ID: 356550
Sample Name: REQUEST FOR OFFER.exe
Cookbook: default.jbs
Time: 09:58:47
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report REQUEST FOR OFFER.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 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 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 14
General 15
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 17
Sections 17
Resources 17
Imports 17

Version Infos 18
Network Behavior 18
UDP Packets 18
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: REQUEST FOR OFFER.exe PID: 4156 Parent PID: 5524 19
General 19
File Activities 20
File Created 20
File Written 20
File Read 22
Registry Activities 22
Analysis Process: cmd.exe PID: 3664 Parent PID: 4156 22
General 22
File Activities 23
Analysis Process: conhost.exe PID: 4900 Parent PID: 3664 23
General 23
Analysis Process: reg.exe PID: 4908 Parent PID: 3664 23
General 23
File Activities 23
Registry Activities 23
Key Value Created 23
Analysis Process: badman.exe PID: 5900 Parent PID: 4156 24
General 24
File Activities 24
File Created 24
File Written 24
File Read 25
Registry Activities 25
Analysis Process: InstallUtil.exe PID: 1936 Parent PID: 5900 25
General 25
File Activities 26
File Created 26
File Read 26
Disassembly 26
Code Analysis 26

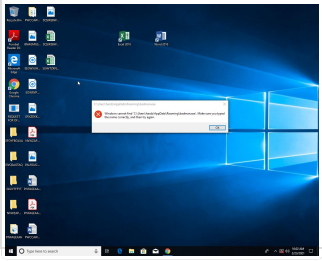
Analysis Report REQUEST FOR OFFER.exe

Overview

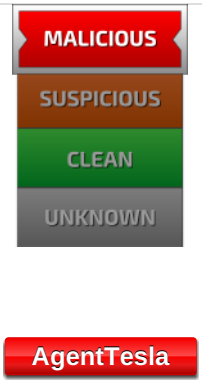
General Information

Sample Name:	REQUEST FOR OFFER.exe
Analysis ID:	356550
MD5:	0fc3feecc0164c5…
SHA1:	60115fc27261ecf..
SHA256:	b5a2fbfeb80e2e9..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



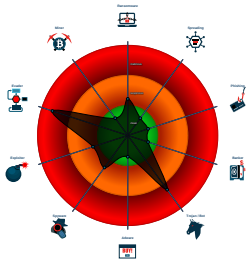
AgentTesla

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…
- Allocates memory in foreign process…
- 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…

Classification



Startup

- **System is w10x64**
- REQUEST FOR OFFER.exe (PID: 4156 cmdline: 'C:\Users\user\Desktop\REQUEST FOR OFFER.exe' MD5: 0FC3FEECC0164C588F7AFAB6E51D566B)
  - cmd.exe (PID: 3664 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: 4900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 4908 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: 5900 cmdline: 'C:\Users\user\AppData\Roaming\badman.exe' MD5: 0FC3FEECC0164C588F7AFAB6E51D566B)
    - InstallUtil.exe (PID: 1936 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.423799814.0000000004AF5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000002.424117469.0000000004C68000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.328242176.0000000004839000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000002.423910607.0000000004B58000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.328670808.0000000004948000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 8 entries

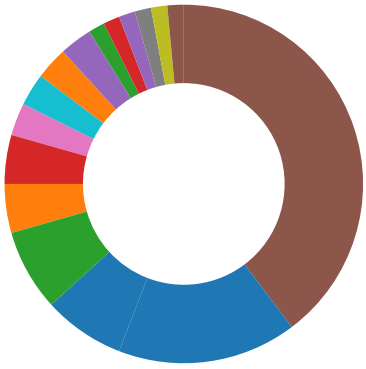
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.REQUEST FOR OFFER.exe.486f7e2.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.2.badman.exe.4c9e3d0.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
15.2.InstallUtil.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.REQUEST FOR OFFER.exe.48a5bb2.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.REQUEST FOR OFFER.exe.49486d2.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 14 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
- 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

Click to jump to signature section

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

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:

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

Remote Access Functionality:

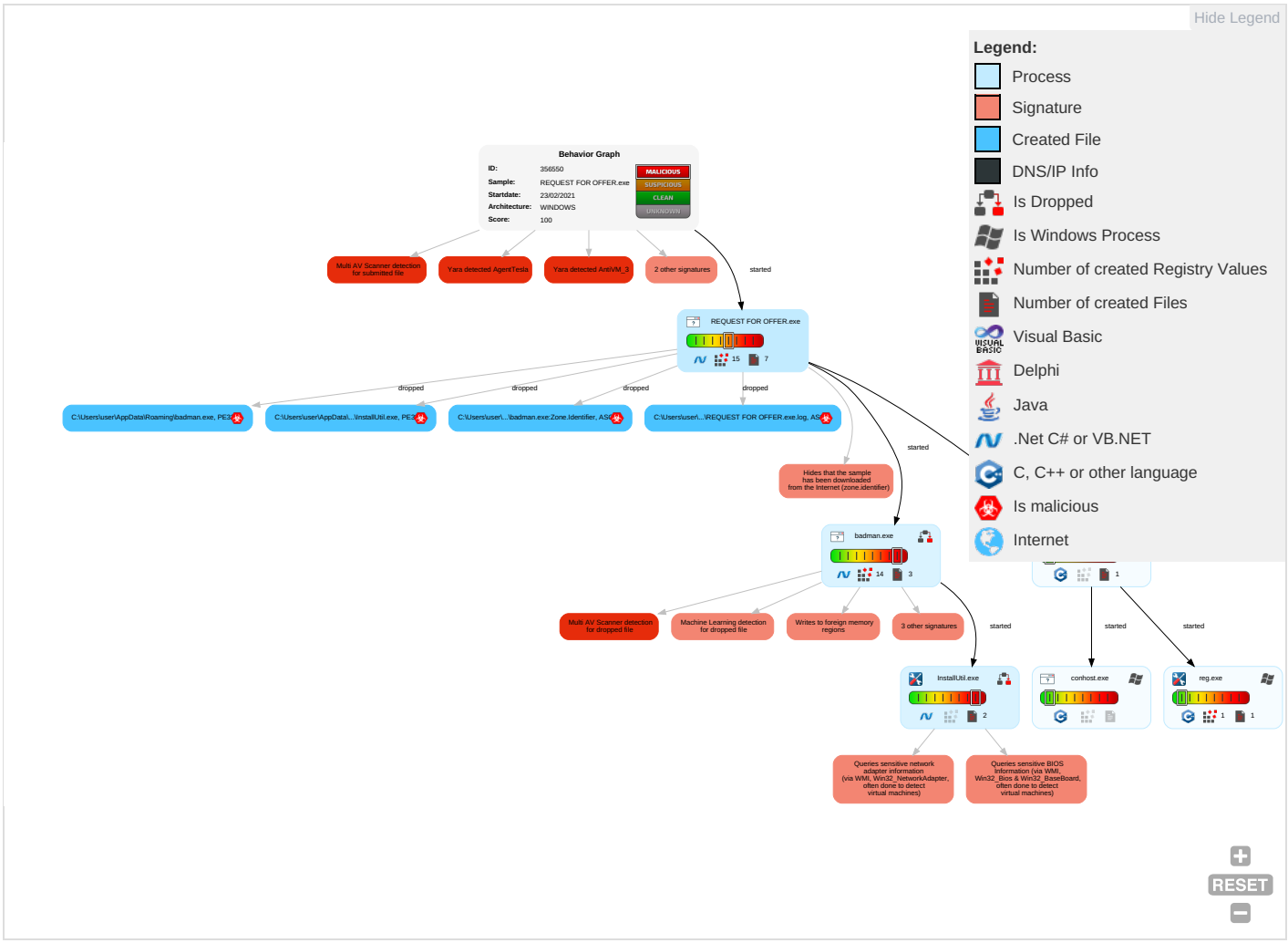
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
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 1	Exfiltration Over Other Network Medium	E C
Default Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	J
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 3 1 2	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	S
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Software Packing 1	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	F I
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Keylogging	Data Transfer Size Limits	F C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M C
External Remote Services	Scheduled Task	Startup Items	Startup Items	Modify Registry 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 1 4	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	V
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 3 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	F F

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M

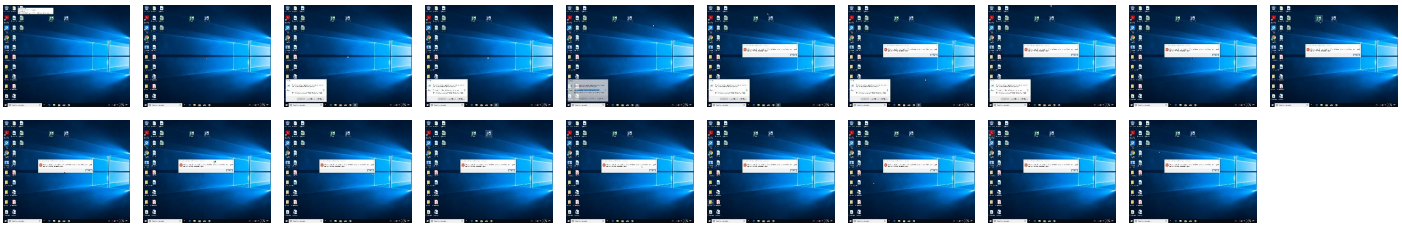
Behavior Graph

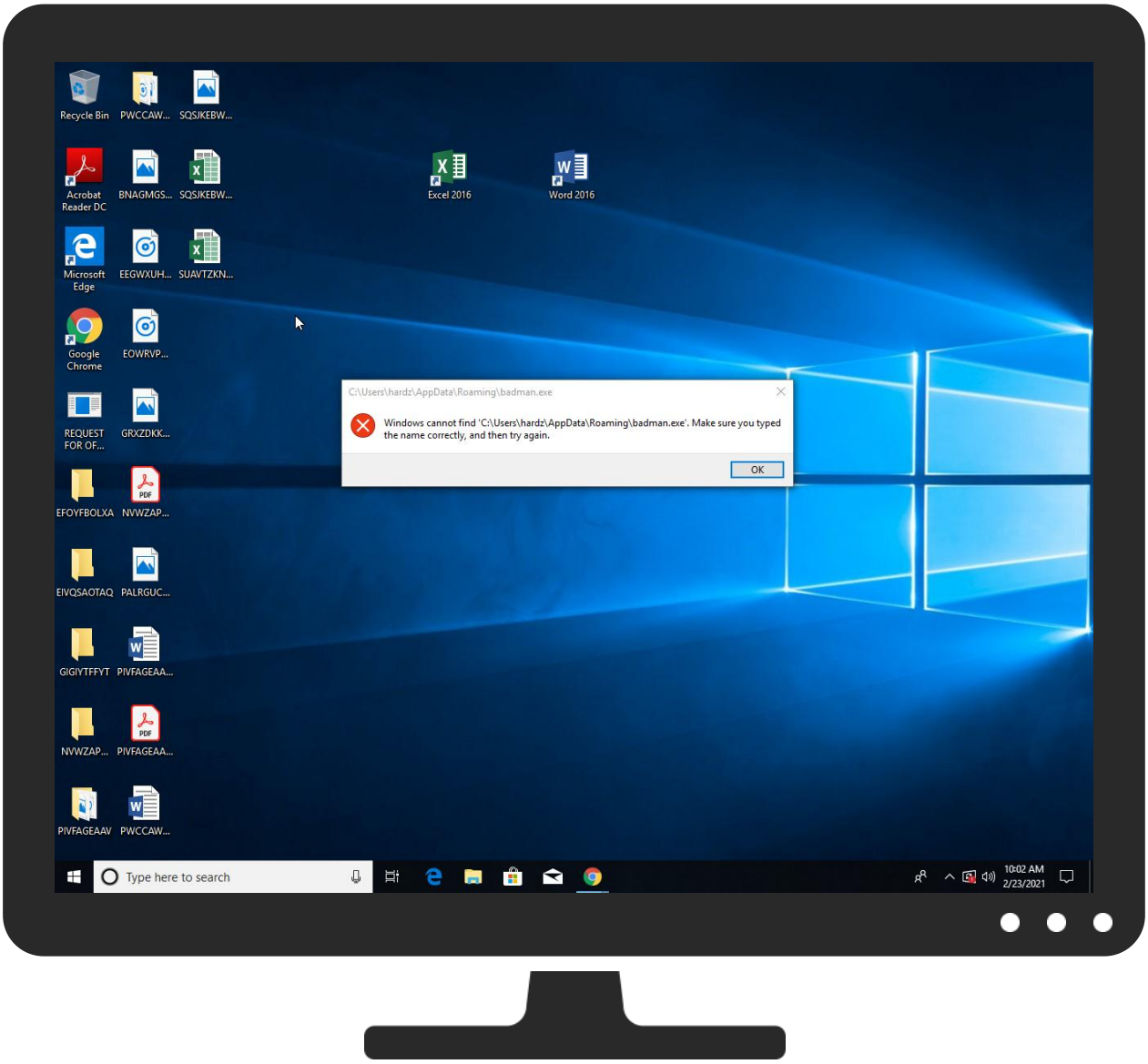


Screenshots

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
REQUEST FOR OFFER.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
REQUEST FOR OFFER.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	35%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

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

Domains

No Antivirus matches

Copyright null 2021

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://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://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://HDgGGv.com	0%	Avira URL Cloud	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://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/g%%vp	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	

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, 0000000F.00000002.477839397.00000000029A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	InstallUtil.exe, 0000000F.00000002.477839397.00000000029A1000.00000004.00000001.sdmp	false	• 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, 0000000F.00000002.477839397.00000000029A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	badman.exe, 0000000E.00000002.416023782.000000000171C000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	badman.exe, 0000000E.00000002.416023782.000000000171C000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://HDgGGv.com	InstallUtil.exe, 0000000F.00000002.477839397.00000000029A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.c/g%%	badman.exe, 0000000E.00000003.414205130.0000000009D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	badman.exe, 0000000E.00000002.416023782.000000000171C000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g	REQUEST FOR OFFER.exe, 00000000.00000003.217353767.0000000009A83000.00000004.00000001.sdmp, badman.exe, 0000000E.00000003.339036712.0000000009D73000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	badman.exe, 0000000E.00000002.416023782.000000000171C000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gsr202	badman.exe, 0000000E.00000002.416023782.000000000171C000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	badman.exe, 0000000E.00000002.416023782.000000000171C000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g%%vp	REQUEST FOR OFFER.exe, 00000000.00000002.332840777.0000000009A85000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	REQUEST FOR OFFER.exe, 00000000.00000002.326675089.0000000002F51000.00000004.00000001.sdmp, badman.exe, 0000000E.00000002.417359766.0000000003271000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	REQUEST FOR OFFER.exe, 00000000.00000002.328242176.0000000004839000.00000004.00000001.sdmp, badman.exe, 0000000E.00000002.423799814.0000000004AF5000.00000004.00000001.sdmp, InstallUtil.exe, 0000000F.00000002.472316965.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/WebPage	REQUEST FOR OFFER.exe, 00000000.00000002.326751684.0000000002F99000.00000004.00000001.sdmp, badman.exe, 0000000E.00000002.417471164.00000000032A2000.00000004.00000001.sdmp	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356550
Start date:	23.02.2021
Start time:	09:58:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	REQUEST FOR OFFER.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:	20
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@10/5@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.5% (good quality ratio 1.2%) • Quality average: 23.1% • Quality standard deviation: 30.1%
HCA Information:	• Successful, ratio: 84% • 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, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 13.64.90.137, 142.250.185.164, 204.79.197.200, 13.107.21.200, 131.253.33.200, 13.107.22.200, 52.147.198.201, 40.88.32.150, 184.30.20.56, 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): www.bing.com, au.download.windowsupdate.com.edgesuite.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus15.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356550/sample/REQUEST FOR OFFER.exe

Simulations

Behavior and APIs

Time	Type	Description
10:00:45	API Interceptor	200x Sleep call for process: REQUEST FOR OFFER.exe modified
10:00:48	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run neil C:\Users\user\AppData\Roaming\badman.exe

Time	Type	Description
10:00:56	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run neil C:\Users\user\AppData\Roaming\badman.exe
10:01:40	API Interceptor	216x Sleep call for process: badman.exe modified
10:02:33	API Interceptor	70x Sleep call for process: InstallUtil.exe modified

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\Local\Temp\InstallUtil.exe	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	
	IMG_144907.exe	Get hash	malicious	Browse	
	VIIIIIIIIIIIC.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	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\REQUEST FOR OFFER.exe.log

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1214
Entropy (8bit):	5.358666369753595
Encrypted:	false

Copyright null 2021

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\REQUEST FOR OFFER.exe.log	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7K84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoM:MIHK5HKXE1qHbHK5AHKzvKviYHKhQnoH
MD5:	1F3BB210B09FE31192C6A822966919E9
SHA1:	A8715FFF2F9D1BE024F462CF702D1E7F71AA4B4F
SHA-256:	C6B3057777EE46AC3544F9FA829E918CD7EF70E490424616650DDA01BF214043
SHA-512:	26897678275FEFDFD96FCB7F7FAFFD5FB0BC0FEB35C89BEB4BA15D074155A06236E8681A2CA9C9DCFDDF2462644CD3603C3592AB310BA84E3D93C8BF2CE28 D5
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:	26897678275FEFDFD96FCB7F7FAFFD5FB0BC0FEB35C89BEB4BA15D074155A06236E8681A2CA9C9DCFDDF2462644CD3603C3592AB310BA84E3D93C8BF2CE28 D5
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\REQUEST FOR OFFER.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%

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Joe Sandbox View:	• 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: 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
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\REQUEST FOR OFFER.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	867840
Entropy (8bit):	6.667025914454025
Encrypted:	false
SSDEEP:	12288:mCiV2B5AJQ3Krcrlhiz6021uysBFcbK5pEfwmjgc1otsf8o1lwPG:mCM2BfKrcBgp2IyySO5cButs
MD5:	0FC3FEECC0164C588F7AFAB6E51D566B
SHA1:	60115FC27261ECF866C1900D3D5F59520A2AB65A
SHA-256:	B5A2FBFEB80E2E92039A23615DF8B8F63F42D1331528F514B312D4946DC22607
SHA-512:	1E01B97A415C25408FFA99C1811C9861B0E3857B55F7EF951C28EDF64F79B6C440CF7BCC3A0240C7DB4400A980E9ED85D2988E036B99AEA3D9027037B7EF61D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...r..8.....2.....P... ...`....@.. ..... ..`.....O..K....`..... ..... ..H.....text...40... ...2..... ..`.rsrc.....`.....4.....@..@.reloc..... .....<.....@..B.....P.....H.....x..8.....3.@.9@yx..B..=H/=.....y....W..y=....l.C....M;...l.7..E.~:...&.....O2.....-.D=.V.i..-.*P.... .L..?.....6.4.=d,.Noa8...^:...g}s.....FA.eG..%....5x.l...7.w...s.{...dz.%.....f..(.#.....]s....O~..s..`..-.[j`..l,\..OT...m.v..R...[..}.i.[zA.L. .ek.....\.v .#F...P+.&..CD./.Vx1.....C.8..O...[. Y.O[c.D..u52..f..u...l..Q..P.Z....}&.y*&y..p.Mw.#*..5h...-.\C=s.....{..d.0.6..l.v.....].j.

C:\Users\user\AppData\Roaming\badman.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\REQUEST FOR OFFER.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
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.667025914454025
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:	REQUEST FOR OFFER.exe
File size:	867840
MD5:	0fc3feecc0164c588f7afab6e51d566b
SHA1:	60115fc27261ecf866c1900d3d5f59520a2ab65a
SHA256:	b5a2fbfeb80e2e92039a23615df8b8f63f42d1331528f514b312d4946dc22607
SHA512:	1e01b97a415c25408ffa99c1811c9861b0e3857b55f7ef951c28edf64f79b6c440cf7bcc3a0240c7db4400a980e9ed85d2988e036b99aea3d9027037b7ef61d5
SSDEEP:	12288:mCiV2B5AJQ3Krcrlhiz6021uysBFcbK5pEfwmjgc1otsf8o1lwPG:mCM2BfKrcBgp2lyySO5cButs
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...r..8.....2.....P... ...`....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d502e
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:	0x3812DF72 [Sun Oct 24 10:29:06 1999 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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0xd4fe0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd6000	0x61e	.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	0xd3034	0xd3200	False	0.641000823342	data	6.67589744501	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0x61e	0x800	False	0.3505859375	data	3.65860521764	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd60a0	0x394	data		
RT_MANIFEST	0xd6434	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

Copyright null 2021

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	Fresh.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	Fresh.exe

Network Behavior

UDP Packets

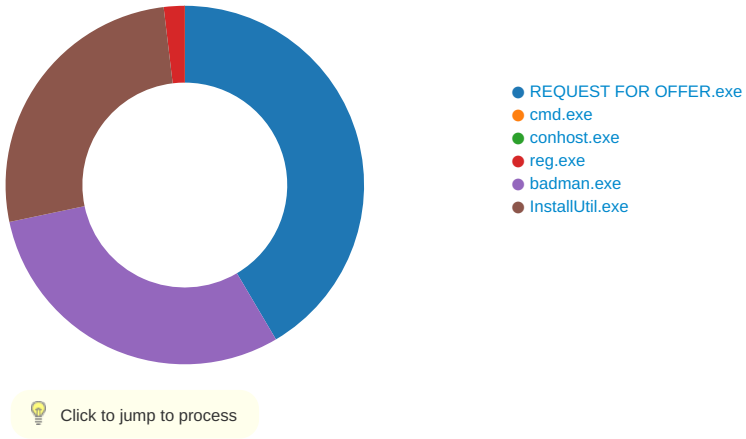
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:00:36.081238985 CET	51904	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:36.132683039 CET	53	51904	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:37.414635897 CET	61328	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:37.463375092 CET	53	61328	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:38.521338940 CET	54130	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:38.570198059 CET	53	54130	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:39.661516905 CET	56961	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:39.713184118 CET	53	56961	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:40.456821918 CET	59353	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:40.522085905 CET	53	59353	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:40.810229063 CET	52238	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:40.859318972 CET	53	52238	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:40.910491943 CET	49873	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:40.982876062 CET	53	49873	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:40.994813919 CET	53196	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:41.043833971 CET	53	53196	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:42.041337967 CET	56777	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:42.090008020 CET	53	56777	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:43.231712103 CET	58643	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:43.280288935 CET	53	58643	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:44.295764923 CET	60985	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:44.344293118 CET	53	60985	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:45.279473066 CET	50200	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:45.328105927 CET	53	50200	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:46.464732885 CET	51281	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:46.516562939 CET	53	51281	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:47.770612955 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:47.833458900 CET	53	49199	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:49.370409966 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:49.419028997 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:50.545496941 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:50.601221085 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:51.684288025 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:51.736004114 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:52.829741955 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:52.888571978 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:55.283130884 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:55.334814072 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 10:00:58.214745998 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:58.263741016 CET	53	64185	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:00:59.293762922 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:00:59.353573084 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 10:01:02.064384937 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:01:02.112971067 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 10:01:06.269579887 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:01:06.328562975 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 10:01:27.109426975 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:01:27.167785883 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 10:01:36.290935993 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:01:36.339538097 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 10:01:36.870996952 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:01:36.919378042 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 10:01:36.936537981 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 10:01:36.985106945 CET	53	50141	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: REQUEST FOR OFFER.exe PID: 4156 Parent PID: 5524

General

Start time:	10:00:38
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\REQUEST FOR OFFER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\REQUEST FOR OFFER.exe'
Imagebase:	0xba0000
File size:	867840 bytes
MD5 hash:	0FC3FEECC0164C588F7AFAB6E51D566B
Has elevated privileges:	true
Has administrator privileges:	true

Copyright null 2021

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.328242176.0000000004839000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.328670808.0000000004948000.00000004.00000001.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	6DE9CF06	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	6DE9CF06	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	4FB1E7B	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	4FB1E7B	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	4FB1E7B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\REQUEST FOR OFFER.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1AC78D	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 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	4FB1E7B	CopyFileExW
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 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 72 df 12 38 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 32 0d 00 00 0a 00 00 00 00 00 00 2e 50 0d 00 00 20 00 00 00 60 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 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...r..8.......... ....2...........P... ...`....@.. ........................ ............`.................	success or wait	4	4FB1E7B	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	4FB1E7B	CopyFileExW

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\REQUEST FOR OFFER.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	6E1AC907	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	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	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: 3664 Parent PID: 4156

General

Start time:	10:00:43

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:	0xbd0000
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: 4900 Parent PID: 3664

General

Start time:	10:00:44
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 4908 Parent PID: 3664

General

Start time:	10:00:44
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:	0xca0000
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

Copyright null 2021

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	CA5A1D	RegSetValueExW

Analysis Process: badman.exe PID: 5900 Parent PID: 4156

General

Start time:	10:01:33
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:	0xee0000
File size:	867840 bytes
MD5 hash:	0FC3FEECC0164C588F7AFAB6E51D566B
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: 0000000E.00000002.423799814.0000000004AF5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.424117469.0000000004C68000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.423910607.0000000004B58000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, 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	6DE9CF06	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	6DE9CF06	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	6E1AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright null 2021

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	6E1AC907	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	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	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: 1936 Parent PID: 5900

General

Start time:	10:02:10

Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x5b0000
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: 0000000F.00000002.477839397.00000000029A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.477839397.00000000029A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.472316965.0000000000402000.00000040.00000001.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	6DE9CF06	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	6DE9CF06	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	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile

Disassembly

Code Analysis

Copyright null 2021