ID: 452431
Sample Name: 41609787.exe
Cookbook: default.jbs
Time: 10:40:48
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 41609787.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 4
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
HIPS / PFW / Operating System Protection Evasion: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 5
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 12
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 12
Data Directories 12
Sections 13
Resources 13
Imports 13
Version Infos 13
Possible Origin 13
Network Behavior 13
Snort IDS Alerts 13
Network Port Distribution 13
TCP Packets 13
UDP Packets 13
ICMP Packets 13
DNS Queries 13
DNS Answers 13
HTTPS Packets 14
Code Manipulations 14
Statistics 14
Behavior 14

System Behavior 14
Analysis Process: 41609787.exe PID: 4548 Parent PID: 5784 14
General 15
Registry Activities 15
Key Created 15
Key Value Created 15
Analysis Process: ieinstal.exe PID: 2120 Parent PID: 4548 15
General 15
File Activities 15
File Created 15
File Written 15
File Read 15
Registry Activities 15
Key Created 15
Key Value Created 15
Analysis Process: cmd.exe PID: 4608 Parent PID: 2120 15
General 16
File Activities 16
Analysis Process: conhost.exe PID: 5156 Parent PID: 4608 16
General 16
Analysis Process: reg.exe PID: 5776 Parent PID: 4608 16
General 16
File Activities 16
Disassembly 16
Code Analysis 16

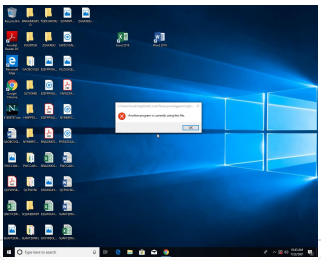
Windows Analysis Report 41609787.exe

Overview

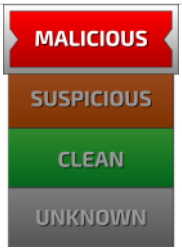
General Information

Sample Name:	41609787.exe
Analysis ID:	452431
MD5:	242fb5498503fda..
SHA1:	e45e4180137ea7..
SHA256:	7984d85806d611..
Infos:	

Most interesting Screenshot:



Detection



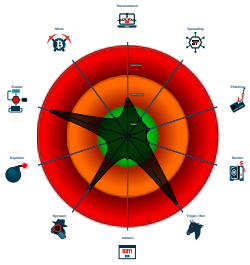
GuLoader Remcos

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

Signatures

- Found malware configuration
- GuLoader behavior detected
- Multi AV Scanner detection for doma…
- Yara detected GuLoader
- Yara detected Remcos RAT
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Installs a global keyboard hook
- Tries to detect Any.run
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- 41609787.exe (PID: 4548 cmdline: 'C:\Users\user\Desktop\41609787.exe' MD5: 242FB5498503FDAE24861CA26F762745)
  - ieinstal.exe (PID: 2120 cmdline: 'C:\Users\user\Desktop\41609787.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
    - cmd.exe (PID: 4608 cmdline: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - reg.exe (PID: 5776 cmdline: C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f MD5: CEE2A7E57DF2A159A065A34913A055C2)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://smokeadmsend.online/loade"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000002.726106922.00000000032B5000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000000.00000002.669650402.0000000002100000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Yara detected Remcos RAT

Networking:

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

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

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:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

GuLoader behavior detected

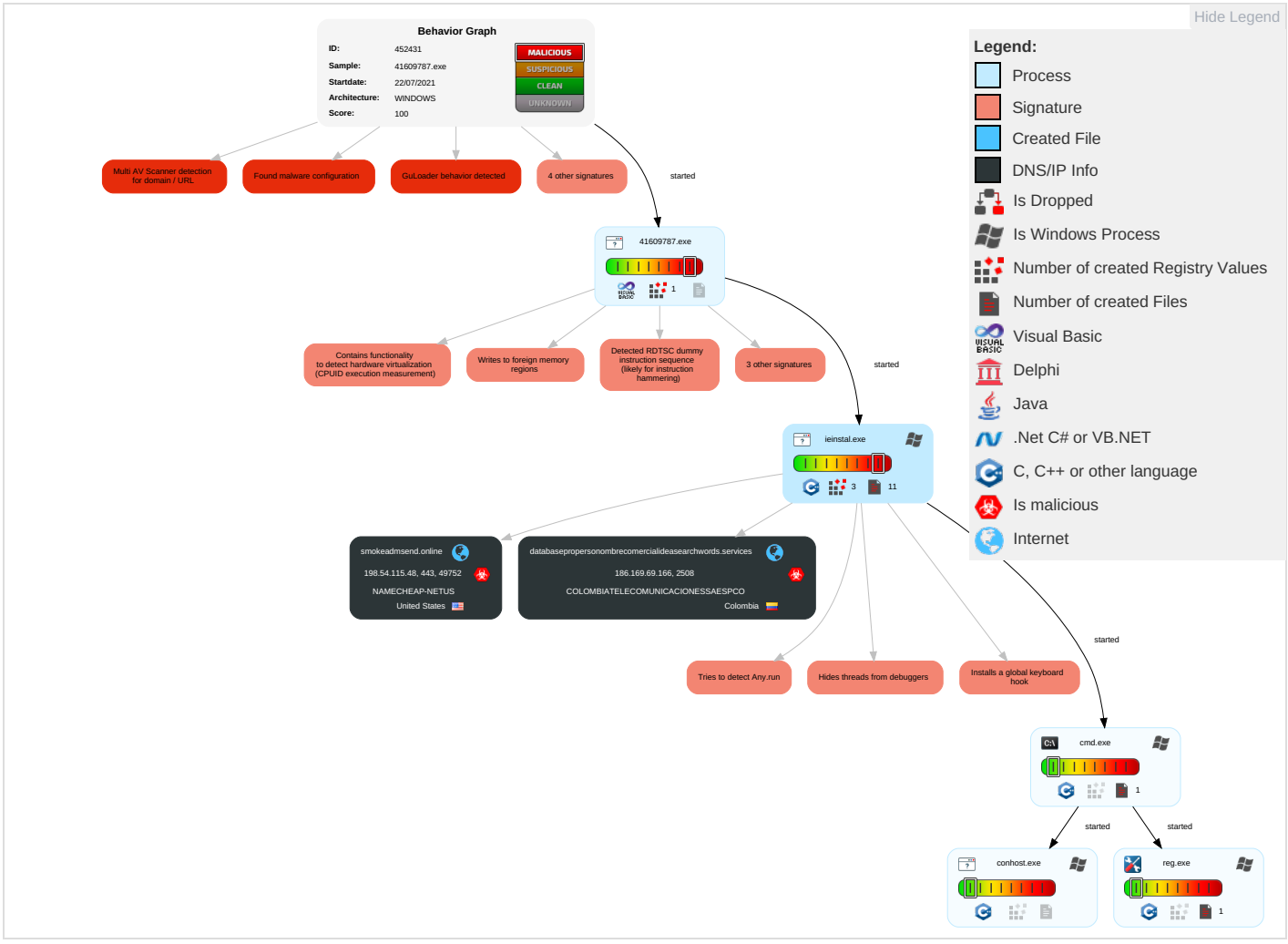
Yara detected Remcos RAT

Remote Access Functionality:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 6 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eave Inse Netv Com
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Modify Registry 1	LSASS Memory	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Expl Red Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 3	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Swa
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	Fallback Channels	Man Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Serv

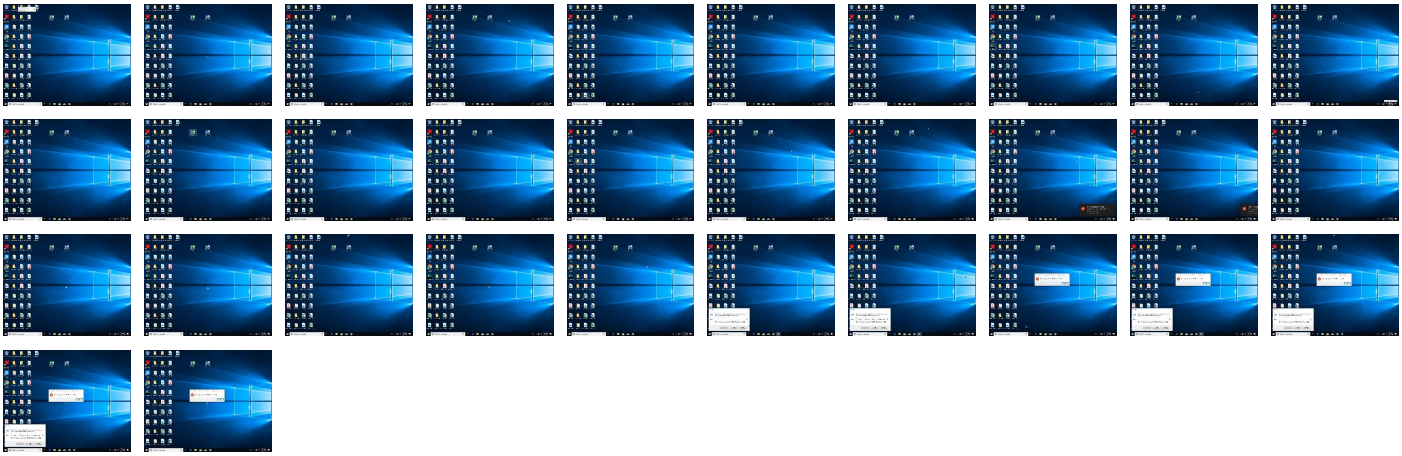
Behavior Graph

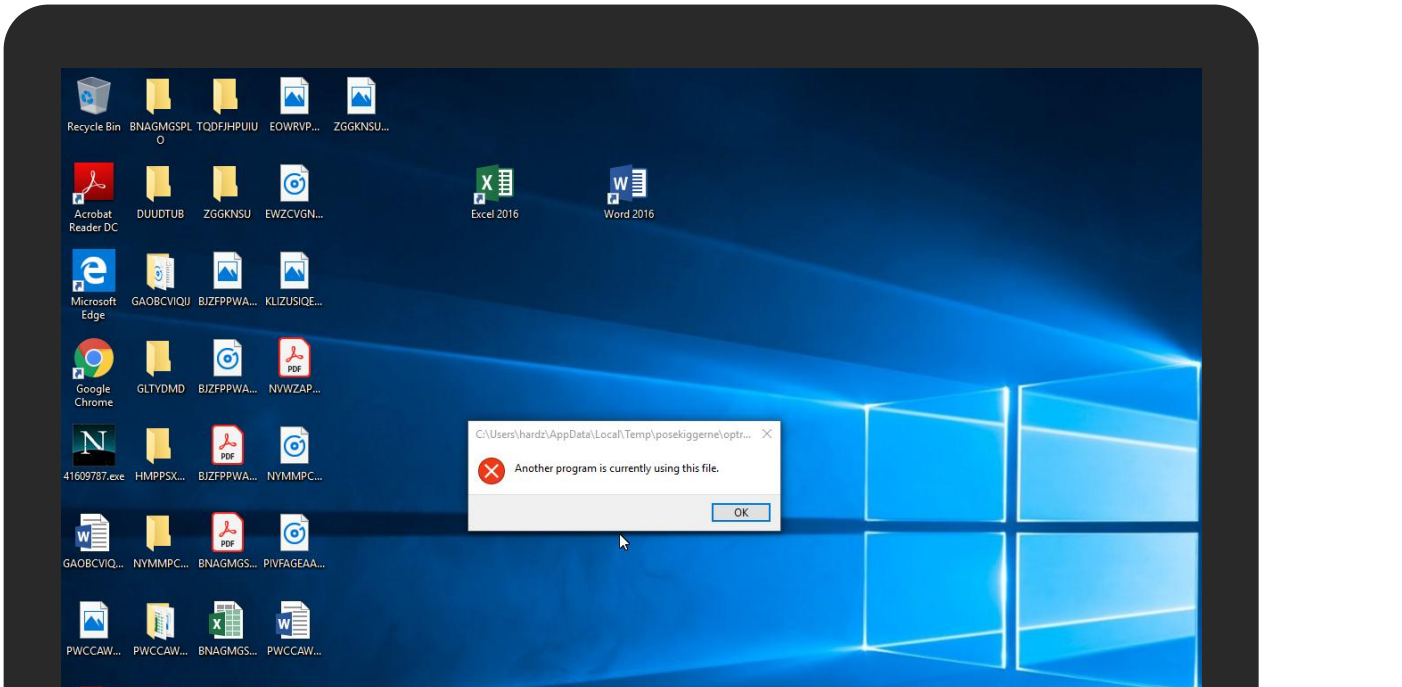


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
databasepropersonombrecomercialideasearchwords.services	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://smokeadmsend.online/loader/1ArmadaNac1copia_YCusoPusF143.bin	0%	Avira URL Cloud	safe	
http://https://smokeadmsend.online/loade	0%	Avira URL Cloud	safe	
http://https://smokeadmsend.online/loader/1ArmadaNac1copia_YCusoPusF143.binwininet.dllMozilla/5.0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smokeadmsend.online	198.54.115.48	true	true		unknown
databasepropersonombrecomercialideasearchwords.services	186.169.69.166	true	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://smokeadmsend.online/loade	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
186.169.69.166	databasepropersonombrecomercialideasearchwords.services	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	true
198.54.115.48	smokeadmsend.online	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452431
Start date:	22.07.2021
Start time:	10:40:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 1s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	41609787.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:	32
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.spyw.evad.winEXE@8/2@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.6% (good quality ratio 0.1%) • Quality average: 4.8% • Quality standard deviation: 11.9%
HCA Information:	• Successful, ratio: 68% • 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 • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:45:06	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SPINTOS C:\Users\user\AppData\Local\Temp\posekiggerne\optrner.exe
10:45:15	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SPINTOS C:\Users\user\AppData\Local\Temp\posekiggerne\optrner.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.115.48	75PO9981.exe	Get hash	malicious	Browse	• www.ownfiles.info/fl/
	21PO7513.exe	Get hash	malicious	Browse	• www.ownfiles.info/fl/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
databasepropersonombrecomercialideasearchwords.services	75030908.exe	Get hash	malicious	Browse	• 186.169.42.8
	76947851729_.exe	Get hash	malicious	Browse	• 181.235.3.85
	166691_pdf.exe	Get hash	malicious	Browse	• 181.235.4.212
	Factura Serfinanza05105370973507723576465319 4.exe	Get hash	malicious	Browse	• 186.169.43.144
	056373_pdf.exe	Get hash	malicious	Browse	• 186.169.43.144
	Factura Serfinanza02385478677524120978364812 9.exe	Get hash	malicious	Browse	• 186.169.43.144
	Factura Serfinanza08539921811122776187355057 0.exe	Get hash	malicious	Browse	• 186.169.43.144
	Factura Serfinanza03861248239738342089115074 3.exe	Get hash	malicious	Browse	• 186.169.43.144
	Factura Serfinanza10610959636331835960872777 1.exe	Get hash	malicious	Browse	• 186.169.72.174

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Factura Serfinanza05028822778874965281796074 4.exe	Get hash	malicious	Browse	• 186.169.72.174
	Factura Serfinanza04999760983251785127463018 4.exe	Get hash	malicious	Browse	• 186.169.72.174
	EXTRACTOSERFINANZA71836541810178615434666 1555.exe	Get hash	malicious	Browse	• 190.255.84.57
	EXTRACTOSERFINANZA98954370403149970409279 8964.exe	Get hash	malicious	Browse	• 190.255.84.57
	32657046_pdf.exe	Get hash	malicious	Browse	• 190.255.84.57
	6565426875_p.exe	Get hash	malicious	Browse	• 186.169.38.241
	4831902122_p.exe	Get hash	malicious	Browse	• 186.169.38.241
	8992538102_p.exe	Get hash	malicious	Browse	• 186.169.38.241
	9604_pdf.exe	Get hash	malicious	Browse	• 186.169.38.241
	Factura Serfinanza08976855354809098586981 4228.exe	Get hash	malicious	Browse	• 186.169.38.241
	EXTRACTOSERFINANZA89497863626880805125245 2885.exe	Get hash	malicious	Browse	• 186.169.38.241

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
COLOMBIATELECOMUNICACIONESS AESPCO	U1R7Ed7940	Get hash	malicious	Browse	• 186.113.206.66
	oEF7GAiRIg	Get hash	malicious	Browse	• 186.113.13 1.237
	BTNNG17tlh	Get hash	malicious	Browse	• 190.255.99.57
	MD5OxTSc6i	Get hash	malicious	Browse	• 190.252.13 6.167
	SUpODCSauS	Get hash	malicious	Browse	• 191.109.10 6.145
	TFG18FA4eD	Get hash	malicious	Browse	• 152.205.93.205
	eAtDhymLzp	Get hash	malicious	Browse	• 181.235.11 5.105
	ehn0f1d63M	Get hash	malicious	Browse	• 186.116.21 2.222
	zWumjXhWWz	Get hash	malicious	Browse	• 190.254.50.129
	e4qhQIKEim	Get hash	malicious	Browse	• 179.48.76.227
	YazlX01sZD	Get hash	malicious	Browse	• 186.116.15 4.100
	7Pvt6Jni6p	Get hash	malicious	Browse	• 167.65.244.226
	a1sMR3Vj8o	Get hash	malicious	Browse	• 167.2.131.28
	471u0A1FPw	Get hash	malicious	Browse	• 190.255.75.41
	395d6gwkWK	Get hash	malicious	Browse	• 152.205.93.229
	YXYFqHRx2m	Get hash	malicious	Browse	• 167.13.146.158
	XfKsLIPLUu	Get hash	malicious	Browse	• 190.67.85.74
	Z7bNxhhS7y	Get hash	malicious	Browse	• 190.67.85.63
	lq2609LxT8	Get hash	malicious	Browse	• 190.254.18 7.199
	khGshuibcr	Get hash	malicious	Browse	• 186.116.21 2.225
NAMECHEAP-NETUS	ORDER . 4500028602 .doc	Get hash	malicious	Browse	• 198.54.122.60
	Payment_invoice.exe	Get hash	malicious	Browse	• 198.54.117.212
	SUpODCSauS	Get hash	malicious	Browse	• 198.54.114.130
	0ZZqw52a6S.exe	Get hash	malicious	Browse	• 199.193.7.228
	nZdwtTEYoW.exe	Get hash	malicious	Browse	• 198.54.122.60
	CORRECT BANK DETAILS FORM.doc	Get hash	malicious	Browse	• 198.54.122.60
	Shipping Documents .doc	Get hash	malicious	Browse	• 198.54.122.60
	QxnlprRUTx.exe	Get hash	malicious	Browse	• 199.188.20 0.230
	0Lh7eA2VUZ.exe	Get hash	malicious	Browse	• 198.54.122.60
	REQUEST FOR QUOTATIO 158930165.doc	Get hash	malicious	Browse	• 198.54.122.60
	Statement.xlsx	Get hash	malicious	Browse	• 162.0.237.9
	Inv PKF312021.doc	Get hash	malicious	Browse	• 198.54.122.60
	RFQ- ROTO Fittings- 19072021.doc	Get hash	malicious	Browse	• 198.54.122.60
	INVOICE.exe	Get hash	malicious	Browse	• 198.54.117.211
	Order.exe	Get hash	malicious	Browse	• 198.54.117.215
	SOA.exe	Get hash	malicious	Browse	• 198.54.122.60
	Inv_7623980.exe	Get hash	malicious	Browse	• 63.250.34.223
	xBMx9OBP97.exe	Get hash	malicious	Browse	• 198.54.114.131
	CSyG3zNcwS.exe	Get hash	malicious	Browse	• 198.54.114.131
	BrCi5pJr8J.exe	Get hash	malicious	Browse	• 198.54.114.131

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	B5xK9XEvzO.exe	Get hash	malicious	Browse	• 198.54.115.48
	RsEvjl1iTt.exe	Get hash	malicious	Browse	• 198.54.115.48
	ORD.ppt	Get hash	malicious	Browse	• 198.54.115.48
	39pfFwU3Ns.exe	Get hash	malicious	Browse	• 198.54.115.48
	47a8af.exe.exe	Get hash	malicious	Browse	• 198.54.115.48
	Comprobante1.vbs	Get hash	malicious	Browse	• 198.54.115.48
	ZlvFNj.dll	Get hash	malicious	Browse	• 198.54.115.48
	QT2kxM315B.exe	Get hash	malicious	Browse	• 198.54.115.48
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 198.54.115.48
	Convert HEX uit phishing mail.htm	Get hash	malicious	Browse	• 198.54.115.48
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 198.54.115.48
	192-3216-Us.gt.com.html	Get hash	malicious	Browse	• 198.54.115.48
	N41101255652.vbs	Get hash	malicious	Browse	• 198.54.115.48
	FILE_2932NH_9923.exe	Get hash	malicious	Browse	• 198.54.115.48
	RDlkHCLRxE.exe	Get hash	malicious	Browse	• 198.54.115.48
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 198.54.115.48
	Swift_Fattura_0093320128_.exe	Get hash	malicious	Browse	• 198.54.115.48
	SecuriteInfo.com.Variant.Graftor.981190.24096.exe	Get hash	malicious	Browse	• 198.54.115.48
	IPVrDRKfYj.exe	Get hash	malicious	Browse	• 198.54.115.48
	11.docx	Get hash	malicious	Browse	• 198.54.115.48

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\posekiggerne\optrner.exe	
Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	data
Category:	dropped
Size (bytes):	192513
Entropy (8bit):	5.613557039365368
Encrypted:	false
SSDEEP:	3072:2+ogFpSWSqqbZ0ZEuwGE5pwFGHiG1InFGHiPZEuwGE5pi:2+7AtqqbZFfGE5pakipkiufGE5pi
MD5:	873CC0BFAAB852FD58C0EB4B8D29026D
SHA1:	07C871EC1385B80D314A9EA0B047CC85D24CEE24
SHA-256:	9E6B7578CAE3E4CC0354AD9912EA36F7E3D0968DE07D30C4F3C60C1183D919C6
SHA-512:	A7609B36561ACD7AACAD21ABF085489C86A72103FCE5F32501B2B660644C6DF1AC5A4A201E39DF67F21D6F3E5C519EC3C51A633E99D8FED07D425497E84997F
Malicious:	false
Reputation:	low
Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$.....+O.E..E..E.X.K..E...L..E..H..E.Rich.E.....PE..L.....1M.... .....@.....P....@.....c.....E..(....p.....0... .....D.....text....;.....@ ....`.data...$....P.....P.....@....rsrc.....p.....`.....@..@..^.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\Runtime2021\xlogs201.dat	
Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	data
Category:	dropped
Size (bytes):	182
Entropy (8bit):	3.366956781623735
Encrypted:	false
SSDEEP:	3:rklKlVnGlNWKUel5JWRal2Jl+7R0DAlBG4J+Rf3GLilXIknNQblovDl9il:llK/yN+65YcleeDAlgRf2e56bW/G
MD5:	CBD9A222C0C0CB1C08C8DC24D7C02F86
SHA1:	40FCA05C695340804995E29FDD5D11A488D8CAEA
SHA-256:	A59E7F82238F3158F2F86EFEFA0A8FB20ACEA309AD84DD61683639197D01A01C
SHA-512:	485877FC044D8046B408C5157BCB29FB3DC06B7DB10695F5886474398217B54EE8A2607527B292D3B179E37904C31FB186FB140ECBA375D7AAE360E6DBDFF44(

C:\Users\user\AppData\Roaming\Runtime2021\xlogs201.dat	
Malicious:	false
Reputation:	low
Preview:	....[.2.0.2.1./.0.7./.2.2. .1.0.:.4.5.:.1.1. .O.f.f.l.i.n.e. .K.e.y.l.o.g.g.e.r. .S.t.a.r.t.e.d.].....[. .R.u.n. .].....[.W.i.n.].r.....[. .P.r.o.g.r.a.m. .M.a.n.a.g.e.r. .]....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.613575589393616
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:	41609787.exe
File size:	192512
MD5:	242fb5498503fdae24861ca26f762745
SHA1:	e45e4180137ea7c9d81f127fac0af48cf3b4e8d7
SHA256:	7984d85806d611e8d7e3ec5640186ebce9b1daccbd07a4bbda0fc6e0e5666299
SHA512:	5717a9d38ff151384fe522b5b55f7a4882bcb897d65d1c9fbd0b155f05138cc698db39805d34150daf5260906d8e09c6d752190e7d681eb181eb3569378a48fd
SSDEEP:	3072:F+ogFpSWSqqbZ0ZEuwGE5pwFGHiG1InFGHiPZEuwGE5p:F+7AtqqbZFfGE5pakipkiufGE5p
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+O..E...E...E.X.K...E...L...E...H...E.Rich..E.....PE..L.....1M.....@.....P....@.....

File Icon

Icon Hash:	734c5974650d010d

Static PE Info

General

Entrypoint:	0x4014f0
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:	0x4D31AB09 [Sat Jan 15 14:11:21 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:	a70b1f0c9f8eea03c5b5d32861bccaa9

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x23b04	0x24000	False	0.399773491753	data	5.92220108342	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x25000	0x1a24	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x27000	0x8ac0	0x9000	False	0.329942491319	data	4.39398480347	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
Kazakh	Kazakhstan	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-10:45:13.302249	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.169.69.166	192.168.2.3
07/22/21-10:45:44.235836	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.169.69.166	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 10:45:09.855098009 CEST	192.168.2.3	8.8.8.8	0x18f2	Standard query (0)	smokeadmsend.online	A (IP address)	IN (0x0001)
Jul 22, 2021 10:45:12.766573906 CEST	192.168.2.3	8.8.8.8	0xfec1	Standard query (0)	databaseproperpersonombrecomercialideasearchwords.services	A (IP address)	IN (0x0001)
Jul 22, 2021 10:45:34.928658009 CEST	192.168.2.3	8.8.8.8	0xf13	Standard query (0)	databaseproperpersonombrecomercialideasearchwords.services	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 10:45:09.919981956 CEST	8.8.8.8	192.168.2.3	0x18f2	No error (0)	smokeadmsend.online		198.54.115.48	A (IP address)	IN (0x0001)
Jul 22, 2021 10:45:12.826633930 CEST	8.8.8.8	192.168.2.3	0xfec1	No error (0)	databaseproopersonombrecomerciallideasearchwords.services		186.169.69.166	A (IP address)	IN (0x0001)
Jul 22, 2021 10:45:34.986488104 CEST	8.8.8.8	192.168.2.3	0xf13	No error (0)	databaseproopersonombrecomerciallideasearchwords.services		186.169.69.166	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 10:45:10.378618956 CEST	198.54.115.48	443	192.168.2.3	49752	CN=smokeadmsend.online CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jun 17 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sat Jun 18 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 41609787.exe PID: 4548 Parent PID: 5784

General

Start time:	10:41:34
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\41609787.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\41609787.exe'
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	242FB5498503FDAE24861CA26F762745
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.669650402.0000000002100000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: ieinstal.exe PID: 2120 Parent PID: 4548

General

Start time:	10:44:29
Start date:	22/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\41609787.exe'
Imagebase:	0xbb0000
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_Remcos, Description: Yara detected Remcos RAT, Source: 0000001B.00000002.726106922.00000000032B5000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 4608 Parent PID: 2120

General

Start time:	10:45:11
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5156 Parent PID: 4608

General

Start time:	10:45:12
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 5776 Parent PID: 4608

General

Start time:	10:45:12
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
Imagebase:	0x1380000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis