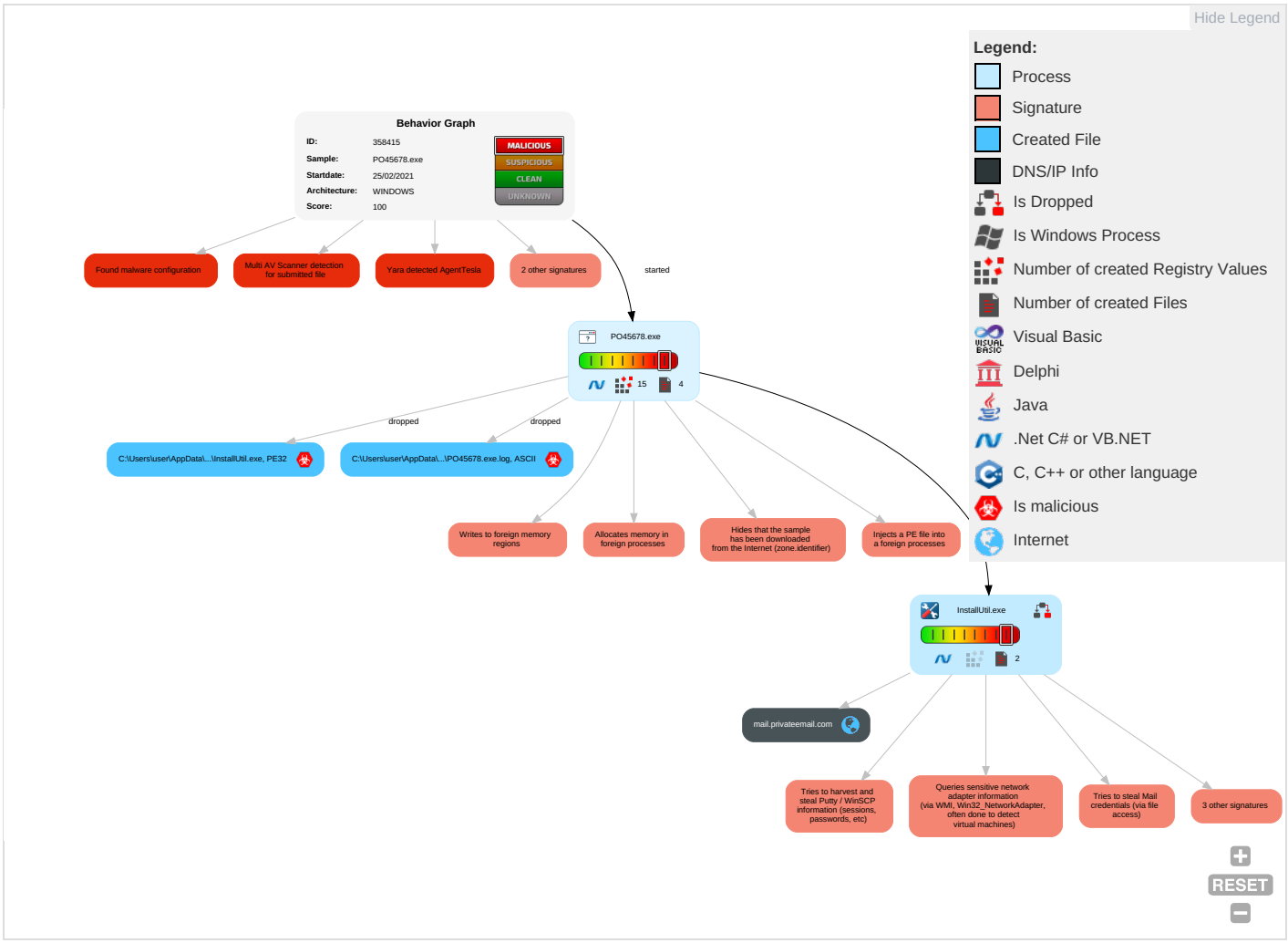
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts 1	Windows Management Instrumentation 2 1 1	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 3 1 2	Obfuscated Files or Information 2	Credentials in Registry 1	Security Software Discovery 1 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Virtualization/Sandbox Evasion 1 3	Distributed Component Object Model	Input Capture 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

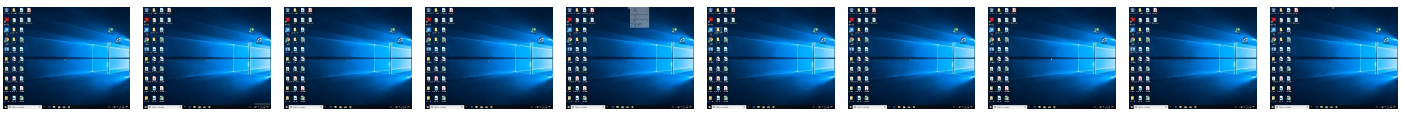
Behavior Graph



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
PO45678.exe	21%	ReversingLabs	Win32.Trojan.Wacatac	
PO45678.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://oAv8kfbDtujMAmvvMu95.org	0%	Avira URL Cloud	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://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	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://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://crl.comodoca.c	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g)	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://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%tordir%%ha	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://https://api.ipify.org%H	0%	Avira URL Cloud	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://ns.adobe.c/g%%	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://SEqkTC.com	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/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	

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://oAv8kfbDtujMAmvvMu95.org	InstallUtil.exe, 00000004.00000002.494036078.0000000002F7100.00000004.00000001.sdmp, InstallUtil.exe, 00000004.00000002.495545429.0000000003270000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	InstallUtil.exe, 00000004.00000002.495371195.0000000003245000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	InstallUtil.exe, 00000004.00000002.494036078.0000000002F7100.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	InstallUtil.exe, 00000004.00000002.494036078.0000000002F7100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	InstallUtil.exe, 00000004.00000002.495371195.0000000003245000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.comodoca.c	InstallUtil.exe, 00000004.00000002.499962081.0000000006BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.c/g)	PO45678.exe, 00000000.00000003.236907309.0000000008EF3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	InstallUtil.exe, 00000004.00000002.495371195.0000000003245000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	InstallUtil.exe, 00000004.00000002.494036078.0000000002F7100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	PO45678.exe, 00000000.00000002.257428591.0000000000902000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	PO45678.exe, 00000000.00000002.257428591.0000000000902000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%H	InstallUtil.exe, 00000004.00000002.494036078.0000000002F7100.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	InstallUtil.exe, 00000004.00000002.494036078.0000000002F7100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ns.adobe.c/g%%	PO45678.exe, 00000000.00000003.256003842.0000000008EFB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	PO45678.exe, 00000000.00000002.257428591.0000000000902000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g	PO45678.exe, 00000000.00000003.244413137.0000000008EF3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://SEqkTC.com	InstallUtil.exe, 00000004.00000002.494036078.0000000002F7100.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	PO45678.exe, 00000000.00000002.257428591.0000000000902000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gsr202	PO45678.exe, 00000000.00000002.257428591.0000000000902000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	PO45678.exe, 00000000.00000002.257428591.0000000000902000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.privateemail.com	InstallUtil.exe, 00000004.00000002.495371195.000000000324500 0.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO45678.exe, 00000000.00000002.258342945.0000000002491000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PO45678.exe, 00000000.00000002.262870817.0000000003D1A000.00000004.00000001.sdmp, InstallUtil.exe, 00000004.00000002.490156222.0000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/WebPage	PO45678.exe, 00000000.00000002.258461700.00000000024C2000.00000004.00000001.sdmp, PO45678.exe, 00000000.00000002.258539906.00000000024D8000.00000004.00000001.sdmp	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358415
Start date:	25.02.2021
Start time:	15:36:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO45678.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:	25
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@3/2@1/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6% (good quality ratio 3.5%) • Quality average: 27.6% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 51.11.168.160, 13.64.90.137, 13.88.21.125, 168.61.161.212, 23.211.6.115, 216.58.206.68, 40.88.32.150, 23.218.208.56, 51.104.144.132, 51.103.5.186, 2.20.142.209, 2.20.142.210, 92.122.213.194, 92.122.213.247, 20.54.26.129, 84.53.167.113 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, ocsp.digicert.com, wildcard.weather.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:37:41	API Interceptor	1x Sleep call for process: PO45678.exe modified
15:37:55	API Interceptor	611x Sleep call for process: InstallUtil.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.privateemail.com	OFFER.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.W32.MSIL_Kryptik.COP.genEldorado.31763.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.TR.AD.AgentTesla.yuenz.18281.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL_DELI.EXE	Get hash	malicious	Browse	• 198.54.122.60
	4MyakrzyM2.exe	Get hash	malicious	Browse	• 198.54.122.60
	yJMBdPH5Uj.exe	Get hash	malicious	Browse	• 198.54.122.60
	3KPjI4YLvT.exe	Get hash	malicious	Browse	• 198.54.122.60
	qUvEiyPz1P.exe	Get hash	malicious	Browse	• 198.54.122.60
	Z5clpoFy0o.exe	Get hash	malicious	Browse	• 198.54.122.60
	fNhla8Q8Ll.exe	Get hash	malicious	Browse	• 198.54.122.60
	Document_25102020.doc	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Win32.32289.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Win32.18332.exe	Get hash	malicious	Browse	• 198.54.122.60
	s3HAoqkLuR.exe	Get hash	malicious	Browse	• 198.54.122.60
	Request For Quotation RFQ 53253quote Pricelist of Order.doc	Get hash	malicious	Browse	• 198.54.122.60
	Order Specification.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER.doc	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.FileRepMalware.4966.exe	Get hash	malicious	Browse	• 198.54.122.60
	dwXuNeEeql.exe	Get hash	malicious	Browse	• 198.54.122.60
	DG6PQDuCfL.exe	Get hash	malicious	Browse	• 198.54.122.60

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	HblVSJaQa1.exe	Get hash	malicious	Browse	
	DEBIT NOTE.exe	Get hash	malicious	Browse	
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	
	New Order 632487 PDF.exe	Get hash	malicious	Browse	
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASERAL FERDAN.exe	Get hash	malicious	Browse	
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASERAL FERDAN.exe	Get hash	malicious	Browse	
	REQUEST FOR OFFER.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	v2.exe	Get hash	malicious	Browse	
	MPO-003234.exe	Get hash	malicious	Browse	
	Payment copy.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	YKRAB010B_KHE_Preminary Packing List.xlsx.exe	Get hash	malicious	Browse	
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis249E62CF9BAE.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.42841.18110.exe	Get hash	malicious	Browse	
	DETALLE DE TRANSFERENCIA BANCO AGRARO DE COLOMBIA.exe	Get hash	malicious	Browse	
	index_2021-02-18-20_41.exe	Get hash	malicious	Browse	
	XXXXXXXXXXXXX.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO45678.exe.log

Process:	C:\Users\user\Desktop\PO45678.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO45678.exe.log	
Category:	dropped
Size (bytes):	1214
Entropy (8bit):	5.358666369753595
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7K84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoM:MIHK5HKXE1qHbHK5AHKzvKviYHKhQnoH
MD5:	1F3BB210B09FE31192C6A822966919E9
SHA1:	A8715FFF2F9D1BE024F462CF702D1E7F71AA4B4F
SHA-256:	C6B3057777EE46AC3544F9FA829E918CD7EF70E490424616650DDA01BF214043
SHA-512:	26897678275FEFDFD96FCB7F7FAFFD5FB0BC0FEB35C89BEB4BA15D074155A06236E8681A2CA9C9DCFDDF2462644CD3603C3592AB310BA84E3D93C8BF2CE28D5
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Co

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\PO45678.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: HblVSJaQa1.exe, Detection: malicious, Browse • Filename: DEBIT NOTE.exe, Detection: malicious, Browse • Filename: MT SC GUANGZHOU.exe, Detection: malicious, Browse • Filename: MT WOOJIN CHEMS V.2103.exe, Detection: malicious, Browse • Filename: New Order 632487 PDF.exe, Detection: malicious, Browse • Filename: HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe, Detection: malicious, Browse • Filename: HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe, Detection: malicious, Browse • Filename: REQUEST FOR OFFER.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: v2.exe, Detection: malicious, Browse • Filename: MPO-003234.exe, Detection: malicious, Browse • Filename: Payment copy.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: YKRAB010B_KHE_Preminary Packing List.xlsx.exe, Detection: malicious, Browse • Filename: RTM DIAS - CTM.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Artemis249E62CF9BAE.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Packed2.42841.18110.exe, Detection: malicious, Browse • Filename: DETALLE DE TRANSFERENCIA BANCO AGRARO DE COLOMBIA.exe, Detection: malicious, Browse • Filename: index_2021-02-18-20_41.exe, Detection: malicious, Browse • Filename: XXXXXXXXXXXXXX.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.661457990127764

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PO45678.exe
File size:	866304
MD5:	0f3ca465173914c361362a754a6bf65e
SHA1:	46dded33d12784afe77619a20ee65d1939f881b0
SHA256:	400b1bf4c7139f7df22748d627aeb7789dd409ae463a0f8f b7d6fa243065d140
SHA512:	fe35ff76ac0e451c3bd6c643d6714c56974a2faaef2c6ff26 85764e6b363b88d004a819d900e7753cc46097a3109c36 1b2ecfe6882183f2b649bc284603b4fd5
SSDEEP:	12288:2+1YHCIVKyxz33JQ3Krcrlhiz6021uysgKtMuL+Y 8VSpW:2+SCJKrcBgp2lyZTe
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....IRI.....,.....NK... ...`....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d4b4e
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, HIGH_ENTROPY_VA
Time Stamp:	0x49526CC3 [Wed Dec 24 17:09:23 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd4b00	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd6000	0x60e	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	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	0xd2b54	0xd2c00	False	0.641939826142	data	6.67037029793	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0x60e	0x800	False	0.345703125	data	3.62726211385	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd60a0	0x384	data		
RT_MANIFEST	0xd6424	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 2011 GAD?49GE:FHAI578@JB>@<
Assembly Version	1.0.0.0
InternalName	PO45678.exe
FileVersion	7.10.14.17
CompanyName	GAD?49GE:FHAI578@JB>@<
Comments	2II?84J=7>977?I
ProductName	>J<J::@8<I>?JB8
ProductVersion	7.10.14.17
FileDescription	>J<J::@8<I>?JB8
OriginalFilename	PO45678.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:37:06.761845112 CET	54302	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:06.810607910 CET	53	54302	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:06.931421041 CET	53784	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:06.980137110 CET	53	53784	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:07.101974964 CET	65307	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:07.138988972 CET	64344	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:07.153562069 CET	53	65307	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:07.187673092 CET	53	64344	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:07.596024990 CET	62060	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:07.644855976 CET	53	62060	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:08.848843098 CET	61805	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:08.897536993 CET	53	61805	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:10.000252962 CET	54795	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:10.049242020 CET	53	54795	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:11.324085951 CET	49557	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:11.382345915 CET	53	49557	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:11.539911032 CET	61733	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:11.588571072 CET	53	61733	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:13.337769032 CET	65447	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:13.386534929 CET	53	65447	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:16.368733883 CET	52441	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:16.431003094 CET	53	52441	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:16.859111071 CET	62176	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:16.916135073 CET	53	62176	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:16.926395893 CET	59596	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:16.975133896 CET	53	59596	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:20.128809929 CET	65296	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:20.177870035 CET	53	65296	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:21.102575064 CET	63183	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:21.154478073 CET	53	63183	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:22.075711966 CET	60151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:22.132915020 CET	53	60151	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:23.222260952 CET	56969	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:23.270998001 CET	53	56969	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:24.172314882 CET	55161	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:24.229481936 CET	53	55161	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:25.153867006 CET	54757	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:25.202584028 CET	53	54757	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:33.327308893 CET	49992	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:33.385937929 CET	53	49992	8.8.8.8	192.168.2.5
Feb 25, 2021 15:37:50.545897007 CET	60075	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:37:50.594573975 CET	53	60075	8.8.8.8	192.168.2.5
Feb 25, 2021 15:38:01.761070013 CET	55016	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:38:01.809783936 CET	53	55016	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:38:02.337074995 CET	64345	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:38:02.407722950 CET	53	64345	8.8.8.8	192.168.2.5
Feb 25, 2021 15:38:09.504225016 CET	57128	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:38:09.562475920 CET	53	57128	8.8.8.8	192.168.2.5
Feb 25, 2021 15:38:13.899379015 CET	54791	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:38:13.959279060 CET	53	54791	8.8.8.8	192.168.2.5
Feb 25, 2021 15:38:21.249206066 CET	50463	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:38:21.308343887 CET	53	50463	8.8.8.8	192.168.2.5
Feb 25, 2021 15:38:46.156953096 CET	50394	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:38:46.215894938 CET	53	50394	8.8.8.8	192.168.2.5
Feb 25, 2021 15:38:47.689454079 CET	58530	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:38:47.738306046 CET	53	58530	8.8.8.8	192.168.2.5
Feb 25, 2021 15:38:51.317082882 CET	53813	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:38:51.374279022 CET	53	53813	8.8.8.8	192.168.2.5
Feb 25, 2021 15:39:18.096446991 CET	63732	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:39:18.156415939 CET	53	63732	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 15:39:18.096446991 CET	192.168.2.5	8.8.8.8	0x9e87	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)

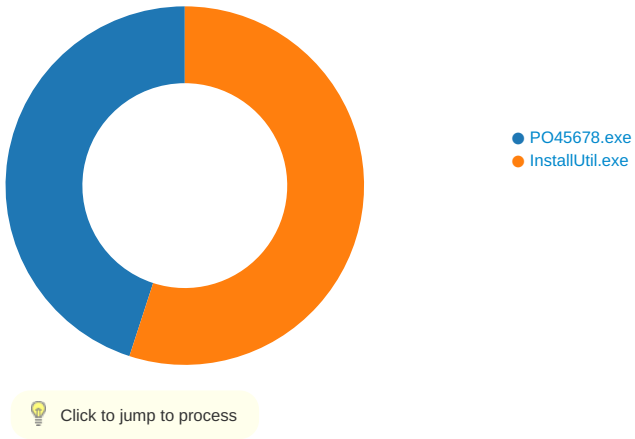
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 15:39:18.156415939 CET	8.8.8.8	192.168.2.5	0x9e87	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO45678.exe PID: 6392 Parent PID: 5704

General

Start time:	15:37:27
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\PO45678.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO45678.exe'
Imagebase:	0xa0000
File size:	866304 bytes
MD5 hash:	0F3CA465173914C361362A754A6BF65E
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: 00000000.00000002.262870817.0000000003D1A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.263060829.0000000003E8B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.262927323.0000000003D7D000.00000004.00000001.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	6DAECF06	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	6DAECF06	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.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	45102E3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO45678.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDFC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0	41064	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 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 07 5a 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 54 00 00 00 0c 00 00 00 00 00 00 86 72 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 9a 80 01 00 03 00 60 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....Z.Z.......... ....0..T...........r... ....@.. ....`.................	success or wait	1	45102E3	CopyFileExW
C:\Users\user\AppData\Local\Mi crosoft\CLR_v4.0_32\UsageLogs\PO45678.exe.log	unknown	1214	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,"Win RT", "NotApp",1..2,"System.Win dows.Forms, Version=4.0.0.0, Cultur e=neutral, PublicKeyToken=b77a 5c561934e089",0..3,"Syste m, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c5 61934e 089","C:\Windows\assembl y\NativeImages_v4.0.3	success or wait	1	6DDFC907	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	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DACCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C931B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: InstallUtil.exe PID: 6708 Parent PID: 6392

General

Start time:	15:37:38
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0xc80000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
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: 00000004.00000002.494036078.0000000002F71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.494036078.0000000002F71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.490156222.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

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	6DAECF06	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	6DAECF06	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	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C931B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C931B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C931B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C931B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c7b58468-a762-4739-be9b-b09c8ec5a988	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C931B4F	ReadFile

Disassembly

Code Analysis