ID: 356523
Sample Name: MPO-003234.exe
Cookbook: default.jbs
Time: 09:28:13
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

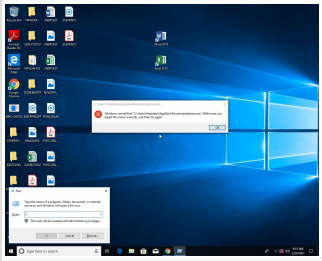
Analysis Report MPO-003234.exe

Overview

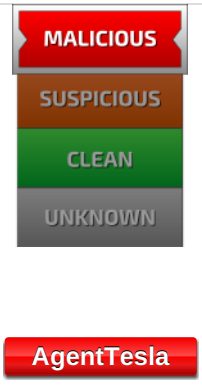
General Information

Sample Name:	MPO-003234.exe
Analysis ID:	356523
MD5:	8bc8526fbaafbac..
SHA1:	7b23c7209b8f37b.
SHA256:	cfe1f69c2984de3..
Tags:	exe

Most interesting Screenshot:



Detection



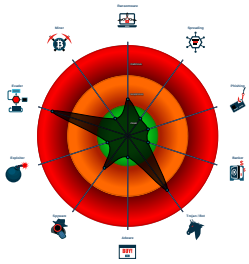
AgentTesla

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

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- Creates multiple autostart registry ke…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Writes to foreign memory regions

Classification



Startup

- **System is w10x64**
- MPO-003234.exe (PID: 6584 cmdline: 'C:\Users\user\Desktop\MPO-003234.exe' MD5: 8BC8526FBAAFBAC33118EE652AC97DA6)
  - cmd.exe (PID: 6720 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'neil' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\badman.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 6764 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'neil' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\badman.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - badman.exe (PID: 7052 cmdline: 'C:\Users\user\AppData\Roaming\badman.exe' MD5: 8BC8526FBAAFBAC33118EE652AC97DA6)
    - InstallUtil.exe (PID: 6980 cmdline: C:\Users\user~1\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.432474443.0000000003EAA000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000019.00000002.497669421.00000000029B1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000019.00000002.497669421.00000000029B1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000010.00000002.432224674.0000000003D39000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.334911428.00000000049BE000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 9 entries

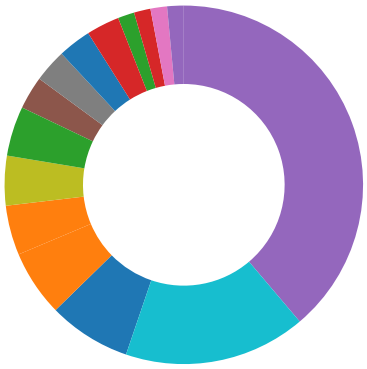
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.MPO-003234.exe.4b021b8.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.2.badman.exe.3ee08b0.6.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.2.badman.exe.3e089da.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.MPO-003234.exe.4acc202.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.MPO-003234.exe.4a602a2.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

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

Boot Survival:

Creates multiple autostart registry keys

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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:

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

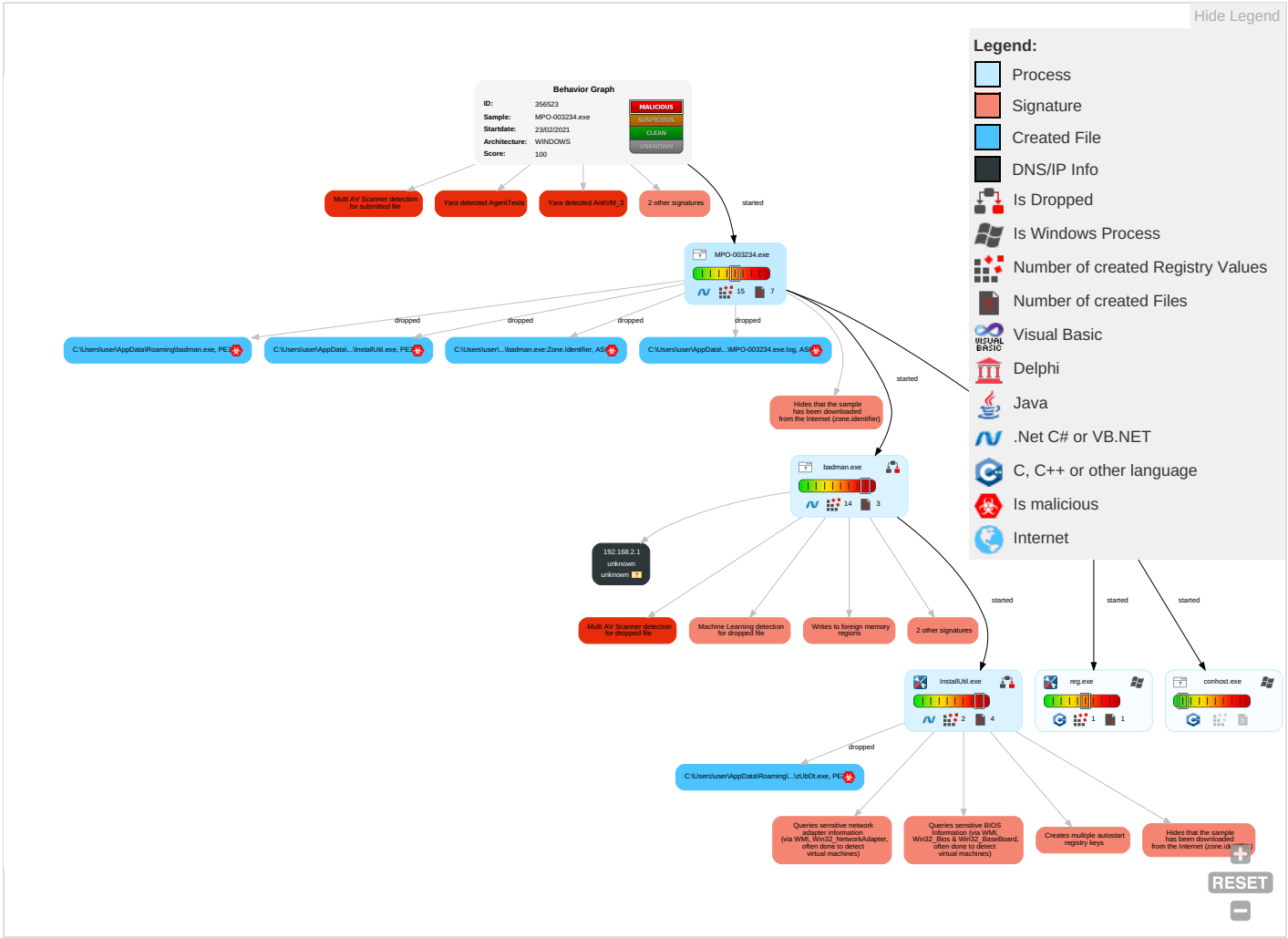
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Valid Accounts 1	Windows Management Instrumentation 2 1 1	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1	Input Capture 1	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	En Ch
Default Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1 1	Access Token Manipulation 1	Obfuscated Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ju
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 2 1 2	Software Packing 1	Security Account Manager	System Information Discovery 1 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	St
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1 1	Masquerading 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Pr Im
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Valid Accounts 1	LSA Secrets	Security Software Discovery 2 2 1	SSH	Keylogging	Data Transfer Size Limits	Fa Ch
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Modify Registry 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 4	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2 1 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr

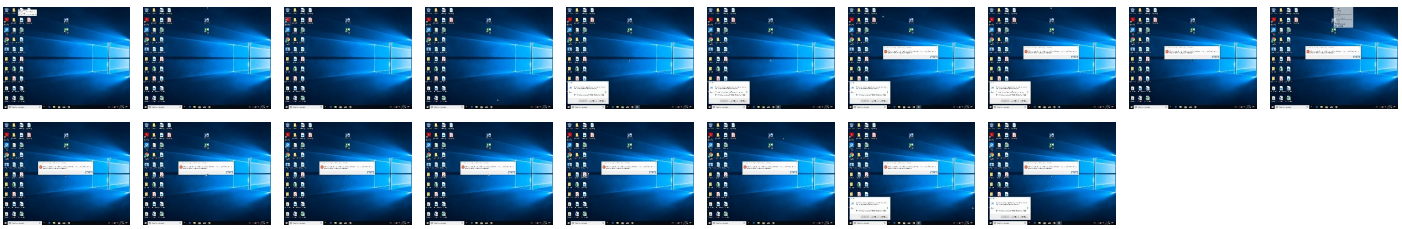
Behavior Graph

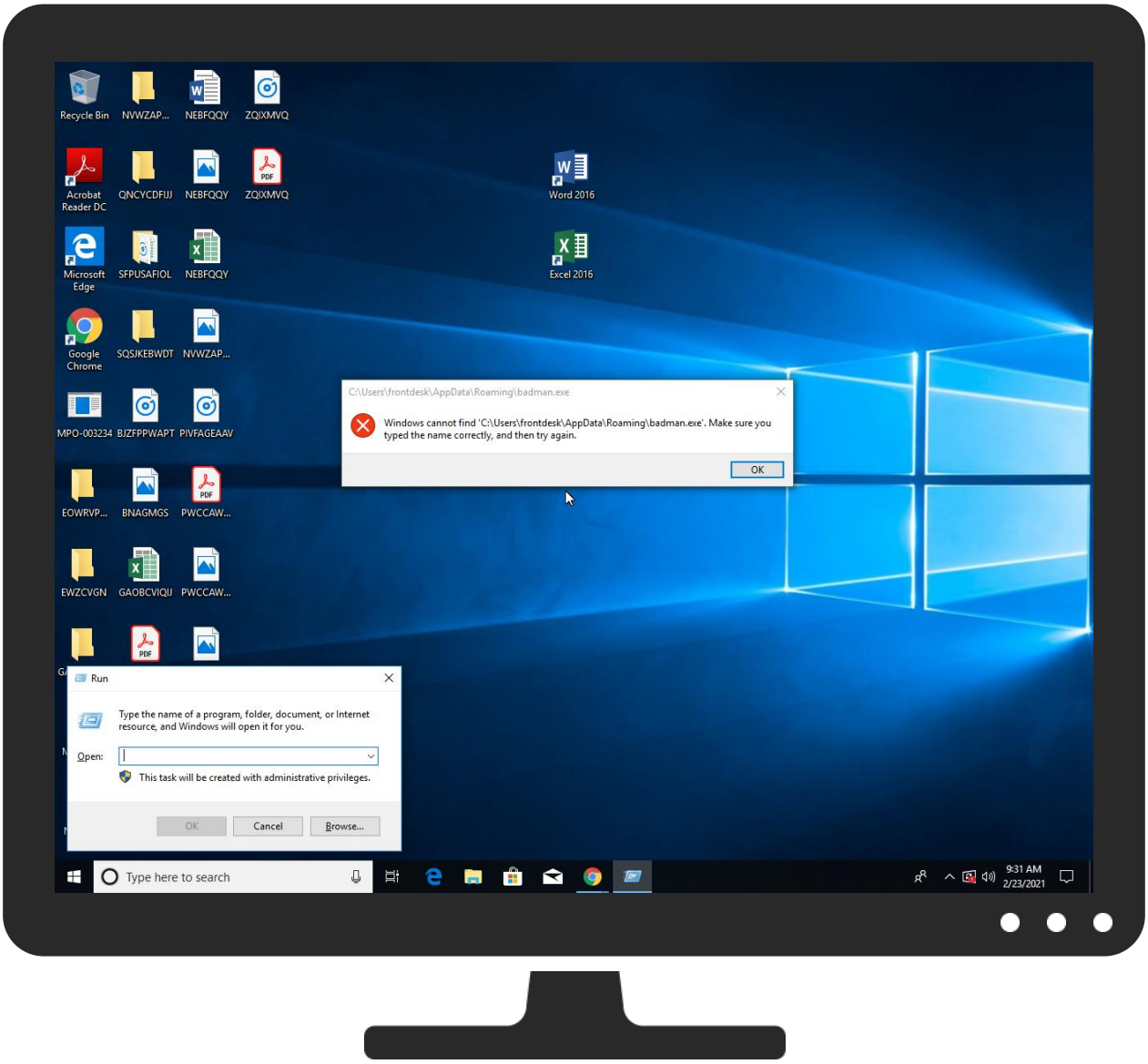


Screenshots

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
MPO-003234.exe	24%	Virustotal		Browse
MPO-003234.exe	19%	ReversingLabs	Win32.Trojan.Wacatac	
MPO-003234.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\badman.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\badman.exe	19%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\user\AppData\Roaming\zUbDt\zUbDt.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\zUbDt\zUbDt.exe	0%	ReversingLabs		

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://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://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://wqDPxI.com	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://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://ns.adobe.c/gp	0%	Avira URL Cloud	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://ns.adb	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://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.cobjp	0%	Avira URL Cloud	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://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://ns.adobe.c/g5~	0%	Avira URL Cloud	safe	
http://ns.ado/1p	0%	Avira URL Cloud	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://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

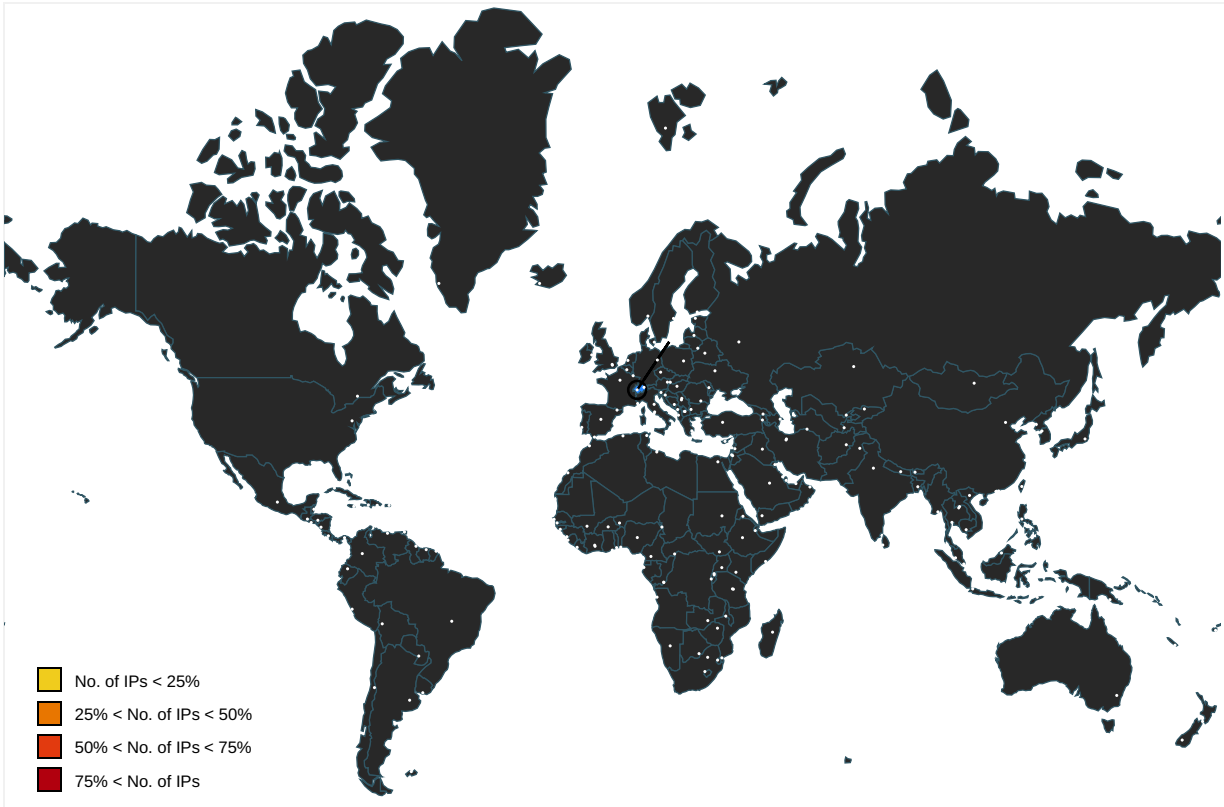
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	InstallUtil.exe, 00000019.00000002.497669421.00000000029B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	InstallUtil.exe, 00000019.00000002.497669421.00000000029B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	MPO-003234.exe, 00000000.00000003.329342490.0000000009BEB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://wqDPxI.com	InstallUtil.exe, 00000019.00000002.497669421.00000000029B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	InstallUtil.exe, 00000019.00000002.497669421.00000000029B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	MPO-003234.exe, 00000000.00000003.307873312.000000000136A000.00000004.00000001.sdmp, badman.exe, 00000010.00000002.426421947.000000000092D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/gp	MPO-003234.exe, 00000000.00000003.238711117.0000000009BE4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	MPO-003234.exe, 00000000.00000003.307873312.000000000136A000.00000004.00000001.sdmp, badman.exe, 00000010.00000002.426421947.000000000092D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adb	MPO-003234.exe, 00000000.00000003.238538980.0000000009BE4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	InstallUtil.exe, 00000019.00000002.497669421.00000000029B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ns.adobe.c/g%%	badman.exe, 00000010.00000003.422941176.000000000903D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	MPO-003234.exe, 00000000.00000003.307873312.000000000136A000.00000004.00000001.sdmp, badman.exe, 00000010.00000002.426421947.000000000092D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobjp	MPO-003234.exe, 00000000.00000003.238711117.0000000009BE4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.c/g	MPO-003234.exe, 00000000.00000003.329342490.0000000009BEB000.00000004.00000001.sdmp, badman.exe, 00000010.00000003.347728528.0000000009035000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	MPO-003234.exe, 00000000.00000003.307873312.000000000136A000.00000004.00000001.sdmp, badman.exe, 00000010.00000002.426421947.000000000092D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gsr202	MPO-003234.exe, 00000000.00000003.307873312.000000000136A000.00000004.00000001.sdmp, badman.exe, 00000010.00000002.426421947.000000000092D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pki.goog/repository/0	MPO-003234.exe, 00000000.00000003.307873312.000000000136A000.00000004.00000001.sdmp, badman.exe, 00000010.00000002.426421947.000000000092D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g5~	badman.exe, 00000010.00000003.347207533.0000000009035000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.ado/1p	MPO-003234.exe, 00000000.00000003.238711117.0000000009BE4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	MPO-003234.exe, 00000000.00000002.331380288.00000000030D1000.00000004.00000001.sdmp, badman.exe, 00000010.00000002.426997303.00000000024B1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	MPO-003234.exe, 00000000.00000002.334911428.00000000049BE000.00000004.00000001.sdmp, badman.exe, 00000010.00000002.432474443.0000000003EAA000.00000004.00000001.sdmp, InstallUtil.exe, 00000019.00000002.492241366.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/WebPage	MPO-003234.exe, 00000000.00000002.331426011.0000000003102000.00000004.00000001.sdmp, badman.exe, 00000010.00000002.427101971.00000000024E2000.00000004.00000001.sdmp	false		high
http://ns.ado/1	MPO-003234.exe, 00000000.00000003.329342490.0000000009BEB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356523
Start date:	23.02.2021
Start time:	09:28:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MPO-003234.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:	31
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.evad.winEXE@10/6@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.6% (good quality ratio 1.8%) • Quality average: 24.9% • Quality standard deviation: 30.8%
HCA Information:	• Successful, ratio: 89% • 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, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 51.11.168.160, 52.255.188.83, 92.122.145.220, 104.43.193.48, 168.61.161.212, 142.250.185.164, 23.210.248.85, 93.184.221.240, 51.103.5.186, 204.79.197.200, 13.107.21.200, 51.104.144.132, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): 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, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many 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
09:29:09	API Interceptor	194x Sleep call for process: MPO-003234.exe modified
09:29:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run neil C:\Users\user\AppData\Roaming\badman.exe
09:29:20	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run neil C:\Users\user\AppData\Roaming\badman.exe
09:29:58	API Interceptor	222x Sleep call for process: badman.exe modified
09:30:48	API Interceptor	135x Sleep call for process: InstallUtil.exe modified
09:30:59	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run zUbDt C:\Users\user\AppData\Roaming\zUbDt\zUbDt.exe
09:31:07	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run zUbDt C:\Users\user\AppData\Roaming\zUbDt\zUbDt.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\zUbDt\zUbDt.exe	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	
	XXXXXXXXXXXXXX.exe	Get hash	malicious	Browse	
	IMG_144907.exe	Get hash	malicious	Browse	
	VIIIIIIIIIIIIC.exe	Get hash	malicious	Browse	
	lQN1zlLSGa.exe	Get hash	malicious	Browse	
	Sorted Properties.exe	Get hash	malicious	Browse	
	DB_DHL_AWB_00117390021_AD03990399003920032.exe	Get hash	malicious	Browse	
	New Order 83329 PDF.exe	Get hash	malicious	Browse	
	NEW TENDER_ORDER 900930390097733000999_10_02_2021.exe	Get hash	malicious	Browse	
	Proforma Invoice February.exe	Get hash	malicious	Browse	
	jmsg.exe	Get hash	malicious	Browse	
	FORM DB_DHL_AWB_0299202920920399930293332 21AD.exe	Get hash	malicious	Browse	
	Mortgage Description.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	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	
	XXXXXXXXXXXXXX.exe	Get hash	malicious	Browse	
	IMG_144907.exe	Get hash	malicious	Browse	
	VIIIIIIIIIIIIC.exe	Get hash	malicious	Browse	
	lQN1zlLSGa.exe	Get hash	malicious	Browse	
	Sorted Properties.exe	Get hash	malicious	Browse	
	DB_DHL_AWB_00117390021_AD03990399003920032.exe	Get hash	malicious	Browse	
	New Order 83329 PDF.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW TENDER_ORDER 900930390097733000999_10_02_2021.exe	Get hash	malicious	Browse	
	Proforma Invoice February.exe	Get hash	malicious	Browse	
	jmsg.exe	Get hash	malicious	Browse	
	FORM DB_DHL_AWB_0299202920920399930293332 21AD.exe	Get hash	malicious	Browse	
	Mortgage Description.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MPO-003234.exe.log	
Process:	C:\Users\user\Desktop\MPO-003234.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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\Microsoft\CLR_v4.0_32\UsageLogs\badman.exe.log	
Process:	C:\Users\user\AppData\Roaming\badman.exe
File Type:	ASCII text, with CRLF line terminators
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:	false
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\MPO-003234.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:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• 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: XXXXXXXXXXXXX.exe, Detection: malicious, Browse • Filename: IMG_144907.exe, Detection: malicious, Browse • Filename: VIIIIIIIIIIIIC.exe, Detection: malicious, Browse • Filename: lQN1zlLSGa.exe, Detection: malicious, Browse • Filename: Sorted Properties.exe, Detection: malicious, Browse • Filename: DB_DHL_AWB_00117390021_AD03990399003920032.exe, Detection: malicious, Browse • Filename: New Order 83329 PDF.exe, Detection: malicious, Browse • Filename: NEW TENDER_ORDER 900930390097733000999_10_02_2021.exe, Detection: malicious, Browse • Filename: Proforma Invoice February.exe, Detection: malicious, Browse • Filename: jmsg.exe, Detection: malicious, Browse • Filename: FORM DB_DHL_AWB_02992029209203993029333221 AD.exe, Detection: malicious, Browse • Filename: Mortgage Description.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

C:\Users\user\AppData\Roaming\badman.exe	
Process:	C:\Users\user\Desktop\MPO-003234.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	877568
Entropy (8bit):	6.6376111502973485
Encrypted:	false
SSDEEP:	12288:woUUhJQ3Krcrlhiz6021uysHmL95K0/Y7n03vSt0BgVb:wvKrcBgp2IyGuK0/Y70f7
MD5:	8BC8526FBAAFBAC33118EE652AC97DA6
SHA1:	7B23C7209B8F37BB32803971C36AB706B4A8E34D
SHA-256:	CFE1F69C2984DE3F5D476DB3CE45AA4D95A8137F0FF1BA07C1B0CECF15075C93
SHA-512:	439595E5CAE6B32B36223DF24D3DE1FA67BD8EE46ED84358D64633DEBA39B4A25DC38DB1BEF947B9C74E4A3226758876A673AEE353D3E94B168E32BE9BCD82 2C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 19%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....P.3K.....X.....w... .....@.. ....`.....v..S..... ..... ..H.....text....W... ...X..... ..`.rsrc.....Z.....@..@.reloc..... .....b.....@..B.....v.....H..... .....).F...<.....*...U...u....d...F....yg.#.".#.P...+.m..\....y.....b...i.)e.W.RmV..p~.f...a.l.5..9 a...E...uR....O.1...&.T.....|F.....e....m~.m.S ..`..... ....y."\+.A:....C.....X.1.b..X..ylg.Z.T.1..I.5Q.S....D..K...../.....1k.t.....2.....bl.Q..\N...dH.E.-....c.E.3.w...W<..".`.8..H.N. .x.m.`.|.y..C.5....#.._...1.).w.a..$.(.1.^.r.:....T.E....<..41.....t....-;]2|.U.zn.Bcr.

C:\Users\user\AppData\Roaming\badman.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\MPO-003234.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Roaming\badman.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\zUbDt\zUbDt.exe	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.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:ZBMs2SqdD86lq8gZZFyViML3an
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: 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: XXXXXXXXXXXXX.exe, Detection: malicious, Browse • Filename: IMG_144907.exe, Detection: malicious, Browse • Filename: VIIIIIIIIIIIIC.exe, Detection: malicious, Browse • Filename: lQN1zlLSGa.exe, Detection: malicious, Browse • Filename: Sorted Properties.exe, Detection: malicious, Browse • Filename: DB_DHL_AWB_00117390021_AD03990399003920032.exe, Detection: malicious, Browse • Filename: New Order 83329 PDF.exe, Detection: malicious, Browse • Filename: NEW TENDER_ORDER 900930390097733000999_10_02_2021.exe, Detection: malicious, Browse • Filename: Proforma Invoice February.exe, Detection: malicious, Browse • Filename: jmsg.exe, Detection: malicious, Browse • Filename: FORM DB_DHL_AWB_0299202929092039993029333221 AD.exe, Detection: malicious, Browse • Filename: Mortgage Description.exe, Detection: malicious, Browse
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):	6.6376111502973485
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:	MPO-003234.exe
File size:	877568
MD5:	8bc8526fbaafbac33118ee652ac97da6
SHA1:	7b23c7209b8f37bb32803971c36ab706b4a8e34d
SHA256:	cfe1f69c2984de3f5d476db3ce45aa4d95a8137f0ff1ba07c1b0cecf15075c93
SHA512:	439595e5cae6b32b36223df24d3de1fa67bd8ee46ed8438d64633deba39b4a25dc38db1bef947b9c74e4a3226758876a673aee353d3e94b168e32be9bcd822c
SSDEEP:	12288:woUUhJQ3Krcrlhiz6021uysHmL95K0/Y7n03vSt0BgVb:wvKrcBgp2IyGuK0/Y70f7

General

File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L... P.3K.................X...........w... ....@.. ....`................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d770e
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:	0x4B33FC50 [Thu Dec 24 23:42:08 2009 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd76b8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x616	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	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	0xd5714	0xd5800	False	0.635758196721	SysEx File -	6.6463233151	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x616	0x800	False	0.349609375	data	3.66123376299	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	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	0xd80a0	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0xd842c	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 E5?5I5:6IG=BH49I2J<;6C
Assembly Version	1.0.0.0
InternalName	Raj.exe
FileVersion	7.11.14.18
CompanyName	E5?5I5:6IG=BH49I2J<;6C
Comments	AF95E:7>3632AD@G@9
ProductName	5EGCD4ACFEGCGA7;?A2
ProductVersion	7.11.14.18
FileDescription	5EGCD4ACFEGCGA7;?A2
OriginalFilename	Raj.exe

Network Behavior

UDP Packets

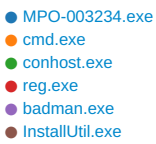
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:28:55.101944923 CET	61242	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:28:55.126588106 CET	58562	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:28:55.150718927 CET	53	61242	8.8.8.8	192.168.2.7
Feb 23, 2021 09:28:55.176758051 CET	56590	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:28:55.178112030 CET	53	58562	8.8.8.8	192.168.2.7
Feb 23, 2021 09:28:55.225357056 CET	53	56590	8.8.8.8	192.168.2.7
Feb 23, 2021 09:28:58.107235909 CET	60501	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:28:58.172266960 CET	53	60501	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:01.079483032 CET	53775	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:01.130961895 CET	53	53775	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:02.069763899 CET	51837	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:02.118594885 CET	53	51837	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:03.205269098 CET	55411	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:03.254051924 CET	53	55411	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:04.208017111 CET	63668	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:04.257010937 CET	53	63668	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:04.298306942 CET	54640	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:04.357367039 CET	53	54640	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:04.622805119 CET	58739	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:04.671376944 CET	53	58739	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:04.687341928 CET	60338	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:04.736023903 CET	53	60338	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:05.337219954 CET	58717	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:05.386883020 CET	53	58717	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:09.311932087 CET	59762	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:09.360644102 CET	53	59762	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:10.319719076 CET	54329	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:10.368494987 CET	53	54329	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:11.290817022 CET	58052	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:11.339703083 CET	53	58052	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:12.295756102 CET	54008	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:12.344485044 CET	53	54008	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:13.266511917 CET	59451	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:13.318264008 CET	53	59451	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:14.236737967 CET	52914	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:14.285512924 CET	53	52914	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:15.220974922 CET	64569	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:15.279983044 CET	53	64569	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:16.285648108 CET	52816	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:16.345727921 CET	53	52816	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:18.440898895 CET	50781	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:18.493890047 CET	53	50781	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:20.617420912 CET	54230	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:20.668917894 CET	53	54230	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:21.480077982 CET	54911	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:21.540224075 CET	53	54911	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:22.158849001 CET	49958	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:22.207703114 CET	53	49958	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:24.030318022 CET	50860	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:24.081851959 CET	53	50860	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:30.098707914 CET	50452	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:30.158178091 CET	53	50452	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:31.191107988 CET	59730	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:31.239974022 CET	53	59730	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:32.180849075 CET	59310	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:32.233937025 CET	53	59310	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:34.110220909 CET	51919	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:34.160742998 CET	53	51919	8.8.8.8	192.168.2.7

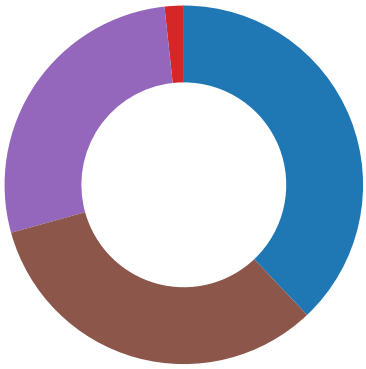
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:29:50.333293915 CET	64296	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:50.382025003 CET	53	64296	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:51.508300066 CET	56680	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:51.556991100 CET	53	56680	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:53.156857014 CET	58820	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:53.208484888 CET	53	58820	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:53.660867929 CET	60983	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:53.713583946 CET	53	60983	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:53.726845980 CET	49247	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:53.775630951 CET	53	49247	8.8.8.8	192.168.2.7
Feb 23, 2021 09:29:56.399905920 CET	52286	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:29:56.448682070 CET	53	52286	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:04.419305086 CET	56064	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:04.480340004 CET	53	56064	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:21.199871063 CET	63744	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:21.251580954 CET	53	63744	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:21.903512001 CET	61457	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:21.966276884 CET	53	61457	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:22.318589926 CET	58367	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:22.378510952 CET	53	58367	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:22.550931931 CET	60599	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:22.608385086 CET	53	60599	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:23.137856007 CET	59571	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:23.196151018 CET	53	59571	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:23.692564964 CET	52689	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:23.750958920 CET	53	52689	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:24.330089092 CET	50290	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:24.390232086 CET	53	50290	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:25.018570900 CET	60427	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:25.079519033 CET	53	60427	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:25.962924004 CET	56209	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:26.011715889 CET	53	56209	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:26.881119013 CET	59582	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:26.940684080 CET	53	59582	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:27.540143013 CET	60949	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:27.600292921 CET	53	60949	8.8.8.8	192.168.2.7
Feb 23, 2021 09:30:55.509000063 CET	58542	53	192.168.2.7	8.8.8.8
Feb 23, 2021 09:30:55.557792902 CET	53	58542	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: MPO-003234.exe PID: 6584 Parent PID: 5632

General

Start time:	09:29:01
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\MPO-003234.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\MPO-003234.exe'
Imagebase:	0xca0000
File size:	877568 bytes
MD5 hash:	8BC8526FBAAFBAC33118EE652AC97DA6
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: 00000000.00000002.334911428.00000000049BE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.336384581.0000000004ACC000.00000004.00000001.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	6D39CF06	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	6D39CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\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	50D31F3	CopyFileExW
C:\Users\user\AppData\Roaming\badman.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	50D31F3	CopyFileExW
C:\Users\user\AppData\Roaming\badman.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	50D31F3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MPO-003234.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6AC78D	CreateFileW

File Written

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 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 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 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....Z.Z..... ....0..T.....r... .....@.. ....`.....	success or wait	1	50D31F3	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\badman.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 50 fc 33 4b 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 58 0d 00 00 0a 00 00 00 00 00 00 0e 77 0d 00 00 20 00 00 00 80 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0d 00 00 02 00 00 00 00 00 00 02 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...P.3K.......... ....X...........w... ....@.. ....`................	success or wait	4	50D31F3	CopyFileExW
C:\Users\user\AppData\Roaming\badman.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	50D31F3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MPO-003234.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,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D6AC907	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	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D375705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D37CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1E1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6720 Parent PID: 6584

General

Start time:	09:29:07
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'neil' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\badman.exe'
Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6728 Parent PID: 6720

General

Start time:	09:29:08
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 6764 Parent PID: 6720

General

Start time:	09:29:08
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'neil' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\badman.exe'
Imagebase:	0x1370000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	neil	unicode	C:\Users\user\AppData\Roaming\badman.exe	success or wait	1	1375A1D	RegSetValueExW

Analysis Process: badman.exe PID: 7052 Parent PID: 6584

General

Start time:	09:29:49
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\badman.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\badman.exe'
Imagebase:	0xc0000
File size:	877568 bytes
MD5 hash:	8BC8526FBAAFBAC33118EE652AC97DA6
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: 00000010.00000002.432474443.0000000003EAA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.432224674.0000000003D39000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.432317195.0000000003D9C000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 19%, ReversingLabs
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	6D39CF06	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	6D39CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\badman.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\badman.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,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D6AC907	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	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D375705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D37CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1E1B4F	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: 6980 Parent PID: 7052

General

Start time:	09:30:28
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x6e0000
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: 00000019.00000002.497669421.00000000029B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000019.00000002.497669421.00000000029B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000019.00000002.492241366.0000000000402000.00000040.00000001.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	6D39CF06	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	6D39CF06	unknown
C:\Users\user\AppData\Roaming\zUbDt	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1EBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\zUbDt\zUbDt.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	6C1EDD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\zUbDt\zUbDt.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 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 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z.Z.......... ....0..T...........r... ....@.. ....`.................	success or wait	1	6C1EDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D375705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D37CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D375705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1E1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	zUbDt	unicode	C:\Users\user\AppData\Roaming\zUbDt\zUbDt.exe	success or wait	1	6C1E646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	zUbDt	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C1EDE2E	RegSetValueExW

Disassembly

Code Analysis