ID: 558240
Sample Name:
171121_PDF.exe
Cookbook: default.jbs
Time: 06:42:50
Date: 23/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 171121_PDF.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Jbx Signature Overview 5
AV Detection 5
Networking 5
System Summary 5
Data Obfuscation 5
Malware Analysis System Evasion 5
Anti Debugging 5
HIPS / PFW / Operating System Protection Evasion 5
Stealing of Sensitive Information 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
World Map of Contacted IPs 8
General Information 8
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
C:\Users\user\AppData\Local\Temp\CUSCONINE\vagabo.exe 9
C:\Users\user\AppData\Local\Temp\~DFD14B856B0CE15507.TMP 10
Static File Info 10
General 10
File Icon 10
Static PE Info 11
General 11
Authenticode Signature 11
Entrypoint Preview 11
Data Directories 13
Sections 13
Resources 13
Imports 14
Version Infos 14
Possible Origin 14
Network Behavior 14
UDP Packets 14
DNS Queries 14
DNS Answers 14
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: 171121_PDF.exePID: 6968, Parent PID: 4448 15
General 15
File Activities 15
Analysis Process: ieinstal.exePID: 5012, Parent PID: 6968 15
General 15

Analysis Process: ieinstal.exePID: 7124, Parent PID: 6968 16
General 16
File Activities 16
File Created 16
File Written 16
File Read 16
Registry Activities 17
Key Value Created 17
Disassembly 17

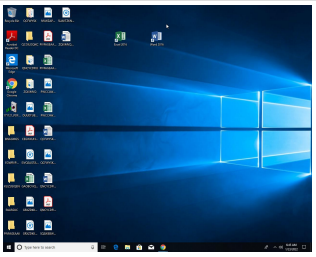
Windows Analysis Report

171121_PDF.exe

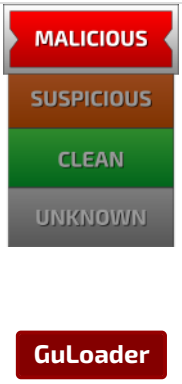
Overview

General Information

Sample Name:	171121_PDF.exe
Analysis ID:	558240
MD5:	60d8b8589ba804.
SHA1:	328a778d026ad6.
SHA256:	8f34d0008f07a44.
Infos:	



Detection



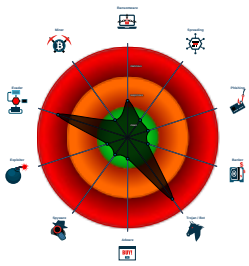
GuLoader

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Found stalling execution ending in A…
- Tries to detect Any.run
- C2 URLs / IPs found in malware con…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- 171121_PDF.exe (PID: 6968 cmdline: "C:\Users\user\Desktop\171121_PDF.exe" MD5: 60D8B8589BA8045361AE148EE76C7582)
  - ieinstal.exe (PID: 5012 cmdline: "C:\Users\user\Desktop\171121_PDF.exe" MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 7124 cmdline: "C:\Users\user\Desktop\171121_PDF.exe" MD5: DAD17AB737E680C47C8A44CBB95EE67E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://onedrive.live.com/downloa"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.543844211.0000000003200000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000F.00000000.352935282.0000000003200000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000002.498027231.0000000002320000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

System Summary

Initial sample is a PE file and has a suspicious name

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Found stalling execution ending in API Sleep call

Tries to detect Any.run

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

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Stealing of Sensitive Information

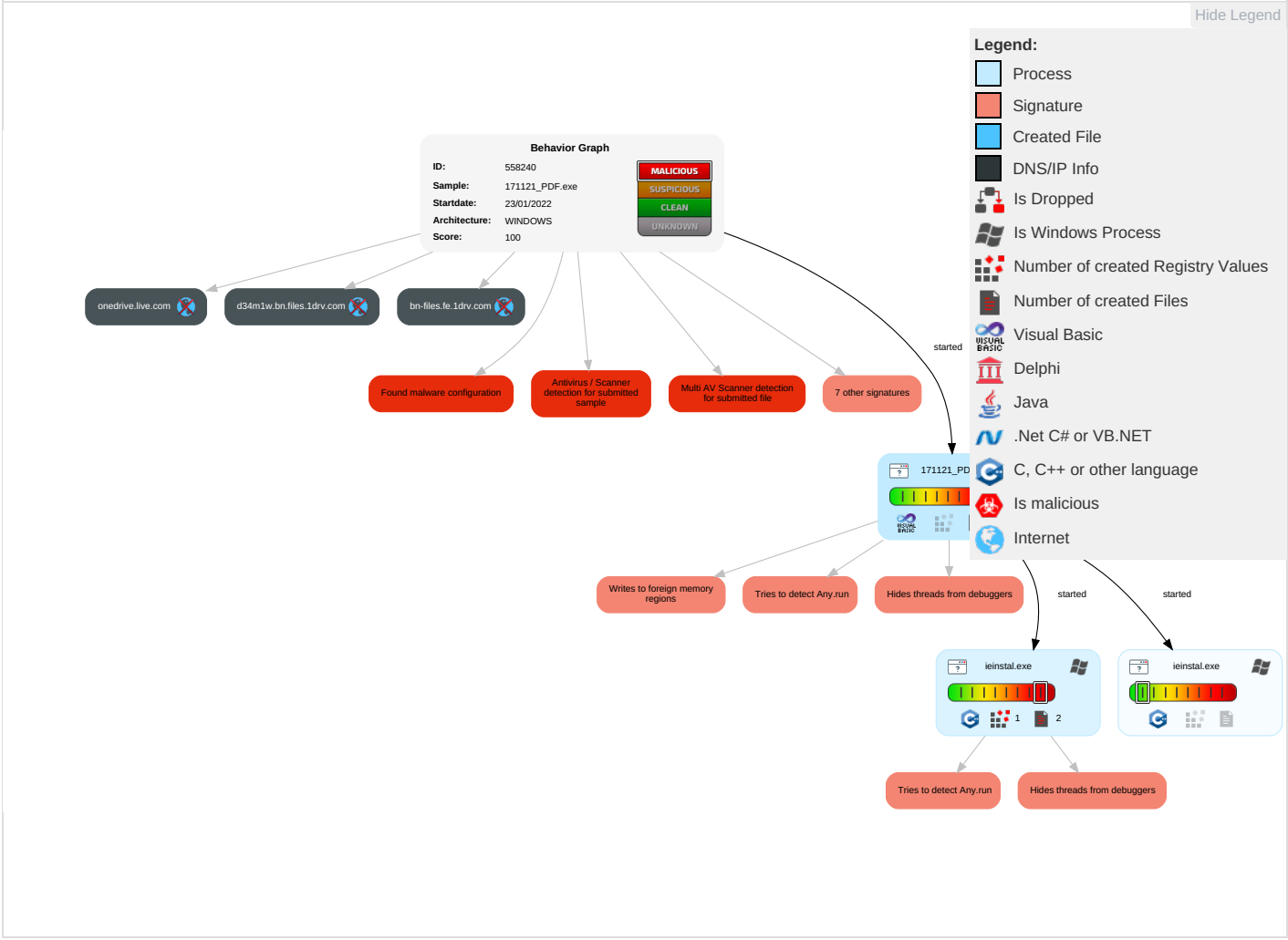
GuLoader behavior detected

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	2 Virtualization/Sandbox Evasion	OS Credential Dumping	3 1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Software Packing	LSASS Memory	2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 2 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

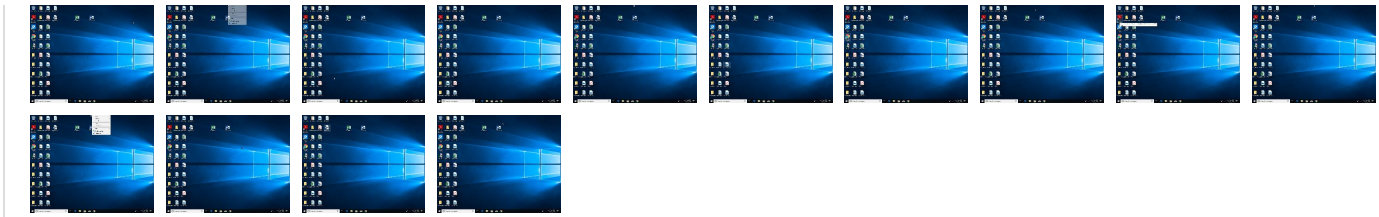
Behavior Graph



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
171121_PDF.exe	60%	Virustotal		Browse
171121_PDF.exe	17%	Metadefender		Browse
171121_PDF.exe	68%	ReversingLabs	Win32.Trojan.Shelsy	
171121_PDF.exe	100%	Avira	TR/AD.Nekark.jinay	
171121_PDF.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.171121_PDF.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1107800		Download File
0.0.171121_PDF.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.jinay		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
d34m1w.bn.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/downloa	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	558240
Start date:	23.01.2022
Start time:	06:42:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	171121_PDF.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@5/2@2/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 8.4% (good quality ratio 4.3%) • Quality average: 24.5% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 79% • 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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.4.86, 13.107.42.13, 13.107.42.12
- Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, fs.microsoft.com, bn-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, odc-web-geo.onedrive.akadns.net, odc-bn-files-brs.onedrive.akadns.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, odc-bn-files-geo.onedrive.akadns.net, ris.api.iris.microsoft.com, l-0004.l-msedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, l-0003.l-msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
06:45:46	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Skuffejernenesco2 C:\Users\user\AppData\Local\Temp\CUSCONINE\vagabo.exe
06:45:54	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Skuffejernenesco2 C:\Users\user\AppData\Local\Temp\CUSCONINE\vagabo.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\CUSCONINE\vagabo.exe

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

File Type:	data
Category:	dropped
Size (bytes):	112464
Entropy (8bit):	6.100427719868403
Encrypted:	false
SSDEEP:	1536:9PtG0c3vhsblLAvTlpS1HP9CGZG48TdiwOeQqn4kFgGYglLg:61JsblLAvI+FW48QwOen4Hi8
MD5:	68F03A1A9EC55A9B943A015C091817D6
SHA1:	C952F771410E036D5C897EC956FFBB09291B167E
SHA-256:	75E5DC79753DA6494A68CF2F5E9101FB6433103DD3AA7D8BADCD23DDD2F5F651
SHA-512:	A9C5946EEF3B54BCAF23EB53CBBABA0B1BB6438A0A6DEC675F7F2E4AF7CA1CED7AF2737DB1079A68F9EBE1126D9338EE91436E847D57C9A5726759B4F8EA5C0C
Malicious:	false
Reputation:	low
Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$....._.....Rich.....PE..L....~.N.....`. ..P.....p....@.....m..(.....+.....P.....8... .....text....\_.....`..... ..`.data.....p.....p.....@....rsrc....+.....0.....@..@..^.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\~DFD14B856B0CE15507.TMP

Process:	C:\Users\user\Desktop\171121_PDF.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.623084520004525
Encrypted:	false
SSDEEP:	12:rl3lKFQCb776fGZHbYS6TS63TXlYdl7HtllGXPuK9iUmTc:rbQylDVYdtNllG/uw7
MD5:	23BC92D1C5A3C3698C8524B7CEB3F5D9
SHA1:	199D2660FEA3F7310397A37A8C7C600E7A26D461
SHA-256:	5A6730EB0987730B214A46DC814FE2071576A338B2210DECE2780AC6E3B45DD7
SHA-512:	6FA7CAB689912B93C312D35E0E0F218E6138A3BCB8BC1B31CF0F80E4795C079F8589B879CCAC55C14262C710D4772A4067CCA4ED7890AED678EC988D113227D
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.100488610521297
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:	171121_PDF.exe
File size:	112464
MD5:	60d8b8589ba8045361ae148ee76c7582
SHA1:	328a778d026ad6611bb295bf3a799b6499fc7c7c
SHA256:	8f34d0008f07a4460c9ebc5a8d8a558a85979bd0112962eddf9506dc5b627989
SHA512:	6d7ab39a3367d72d70e0cf8af182fdf7b20100be1159465cebf5603c06bd485ffd0b5acee687ad029c1205c1cdadfbfe10002451b484cde1746ed2c8814f58e7
SSDEEP:	1536:OPtG0c3vhsblLAvTlpS1HP9CGZG48TdiwOeQqn4kFgGYglLg:X1JsblLAvI+FW48QwOen4Hi8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.....Rich.....PE..L....~.N.....`...P.....p....@

File Icon

Icon Hash:	f2c2c29190d2c783

Static PE Info

General

Entrypoint:	0x401194
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4ED97EE6 [Sat Dec 3 01:44:06 2011 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:	fca27436e553ec62bb2d0905390fd4e6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Bibaciousnessmnten3@Pinjerforhaa.Non, CN=Vrdiheftesgalets, OU=Formationsskridt, O=ptychoptery, L=Retrickedtrbesk, S=Linoxininvectivel5, C=LV
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 11/16/2021 7:35:05 PM 11/16/2022 7:35:05 PM
Subject Chain	• E=Bibaciousnessmnten3@Pinjerforhaa.Non, CN=Vrdiheftesgalets, OU=Formationsskridt, O=ptychoptery, L=Retrickedtrbesk, S=Linoxininvectivel5, C=LV
Version:	3
Thumbprint MD5:	81C291A64F4EEAD3EB815B820975A11F
Thumbprint SHA-1:	3B9FB2B3310D80BB215D1F0A8A1B4C5CE397126F
Thumbprint SHA-256:	6E26EF48D70BCD9763606EA3E88539664649D7701B6F561892E318BB4DB04839
Serial:	00

Entrypoint Preview

Instruction
push 00401A0Ch
call 00007F4FD4A94823h
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
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx+58h], al
push FFFFFFBFh
fadd st(0), st(7)
int1
dec edi
movsb
jmp 00007F4FD4A94840h

Instruction
sbb al, 8Eh
scasd
inc edx
aas
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
loopne 00007F4FD4A947F8h
or dword ptr [ebx], eax
jnc 00007F4FD4A948A7h
bound ebp, dword ptr [edi+72h]
imul ebp, dword ptr fs:[esi+00h], 20004108h
or byte ptr [ecx+00h], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
add dword ptr [edi+ebx*8-316D0720h], ecx
xor eax, 8026BB49h
nop
dec edx
and eax, 87C64A41h
out E9h, al
cmpsd
pop eax
rol dword ptr [edi-7Dh], 1
arpl word ptr [ebx+7Ah], dx
arpl word ptr [edx], cx
pop ss
and byte ptr [edx], bh
dec edi
lodsd
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
je 00007F4FD4A94835h

Instruction
add byte ptr [eax], al
push ebx
add eax, dword ptr [eax]
add byte ptr [eax], al
push cs
add byte ptr [esi+4Fh], al
inc esp
inc ebp
push edx
inc ecx
dec esp
inc ebp
push edx
push ebx
dec eax
pop ecx
inc esp
push edx
add byte ptr [42000701h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x16d14	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x19000	0x2bca	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1b000	0x750	.rsrc
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	0x90	.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	0x15ffc	0x16000	False	0.495827414773	data	6.39269902756	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x17000	0x17f8	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0x2bca	0x3000	False	0.236735026042	data	3.87641922123	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
SET	0x19724	0x24a6	MS Windows icon resource - 3 icons, 24x24, 16 colors, 4 bits/pixel, 24x24, 8 bits/pixel	English	United States
RT_ICON	0x1943c	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4152326007, next used block 7370615		
RT_GROUP_ICON	0x19428	0x14	data		
RT_VERSION	0x19140	0x2e8	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, _adj_fdiv_m64, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, _adj_fdiv_m32i, _adj_fdivr_m32i, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarSetVar, __vbaLateMemCallLd, _CIatan, __vbaR8IntI4, _allmul, _CItan, _CIexp, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
LegalCopyright	ART
InternalName	Brugstyveriscortic
FileVersion	1.00
CompanyName	ART
LegalTrademarks	ART
Comments	ART
ProductName	ART
ProductVersion	1.00
FileDescription	Classic ART
OriginalFilename	Brugstyveriscortic.exe

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2022 06:45:47.377051115 CET	55102	53	192.168.2.3	8.8.8.8
Jan 23, 2022 06:45:47.926724911 CET	56236	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 23, 2022 06:45:47.377051115 CET	192.168.2.3	8.8.8.8	0x102a	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Jan 23, 2022 06:45:47.926724911 CET	192.168.2.3	8.8.8.8	0x6b8c	Standard query (0)	d34m1w.bn.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 23, 2022 06:45:47.424824953 CET	8.8.8.8	192.168.2.3	0x102a	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 23, 2022 06:45:47.976964951 CET	8.8.8.8	192.168.2.3	0x6b8c	No error (0)	d34m1w.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jan 23, 2022 06:45:47.976964951 CET	8.8.8.8	192.168.2.3	0x6b8c	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 171121_PDF.exe PID: **6968**, Parent PID: **4448**

General

Start time:	06:43:39
Start date:	23/01/2022
Path:	C:\Users\user\Desktop\171121_PDF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\171121_PDF.exe"
Imagebase:	0x400000
File size:	112464 bytes
MD5 hash:	60D8B8589BA8045361AE148EE76C7582
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.498027231.0000000002320000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: **5012**, Parent PID: **6968**

General

Start time:	06:44:14
Start date:	23/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\171121_PDF.exe"
Imagebase:	0xdd0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 7124, Parent PID: 6968

General

Start time:	06:44:15
Start date:	23/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\171121_PDF.exe"
Imagebase:	0xdd0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000002.543844211.0000000003200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000000.352935282.0000000003200000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CUSCONINE\vagabo.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	3210112	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CUSCONINE\vagabo.exe	0	112464	00 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 13 fd 39 fd fd 39 fd fd 39 fd fd 5f fd fd 79 fd fd fd fd fd f9 fd fd fd fd 79 fd fd 52 69 63 68 39 fd fd 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 fd 7e fd 4e 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 60 01 00 00 50 00 00 00 00 00 00 fd 11 00 00 00 10 00 00 00 70 01 00 00 00 40	Z@!L!This program cannot be run in DOS mode.$_RichPEL~N`Pp @	success or wait	1	3204AFE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\171121_PDF.exe	unknown	112464	success or wait	1	3210112	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Skuffejernenesco2	unicode	C:\Users\user\AppData\Local\Temp\CUSCONINE\vagabo.exe	success or wait	1	3203B14	RegSetValueExA

Disassembly

No disassembly