ID: 342213
Sample Name:
NEWORDERrefno0992883jpg.exe
Cookbook: default.jbs
Time: 16:53:41
Date: 20/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

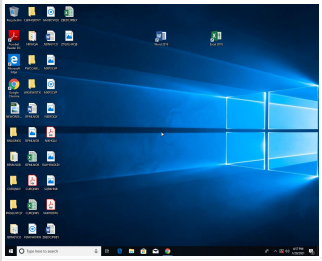
Analysis Report NEWORDERrefno0992883jpg.exe

Overview

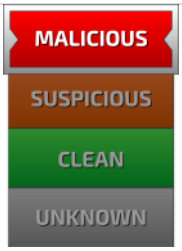
General Information

Sample Name:	NEWORDERrefno0992883jpg.exe
Analysis ID:	342213
MD5:	55124bc60c8715..
SHA1:	a198c5115c4d7f9..
SHA256:	8c6cae9078b175..
Tags:	exe nVpn RAT RemcosRAT

Most interesting Screenshot:



Detection



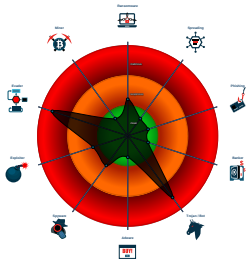
Remcos GuLoader

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

Signatures

- Detected Remcos RAT
- Multi AV Scanner detection for subm…
- Sigma detected: Remcos
- Yara detected GuLoader
- Contains functionality to hide a threa…
- Creates autostart registry keys with …
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…

Classification



Startup

- **System is w10x64**
- NEWORDERrefno0992883jpg.exe (PID: 1908 cmdline: 'C:\Users\user\Desktop\NEWORDERrefno0992883jpg.exe' MD5: 55124BC60C871581F110B6F09E8EE902)
  - NEWORDERrefno0992883jpg.exe (PID: 4712 cmdline: 'C:\Users\user\Desktop\NEWORDERrefno0992883jpg.exe' MD5: 55124BC60C871581F110B6F09E8EE902)
- wscript.exe (PID: 6348 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - PILGRIMIZES.exe (PID: 5668 cmdline: C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe MD5: 55124BC60C871581F110B6F09E8EE902)
    - PILGRIMIZES.exe (PID: 6668 cmdline: C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe MD5: 55124BC60C871581F110B6F09E8EE902)
- wscript.exe (PID: 6728 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - PILGRIMIZES.exe (PID: 6776 cmdline: C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe MD5: 55124BC60C871581F110B6F09E8EE902)
    - PILGRIMIZES.exe (PID: 7140 cmdline: C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe MD5: 55124BC60C871581F110B6F09E8EE902)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.415603840.000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
00000007.00000003.399918336.000002634EBD5000.00000004.00000001.sdmp	SUSP_LNK_SuspiciousCommands	Detects LNK file with suspicious content	Florian Roth	• 0xa8f4:$s12: WScript.Shell • 0xd77c:$s12: WScript.Shell
0000000B.00000002.438708197.000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
00000001.00000002.696666279.000000000562000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

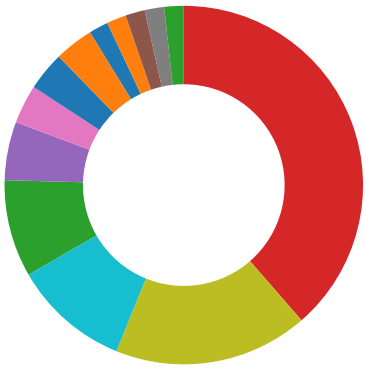
Source	Rule	Description	Author	Strings
Process Memory Space: NEWORDERrefno09928 83jpg.exe PID: 4712	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Click to see the 11 entries				

Sigma Overview

System Summary:

Sigma detected: Remcos

Signature Overview



- AV Detection
- Compliance
- Networking
- 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
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Boot Survival:

Creates autostart registry keys with suspicious values (likely registry only malware)

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

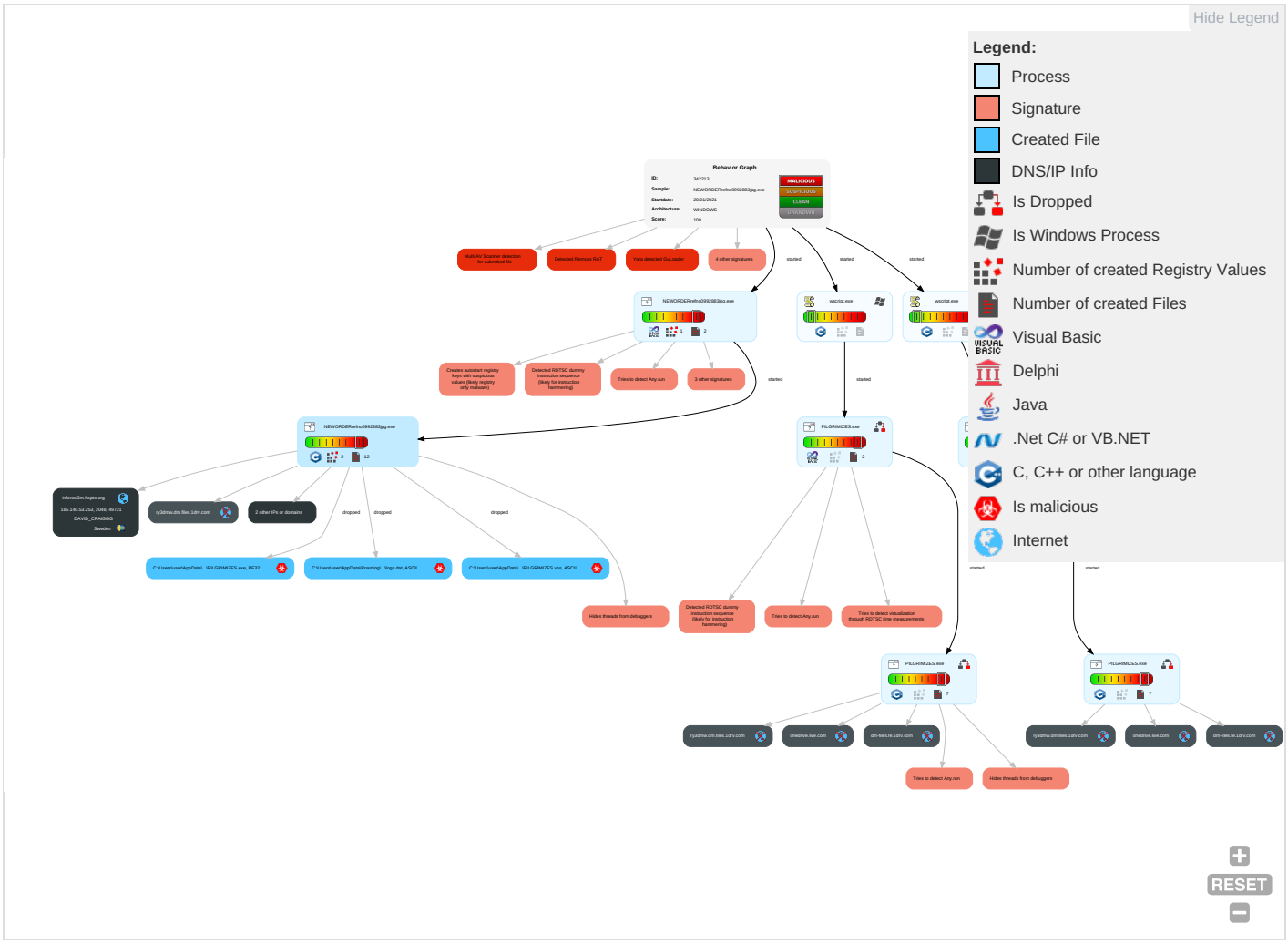
Remote Access Functionality:

Detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1 1	Registry Run Keys / Startup Folder 1 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 6 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1	Jamming or Denial of Service

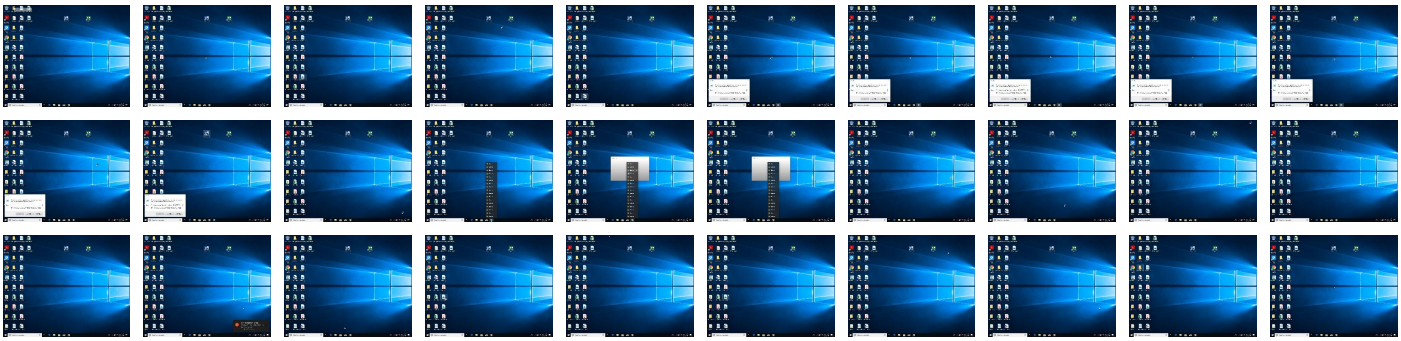
Behavior Graph



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
NEWORDERrefno0992883jpg.exe	24%	Virustotal		Browse
NEWORDERrefno0992883jpg.exe	9%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe	9%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl3.digi	0%	Avira URL Cloud	safe	

Domains and IPs

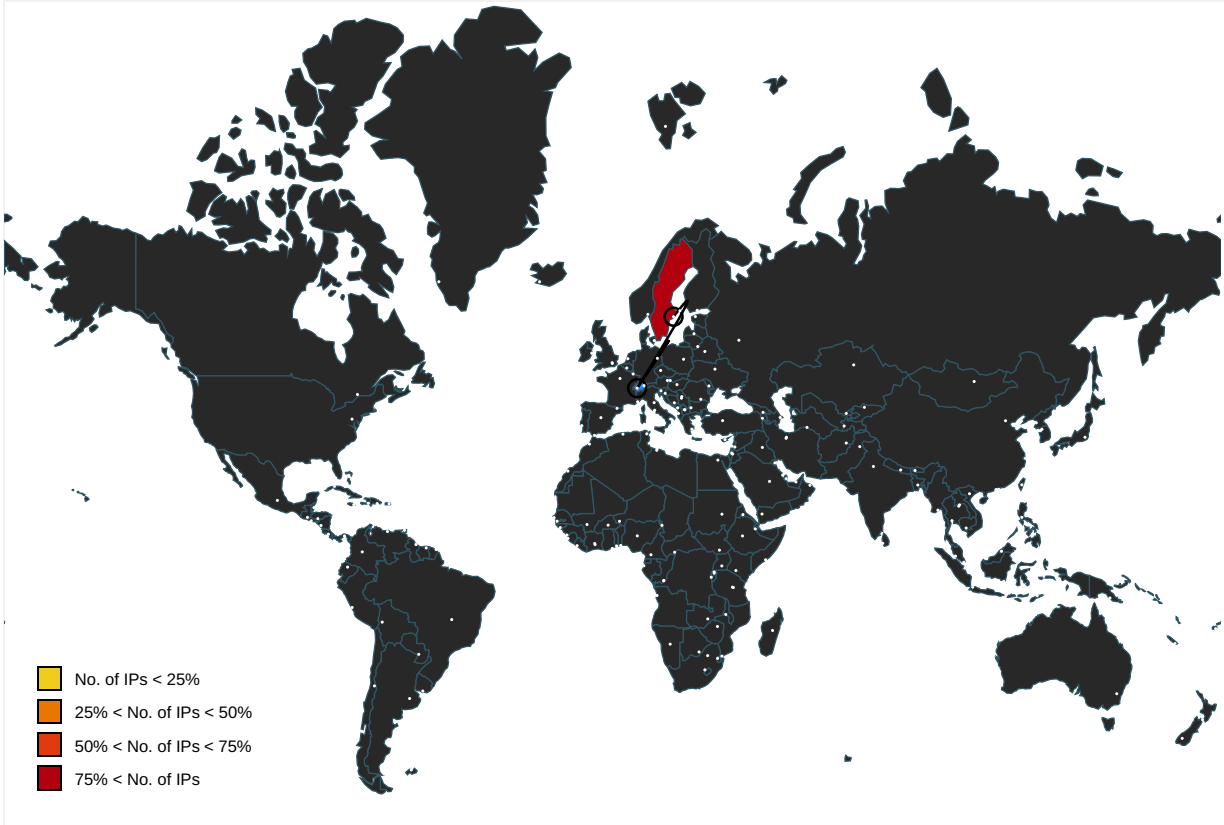
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
inforosi3m.hopto.org	185.140.53.253	true	false		unknown
onedrive.live.com	unknown	unknown	false		high
ry3dmw.dm.files.1drv.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ry3dmw.dm.files.1drv.com/y4mCJVSTmiHuzMhULmUNmg4EimfSRflb83yNVhTry70q37pI5b1gbJ6e_SyvPbvtOFB	PILGRIMIZES.exe, 00000006.00000002.415757520.00000000009B8000.00000004.00000020.sdmp, PILGRIMIZES.exe, 00000006.00000002.415814005.0000000000A1C000.00000004.00000020.sdmp	false		high
http://https://ry3dmw.dm.files.1drv.com/	PILGRIMIZES.exe, 00000006.00000002.415757520.00000000009B8000.00000004.00000020.sdmp	false		high
http://https://ry3dmw.dm.files.1drv.com/y4m5Uk8XK7Wl1Kz2W_ObQ202aCzFbJtOLqXH5zzyoS4s7PNVv2jQFwK-Dxrh70VAS6o	PILGRIMIZES.exe, 00000006.00000002.415798264.0000000000A0000.00000004.00000020.sdmp	false		high
http://crl3.digi	PILGRIMIZES.exe, 00000006.00000002.415798264.0000000000A0000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/download?cid=3EA7AF3CF2A8B6E2&resid=3EA7AF3CF2A8B6E2%21121&authkey=AMq9sG-	PILGRIMIZES.exe	false		high
http://https://onedrive.live.com/	PILGRIMIZES.exe, 00000006.00000002.415757520.00000000009B8000.00000004.00000020.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.253	unknown	Sweden		209623	DAVID_CRAIGGG	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342213
Start date:	20.01.2021
Start time:	16:53:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEWORDERrefno0992883jpg.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@13/3@7/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 36.2% (good quality ratio 21.3%) • Quality average: 38% • Quality standard deviation: 34.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 13.88.21.125, 104.42.151.234, 13.107.42.13, 13.107.42.12, 51.104.139.180, 2.20.142.210, 2.20.142.209, 51.103.5.159, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 23.210.248.85, 51.104.144.132 • Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, au.download.windowsupdate.com.edgesuite.net, odc-dm-files-geo.onedrive.akadns.net, arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, l-0004.l-msedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, odc-dm-files.onedrive.akadns.net.l-0003.dc-msedge.net.l-0003.l-msedge.net, l-0003.l-msedge.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, odc-dm-files-brs.onedrive.akadns.net, client.wns.windows.com, fs.microsoft.com, odc-web-geo.onedrive.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • 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.

Simulations

Behavior and APIs

Time	Type	Description
16:54:46	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce unturbid C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.vbs
16:54:53	API Interceptor	1257x Sleep call for process: NEWORDERrefno0992883jpg.exe modified
16:54:55	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce unturbid C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.vbs

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.253	CompanyLicense.exe	Get hash	malicious	Browse	
	16Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	15Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	
	58Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	57Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	
	15Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	14Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	
	57Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	56Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
inforosi3m.hopto.org	Scan0010110101WW320.vbs	Get hash	malicious	Browse	• 185.244.30.250

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	richiealvin.exe	Get hash	malicious	Browse	• 91.193.75.185
	Quotation.exe	Get hash	malicious	Browse	• 185.140.53.154
	DHL Delivery Shipping Cargo. Pdf.exe	Get hash	malicious	Browse	• 185.244.30.18
	CompanyLicense.exe	Get hash	malicious	Browse	• 185.140.53.253
	Purchase Order 2094742424.exe	Get hash	malicious	Browse	• 185.244.30.132
	PURCHASE OREDER. PRINT. pdf.exe	Get hash	malicious	Browse	• 91.193.75.45
	PO.exe	Get hash	malicious	Browse	• 185.140.53.234
	SWIFT.exe	Get hash	malicious	Browse	• 185.140.53.154
	SecuriteInfo.com.BScope.Trojan-Dropper.Injector.exe	Get hash	malicious	Browse	• 185.140.53.234
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 185.140.53.131
	Orden n.#U00ba STL21119, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	Proof of Payment.exe	Get hash	malicious	Browse	• 185.244.30.51
	DxCHoDnNLn.exe	Get hash	malicious	Browse	• 185.140.53.202
	T7gzTHDZ7g.rtf	Get hash	malicious	Browse	• 185.140.53.202
	PO - 2021-000511.exe	Get hash	malicious	Browse	• 185.244.30.69
	PO AR483-1590436 _ J-3000 PROJT.xlsx	Get hash	malicious	Browse	• 185.140.53.202
	Qotation.exe	Get hash	malicious	Browse	• 185.140.53.154
	PO - 2021-000511.exe	Get hash	malicious	Browse	• 185.244.30.69
	file.exe	Get hash	malicious	Browse	• 91.193.75.155
	Orden n.#U00ba 21115, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe

Process:	C:\Users\user\Desktop\NEWORDERrefno0992883jpg.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	5.509642354428253
Encrypted:	false
SSDEEP:	1536:S1AsZKZAFPlaXjiUqIEARdNW2XLnolNIH:S1FwKPlaOUqIEqN/LnkmH
MD5:	55124BC60C871581F110B6F09E8EE902
SHA1:	A198C5115C4D7F9E61A06020C814C2B5B4FBA0F8

C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe	
SHA-256:	8C6CAE9078B175B331C1D6154045DEEA386850A75E4E2A250FE4F4D920CF1A4A
SHA-512:	50D7E57EAD5BABA4435F06111885B77656DA56719DA1FCDCDA4993E9CD1A95EF34DCD106EE665F0C347A761E357D2FAEE089840DE3CFB098DF87F378F534153
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 9%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I.....Rich.....PE..L..../R..... ....`.....0....@.....(....P..T>.....8... .....text..... .....`.data.....0.....0.....@....rsrc...T>...P...@...@.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.vbs	
Process:	C:\Users\user\Desktop\NEWORDERrefno0992883jpg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	119
Entropy (8bit):	5.0607448363385545
Encrypted:	false
SSDEEP:	3:jfF+m8nhvF3mRDN+E2J5xAIw3g5mpis/NHM:jFqhv9IN723fUpHVM
MD5:	F830DCDA7316D6A07DDEC96C4618FBCA
SHA1:	E5B094BDC86C7CDD22FB136582728FA78BB3C111
SHA-256:	1D5B85D9BACDBED9129AFDD86EDBE1EEC45228213466C50DBA784C919EA8A2EF
SHA-512:	46F4312E1C92517EF0256B49E99EC358FFCA4C14DEAC4D618D5B92D6AF37643C2B3A8675BC2434B1BC498DBB7DD603F687890EE96390A9DF3F77B3B1F8FA4BD
Malicious:	**true**
Reputation:	low
Preview:	Set W = CreateObject("WScript.Shell")..Set C = W.Exec ("C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe")

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Users\user\Desktop\NEWORDERrefno0992883jpg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	87
Entropy (8bit):	4.736705242846249
Encrypted:	false
SSDEEP:	3:ttUoUbyrA4RXMRPHv33a1oy61aeo:tmoNXqdHv3qv6IP
MD5:	8AD37A232C951978EC99117FF0D20AC6
SHA1:	E9FA52001367F58F77201EED4AD69784C0FB6DCC
SHA-256:	03951F0AB8171312ABF1FF33CAEF8E94131A5E05166EB04FCBC6960F0E32CAE0
SHA-512:	C51E2A7EA89F26307A31AE5EA552A36B85DEA5A5F220F389C27A897A37D442A6946E40F695DE136F4994CFF319F49E1A73698CA7BC17FBEB23ED9BEC51688C16
Malicious:	**true**
Reputation:	low
Preview:	..[2021/01/20 16:54:53 Offline Keylogger Started]....[Run]..[r..[Program Manager]..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.509642354428253
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	NEWORDERrefno0992883jpg.exe
File size:	98304
MD5:	55124bc60c871581f110b6f09e8ee902
SHA1:	a198c5115c4d7f9e61a06020c814c2b5b4fba0f8

General

SHA256:	8c6cae9078b175b331c1d6154045deea386850a75e4e2a250fe4f4d920cf1a4a
SHA512:	50d7e57ead5baba4435f06111885b77656da56719da1fcdcda4993e9cd1a95ef34dcd106ee665f0c347a761e357d2faee089840de3cfb098df87f378f5341543
SSDEEP:	1536:S1AsZKZAFPlaXjiUqIEARdNW2XLnolNIH:S1FwKPlaOUqIEqN/LnkmH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I.....Rich.....PE..L...../R..... ...`.....0....@

File Icon

Icon Hash:	0919914f4707077b

Static PE Info

General

Entrypoint:	0x401480
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x522F8FEE [Tue Sep 10 21:32:30 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	cdaaae34b462dd94bb47458bdb1adef4

Entrypoint Preview

Instruction
push 00402814h
call 00007F9C7083BCF3h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push es
inc edi
stosb
jnc 00007F9C7083BCD1h
xor eax, 8BBAA147h
sbb eax, 274E8692h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
call 00007F9CB886DFBFh
push 0000006Ch
jo 00007F9C7083BD75h
outsd
insd
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
add eax, A4054858h
xor dword ptr [edx-5Bh], esp
inc eax
mov ah, 01h
cmc
pushfd
and dl, byte ptr [edi]
out CBh, eax
mov edi, 96799639h
mov bh, byte ptr [ebp+46h]
test byte ptr [edi-0Ch], bl
pushad
xlatb
push AD4F3AECh
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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
mov ecx, D2000010h
sldt word ptr [eax]
add byte ptr [726F5700h], cl
imul ebp, dword ptr [ebp+69h], 73h
je 00007F9C7083BD74h
jnc 00007F9C7083BD76h
xor eax, 0F010D00h
add byte ptr [ebx+6Bh], dl
jne 00007F9C7083BD74h
imul esp, dword ptr [ebp+73h], 74h
jc 00007F9C7083BD67h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11fe4	0x28	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x15000	0x3e54	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x118	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x11480	0x12000	False	0.345458984375	data	5.50668212357	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x13000	0x1598	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x15000	0x3e54	0x4000	False	0.405029296875	data	5.82015845972	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x15148	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x155b0	0x10a8	data		
RT_ICON	0x16658	0x25a8	data		
RT_GROUP_ICON	0x18c00	0x30	data		
RT_VERSION	0x18c30	0x224	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryVar, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaVarTstEq, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaI2Str, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarDup, _CIatan, __vbaStrMove, __vbaAryCopy, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

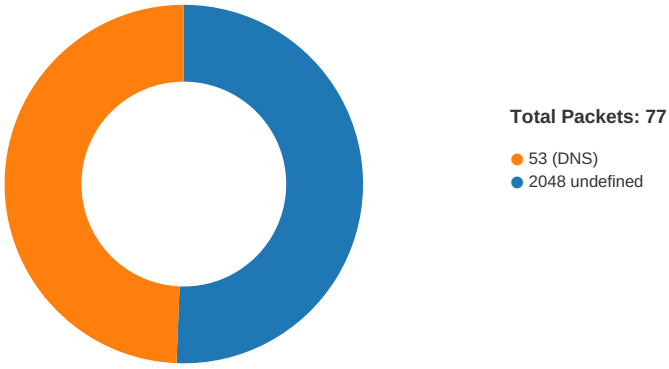
Description	Data
Translation	0x0409 0x04b0
InternalName	SELVMODSIGELSE
FileVersion	1.00
CompanyName	Above
ProductName	Hjlpsom
ProductVersion	1.00
OriginalFilename	SELVMODSIGELSE.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 16:54:53.446971893 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:54:54.065287113 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:54:54.065565109 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:54:54.066756010 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:54:55.177615881 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:54:57.037013054 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:54:57.161019087 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:54:57.230752945 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:54:57.233791113 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:54:57.820385933 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:00.349071026 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:00.353962898 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:00.533977985 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:05.339541912 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:05.345825911 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:05.516230106 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:10.340755939 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:10.444410086 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:11.105350018 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:11.660034895 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:15.342780113 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:15.345257998 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:15.843564034 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:20.343687057 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:20.350860119 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:20.520826101 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:25.344441891 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:25.346466064 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:25.519068956 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:30.348246098 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:30.350378036 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:30.794372082 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:35.348925114 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:35.351710081 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:35.811310053 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:40.350337982 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:40.352926016 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:40.525615931 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:45.350980997 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:45.387824059 CET	49731	2048	192.168.2.6	185.140.53.253

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 16:55:45.856873989 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:50.366103888 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:50.370595932 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:50.679147959 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:55.366919994 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:55:55.369972944 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:55:55.539298058 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:00.687216997 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:00.695122004 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:01.361176968 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:01.361279964 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:01.448623896 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:01.976331949 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:02.289367914 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:05.357477903 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:05.464627028 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:06.061624050 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:06.660820007 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:10.362004042 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:10.366336107 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:10.732948065 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:15.361697912 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:15.363843918 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:15.534502983 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:20.361860991 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:20.364300966 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:20.536669970 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:25.364950895 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:25.370362043 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:25.585580111 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:30.366152048 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:30.370079041 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:30.803399086 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:35.368503094 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:35.370753050 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:35.718331099 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:40.368340969 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:40.374795914 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:40.545203924 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:45.370646954 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:45.374006033 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:45.856628895 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:50.381683111 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:50.385859013 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:50.767817020 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:55.372123957 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:56:55.374928951 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:56:55.786494017 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:57:00.375139952 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:57:00.377547026 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:57:00.598162889 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:57:05.376633883 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:57:05.379839897 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:57:05.672014952 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:57:10.377461910 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:57:10.382093906 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:57:10.738368034 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:57:16.749614954 CET	2048	49731	185.140.53.253	192.168.2.6
Jan 20, 2021 16:57:16.792251110 CET	49731	2048	192.168.2.6	185.140.53.253
Jan 20, 2021 16:57:17.504452944 CET	49731	2048	192.168.2.6	185.140.53.253

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 16:54:29.580313921 CET	56023	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:29.629131079 CET	53	56023	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:30.362940073 CET	58384	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:30.410828114 CET	53	58384	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:31.526614904 CET	60261	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:31.574543953 CET	53	60261	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:32.699304104 CET	56061	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:32.747380018 CET	53	56061	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:33.546104908 CET	58336	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:33.597208023 CET	53	58336	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:34.665492058 CET	53781	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:34.713407993 CET	53	53781	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:35.451287031 CET	54064	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:35.510778904 CET	53	54064	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:36.781151056 CET	52811	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:36.832160950 CET	53	52811	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:39.785057068 CET	55299	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:39.833184958 CET	53	55299	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:41.069011927 CET	63745	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:41.119613886 CET	53	63745	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:43.342288971 CET	50055	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:43.398510933 CET	53	50055	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:46.899415016 CET	61374	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:46.951332092 CET	53	61374	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:51.016771078 CET	50339	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:51.064860106 CET	53	50339	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:52.487951040 CET	63307	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:52.577634096 CET	53	63307	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:53.382000923 CET	49694	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:53.445444107 CET	53	49694	8.8.8.8	192.168.2.6
Jan 20, 2021 16:54:59.204571009 CET	54982	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:54:59.252686977 CET	53	54982	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:11.684097052 CET	50010	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:11.733552933 CET	53	50010	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:12.183809996 CET	63718	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:12.250924110 CET	53	63718	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:18.469130039 CET	62116	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:18.529723883 CET	53	62116	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:20.379296064 CET	63816	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:20.440028906 CET	53	63816	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:22.543064117 CET	55014	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:22.593735933 CET	53	55014	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:23.130413055 CET	62208	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:23.189975023 CET	53	62208	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:32.629980087 CET	57574	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:32.686336040 CET	53	57574	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:36.366578102 CET	51818	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:36.421276093 CET	53	51818	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:36.987466097 CET	56628	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:37.043663025 CET	53	56628	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:37.619988918 CET	60778	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:37.678622007 CET	53	60778	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:38.126915932 CET	53799	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:38.186309099 CET	53	53799	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:38.414350033 CET	54683	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:38.470679998 CET	53	54683	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:38.628679037 CET	59329	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:38.685170889 CET	53	59329	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:39.244544983 CET	64021	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:39.301084042 CET	53	64021	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:40.126840115 CET	56129	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:40.183212042 CET	53	56129	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:41.036498070 CET	58177	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:41.093053102 CET	53	58177	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 16:55:42.364470959 CET	50700	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:42.421240091 CET	53	50700	8.8.8.8	192.168.2.6
Jan 20, 2021 16:55:42.894944906 CET	54069	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:55:42.954122066 CET	53	54069	8.8.8.8	192.168.2.6
Jan 20, 2021 16:56:01.083044052 CET	61178	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:56:01.139086008 CET	53	61178	8.8.8.8	192.168.2.6
Jan 20, 2021 16:56:02.436227083 CET	57017	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:56:02.493866920 CET	53	57017	8.8.8.8	192.168.2.6
Jan 20, 2021 16:56:07.424877882 CET	56327	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:56:07.472803116 CET	53	56327	8.8.8.8	192.168.2.6
Jan 20, 2021 16:56:25.307404995 CET	50243	53	192.168.2.6	8.8.8.8
Jan 20, 2021 16:56:25.355210066 CET	53	50243	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 20, 2021 16:54:51.016771078 CET	192.168.2.6	8.8.8.8	0x8133	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Jan 20, 2021 16:54:52.487951040 CET	192.168.2.6	8.8.8.8	0x4ebb	Standard query (0)	ry3dmw.dm.files.1drv.com	A (IP address)	IN (0x0001)
Jan 20, 2021 16:54:53.382000923 CET	192.168.2.6	8.8.8.8	0x35c5	Standard query (0)	inforosi3m.hopto.org	A (IP address)	IN (0x0001)
Jan 20, 2021 16:55:11.684097052 CET	192.168.2.6	8.8.8.8	0x3de	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Jan 20, 2021 16:55:12.183809996 CET	192.168.2.6	8.8.8.8	0x6be	Standard query (0)	ry3dmw.dm.files.1drv.com	A (IP address)	IN (0x0001)
Jan 20, 2021 16:55:22.543064117 CET	192.168.2.6	8.8.8.8	0xd50d	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Jan 20, 2021 16:55:23.130413055 CET	192.168.2.6	8.8.8.8	0x4058	Standard query (0)	ry3dmw.dm.files.1drv.com	A (IP address)	IN (0x0001)

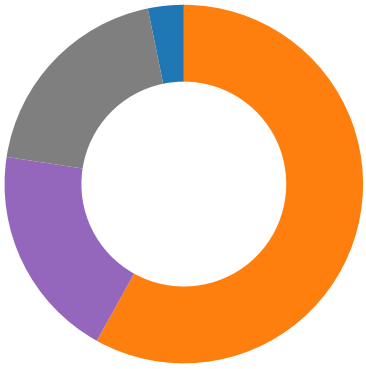
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2021 16:54:51.064860106 CET	8.8.8.8	192.168.2.6	0x8133	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 16:54:52.577634096 CET	8.8.8.8	192.168.2.6	0x4ebb	No error (0)	ry3dmw.dm.files.1drv.com	dm-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 16:54:52.577634096 CET	8.8.8.8	192.168.2.6	0x4ebb	No error (0)	dm-files.fe.1drv.com	odc-dm-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 16:54:53.445444107 CET	8.8.8.8	192.168.2.6	0x35c5	No error (0)	inforosi3m.hopto.org		185.140.53.253	A (IP address)	IN (0x0001)
Jan 20, 2021 16:55:11.733552933 CET	8.8.8.8	192.168.2.6	0x3de	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 16:55:12.250924110 CET	8.8.8.8	192.168.2.6	0x6be	No error (0)	ry3dmw.dm.files.1drv.com	dm-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 16:55:12.250924110 CET	8.8.8.8	192.168.2.6	0x6be	No error (0)	dm-files.fe.1drv.com	odc-dm-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 16:55:22.593735933 CET	8.8.8.8	192.168.2.6	0xd50d	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 16:55:23.189975023 CET	8.8.8.8	192.168.2.6	0x4058	No error (0)	ry3dmw.dm.files.1drv.com	dm-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 16:55:23.189975023 CET	8.8.8.8	192.168.2.6	0x4058	No error (0)	dm-files.fe.1drv.com	odc-dm-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: NEWORDERrefno0992883jpg.exe PID: 1908 Parent PID: 6012

General

Start time:	16:54:35
Start date:	20/01/2021
Path:	C:\Users\user\Desktop\NEWORDERrefno0992883jpg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NEWORDERrefno0992883jpg.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	55124BC60C871581F110B6F09E8EE902
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

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\RunOnce	unturbid	unicode	C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.vbs	success or wait	1	21F1CC8	RegSetValueExA

Analysis Process: NEWORDERrefno0992883jpg.exe PID: 4712 Parent PID: 1908

General

Start time:	16:54:42
Start date:	20/01/2021
Path:	C:\Users\user\Desktop\NEWORDERrefno0992883jpg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NEWORDERrefno0992883jpg.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	55124BC60C871581F110B6F09E8EE902
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000001.00000002.696666279.0000000000562000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	569764	CreateFileW
C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	569764	CreateFileW
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	564906	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA
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	564906	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40564C	CreateDirectoryW
C:\Users\user\AppData\Roaming\remcos\logs.dat	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	4	412D99	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40564C	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe	unknown	98304	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 c8 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 d7 c8 c4 49 93 a9 aa 1a 93 a9 aa 1a 93 a9 aa 1a 10 b5 a4 1a 92 a9 aa 1a dc 8b a3 1a 9f a9 aa 1a a5 8f a7 1a 92 a9 aa 1a 52 69 63 68 93 a9 aa 1a 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 50 45 00 00 4c 01 03 00 ee 8f 2f 52 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 20 01 00 00 60 00 00 00 00 00 00 80 14 00 00 00 10 00 00 00 30 01 00 00 00 40	MZ......................@....................................!..L.!This program cannot be run in DOS mode....$..........I..................................Rich.........................PE..L...../R................. ...`..............0....@	success or wait	1	56207B	WriteFile
C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.vbs	unknown	119	53 65 74 20 57 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 0d 0a 53 65 74 20 43 20 3d 20 57 2e 45 78 65 63 20 28 22 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 42 49 4c 54 4d 4f 52 45 5c 50 49 4c 47 52 49 4d 49 5a 45 53 2e 65 78 65 22 29	Set W = CreateObject("Wscript.Shell")..Set C = W.Exec ("C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe")	success or wait	1	56207B	WriteFile
C:\Users\user\AppData\Roaming\remcos\logs.dat	unknown	51	0d 0a 5b 32 30 32 31 2f 30 31 2f 32 30 20 31 36 3a 35 34 3a 35 33 20 4f 66 66 6c 69 6e 65 20 4b 65 79 6c 6f 67 67 65 72 20 53 74 61 72 74 65 64 5d 0d 0a	..[2021/01/20 16:54:53 Offline Keylogger Started]..	success or wait	4	412DCC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NEWORDERrefno0992883jpg.exe	unknown	98304	success or wait	1	569764	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\idll-LLXXO1\	success or wait	1	40B71B	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\idll-LLXXO1	exepath	binary	0E FE EE B3 0F CB 2C E1 03 D0 40 EB 66 B8 27 62 0E BC F9 0A D8 A2 27 65 E0 58 D2 5D 16 81 C2 83 87 CF 0E F2 6E 56 EC 94 3D ED F9 BF AC 3B F1 3B 84 D6 72 FB 08 24 1F 3C 11 85 ED 0F BE 81 CE C4 2B AC 7E F8 A0 26 58 3E 3E 2B A3 13 E5 F5 9E 53 57 44 D8 97 1B 3D 56 06 29 A0 7D AA E4 41 D5 25 D0 30 32 38 BD 68 26 01 E3 38 B2 85	success or wait	1	40B747	RegSetValueExA
HKEY_CURRENT_USER\Software\idll-LLXXO1	licence	unicode	F980DA39CAEF5CA7DEBAF7FC1AAA23B5	success or wait	1	40B747	RegSetValueExA

Analysis Process: wscript.exe PID: 6348 Parent PID: 3440

General

Start time:	16:54:55
Start date:	20/01/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.vbs'
Imagebase:	0x7ff7931b0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: PILGRIMIZES.exe PID: 5668 Parent PID: 6348

General

Start time:	16:54:56
Start date:	20/01/2021
Path:	C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	55124BC60C871581F110B6F09E8EE902
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 9%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: PILGRIMIZES.exe PID: 6668 Parent PID: 5668

General

Start time:	16:55:01
Start date:	20/01/2021
Path:	C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	55124BC60C871581F110B6F09E8EE902
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000006.00000002.415603840.0000000000560000.00000040.00000001.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	564906	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA
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	564906	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 6728 Parent PID: 3440

General

Start time:	16:55:03
Start date:	20/01/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.vbs'
Imagebase:	0x7ff7931b0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_LNK_SuspiciousCommands, Description: Detects LNK file with suspicious content, Source: 00000007.00000003.399918336.000002634EBD5000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: PILGRIMIZES.exe PID: 6776 Parent PID: 6728

General

Start time:	16:55:05
Start date:	20/01/2021
Path:	C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	55124BC60C871581F110B6F09E8EE902
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: PILGRIMIZES.exe PID: 7140 Parent PID: 6776

General

Start time:	16:55:15
Start date:	20/01/2021
Path:	C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BILTMORE\PILGRIMIZES.exe
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	55124BC60C871581F110B6F09E8EE902

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000B.00000002.438708197.0000000000560000.00000040.00000001.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	564906	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA
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	564906	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564906	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis