ID: 528744
Sample Name: duLT5gkRjy.exe
Cookbook: default.jbs
Time: 18:22:22
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report duLT5gkRjy.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Socelars 4
Yara Overview 4
Initial Sample 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Stealing of Sensitive Information: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
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 10
ASN 11
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
Static File Info 14
General 14
File Icon 14
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 15
Sections 15
Resources 15
Imports 15
Version Infos 15
Possible Origin 15
Network Behavior 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 16
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 16
HTTPS Proxied Packets 16
Code Manipulations 17
Statistics 17
Behavior 17
System Behavior 17
Analysis Process: duLT5gkRjy.exe PID: 5068 Parent PID: 5916 17
General 17
File Activities 18
File Created 18
Analysis Process: WerFault.exe PID: 4060 Parent PID: 5068 18

General 18
File Activities 18
File Created 18
File Deleted 18
File Written 18
Registry Activities 18
Key Created 18
Key Value Created 18
Disassembly 18
Code Analysis 18

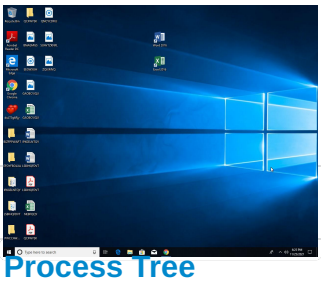
Windows Analysis Report duLT5gkRjy.exe

Overview

General Information

Sample Name:	duLT5gkRjy.exe
Analysis ID:	528744
MD5:	d42456f7afc8126..
SHA1:	30f49d0f3d46cc9..
SHA256:	a5b981c1006598..
Tags:	exe Socelars
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

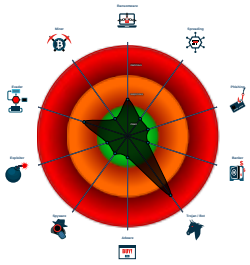
Socelars

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Socelars
- Multi AV Scanner detection for doma…
- May check the online IP address of …
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- One or more processes crash
- Contains functionality to check if a d…
- PE file contains sections with non-s…
- Internet Provider seen in connection…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- duLT5gkRjy.exe (PID: 5068 cmdline: "C:\Users\user\Desktop\duLT5gkRjy.exe" MD5: D42456F7AFC812628A9FF67D8C9340EB)
  - WerFault.exe (PID: 4060 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5068 -s 1932 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Socelars

```
{
  "C2 url": "http://ngdatas.pw/"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
duLT5gkRjy.exe	JoeSecurity_Socelars	Yara detected Socelars	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.266028618.000000000146A000.00000002.00020000.sdmp	JoeSecurity_Socelars	Yara detected Socelars	Joe Security	
00000001.00000000.250943662.000000000146A000.00000002.00020000.sdmp	JoeSecurity_Socelars	Yara detected Socelars	Joe Security	
00000001.00000000.244816151.000000000146A000.00000002.00020000.sdmp	JoeSecurity_Socelars	Yara detected Socelars	Joe Security	
00000001.00000000.251852996.000000000146A000.00000002.00020000.sdmp	JoeSecurity_Socelars	Yara detected Socelars	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: duLT5gkRjy.exe PID: 5068	JoeSecurity_Socelars	Yara detected Socelars	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.duLT5gkRjy.exe.1350000.0.unpack	JoeSecurity_Socelars	Yara detected Socelars	Joe Security	
1.0.duLT5gkRjy.exe.1350000.2.unpack	JoeSecurity_Socelars	Yara detected Socelars	Joe Security	
1.0.duLT5gkRjy.exe.1350000.0.unpack	JoeSecurity_Socelars	Yara detected Socelars	Joe Security	
1.0.duLT5gkRjy.exe.1350000.1.unpack	JoeSecurity_Socelars	Yara detected Socelars	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 submitted file

Multi AV Scanner detection for domain / URL

Networking:

May check the online IP address of the machine

C2 URLs / IPs found in malware configuration

Stealing of Sensitive Information:

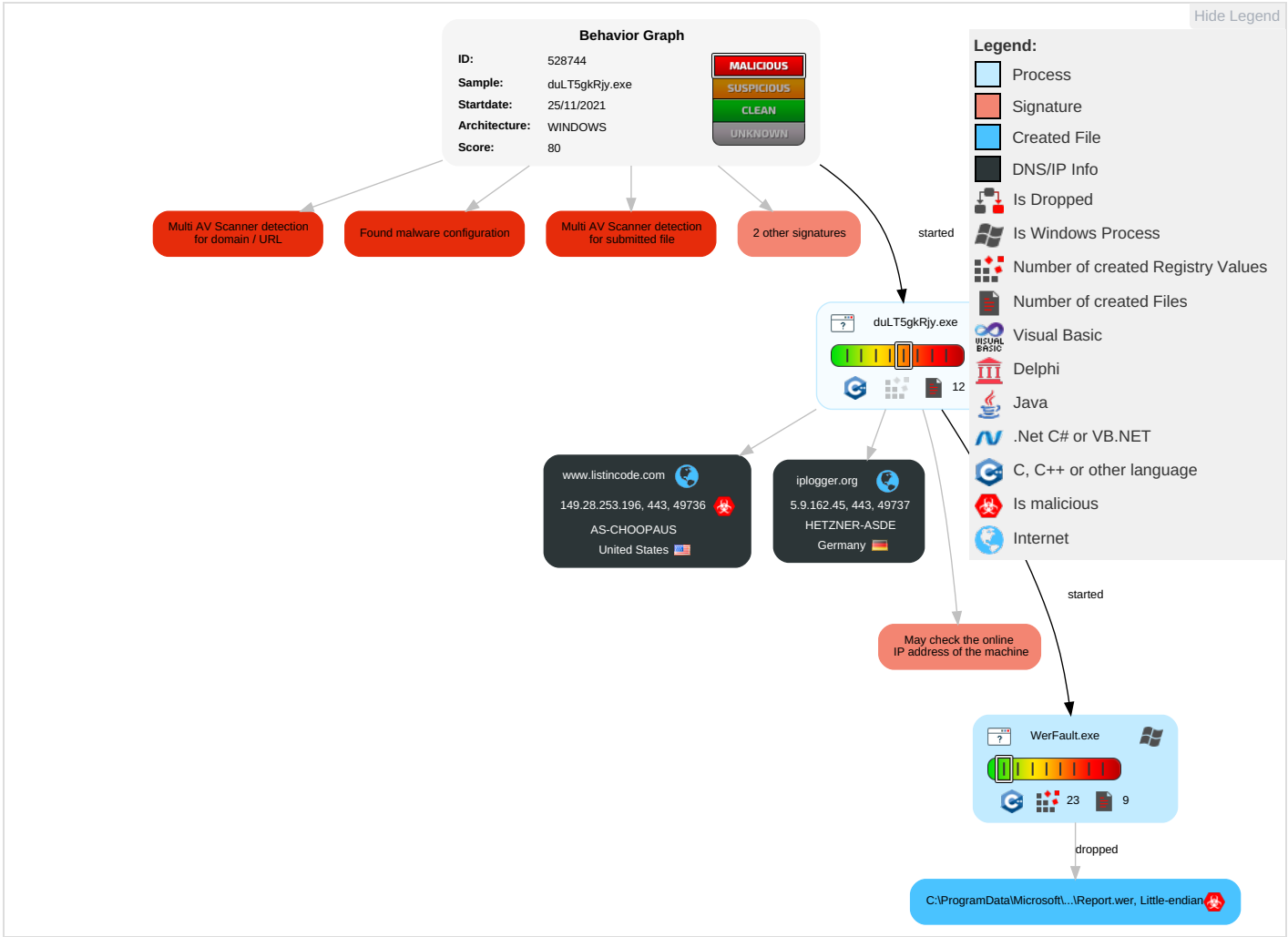
Yara detected Socelars

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	LSASS Driver 1	Process Injection 2	Virtualization/Sandbox Evasion 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop c Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	LSASS Driver 1	Process Injection 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Virtualization/Sandbox Evasion 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

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
duLT5gkRjy.exe	62%	Virustotal		Browse
duLT5gkRjy.exe	59%	ReversingLabs	Win32.Adware.ExtInstaller	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.listincode.com	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.channelinfo.pw/index.php/Home/Index/getExe	0%	URL Reputation	safe	
http://ngdatas.pw/https://www.listincode.com/0.0.0.0%d.%d.%d.%dhttp-1ZIP	0%	URL Reputation	safe	
http://www.ecgbg.com	0%	Virustotal		Browse
http://www.ecgbg.com	0%	Avira URL Cloud	safe	
http://https://www.listincode.com/	0%	URL Reputation	safe	
http://www.ecgbg.com/Home/Index/getdata	0%	Avira URL Cloud	safe	
http://www.channelinfo.pw/index.php/Home/Index/getExeidnameexe_urlexe_namerun_valuecountry_codeaband	0%	URL Reputation	safe	
http://ngdatas.pw/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iplogger.org	5.9.162.45	true	false		high
www.listincode.com	149.28.253.196	true	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://iplogger.org/1GWfv7	false		high
http://https://www.listincode.com/	true	• URL Reputation: safe	unknown
http://ngdatas.pw/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.28.253.196	www.listincode.com	United States		20473	AS-CHOOPAUS	true
5.9.162.45	iplogger.org	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528744
Start date:	25.11.2021
Start time:	18:22:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	duLT5gkRjy.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:	25
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:	mal80.troj.winEXE@2/6@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:23:31	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.28.253.196	EaCmG75WxF.exe	Get hash	malicious	Browse	
	EaCmG75WxF.exe	Get hash	malicious	Browse	
	OPKyR75fJn.exe	Get hash	malicious	Browse	
	LZxr7xI4nc.exe	Get hash	malicious	Browse	
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	
	23062BA932165210EBB3FFCD15474E79F19E6AD74869F.exe	Get hash	malicious	Browse	
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	
	FhP4JYCU7J.exe	Get hash	malicious	Browse	
	FhP4JYCU7J.exe	Get hash	malicious	Browse	
	44E401AAF0B52528AA033257C1A1B8A09A2B10EDF26ED.exe	Get hash	malicious	Browse	
	77012C024869BA2639B54B959FAB1E10EBAAF8EBB9BFC.exe	Get hash	malicious	Browse	
	WQRrng5aiw.exe	Get hash	malicious	Browse	
	WQRrng5aiw.exe	Get hash	malicious	Browse	
	22BA4262D93379DE524029DAFC7528E431E56A22CB293.exe	Get hash	malicious	Browse	
	kq5Of3SOMZ.exe	Get hash	malicious	Browse	
	QABYgAqa5Z.exe	Get hash	malicious	Browse	
	aBGNeDS7yM.exe	Get hash	malicious	Browse	
	aBGNeDS7yM.exe	Get hash	malicious	Browse	
	zMvP34LhcZ.exe	Get hash	malicious	Browse	
5.9.162.45	VDnn1698j5.exe	Get hash	malicious	Browse	• iplogger.org/1YLyj7

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TEiwRyJ2v1.exe	Get hash	malicious	Browse	• iplogger.org/1YLyj7
	sBz6zVtsB1.exe	Get hash	malicious	Browse	• iplogger.org/1YLyj7
	qTtykpVyaY.exe	Get hash	malicious	Browse	• iplogger.org/1YLyj7
	mXLL1BHUQh.exe	Get hash	malicious	Browse	• iplogger.org/1YLyj7
	EVhlUVrKx8.exe	Get hash	malicious	Browse	• iplogger.org/2A2xh6
	pQscpg84Lh.exe	Get hash	malicious	Browse	• iplogger.org/1PZN77
	pl8c1emoOu.exe	Get hash	malicious	Browse	• iplogger.org/1juiu7
	RmzVjXQ0a6.exe	Get hash	malicious	Browse	• iplogger.org/1juiu7
	fMo9q56dnX.exe	Get hash	malicious	Browse	• iplogger.org/1juiu7
	Screenshot00112021.scr.exe	Get hash	malicious	Browse	• iplogger.org/1BwFn7.gz
	SAlxtNmHFR.exe	Get hash	malicious	Browse	• iplogger.org/1BTpm7

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
iplogger.org	EaCmG75WxF.exe	Get hash	malicious	Browse	• 5.9.162.45
	EaCmG75WxF.exe	Get hash	malicious	Browse	• 5.9.162.45
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 5.9.162.45
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	• 5.9.162.45
	j0UcwcqjvM.exe	Get hash	malicious	Browse	• 5.9.162.45
	0K31jgS20G.exe	Get hash	malicious	Browse	• 5.9.162.45
	vAsfZhw32P.exe	Get hash	malicious	Browse	• 5.9.162.45
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 5.9.162.45
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 5.9.162.45
	WQRrng5aiw.exe	Get hash	malicious	Browse	• 5.9.162.45
	WQRrng5aiw.exe	Get hash	malicious	Browse	• 5.9.162.45
	e8rimWGicH.exe	Get hash	malicious	Browse	• 5.9.162.45
	kq5Of3SOMZ.exe	Get hash	malicious	Browse	• 5.9.162.45
	RtpLhZOyaf.exe	Get hash	malicious	Browse	• 5.9.162.45
	vWNrGi9qLx.exe	Get hash	malicious	Browse	• 5.9.162.45
	VDnn1698j5.exe	Get hash	malicious	Browse	• 5.9.162.45
	TEiwRyJ2v1.exe	Get hash	malicious	Browse	• 5.9.162.45
	iIrI72Motw.exe	Get hash	malicious	Browse	• 5.9.162.45
	sBz6zVtsB1.exe	Get hash	malicious	Browse	• 5.9.162.45
	eJV3ZMQ2Go.exe	Get hash	malicious	Browse	• 5.9.162.45
www.listincode.com	EaCmG75WxF.exe	Get hash	malicious	Browse	• 149.28.253.196
	EaCmG75WxF.exe	Get hash	malicious	Browse	• 149.28.253.196
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 149.28.253.196
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	• 149.28.253.196
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 149.28.253.196
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 149.28.253.196
	WQRrng5aiw.exe	Get hash	malicious	Browse	• 149.28.253.196
	WQRrng5aiw.exe	Get hash	malicious	Browse	• 149.28.253.196
	kq5Of3SOMZ.exe	Get hash	malicious	Browse	• 149.28.253.196
	aBGNeDS7yM.exe	Get hash	malicious	Browse	• 149.28.253.196
	aBGNeDS7yM.exe	Get hash	malicious	Browse	• 149.28.253.196
	f4gxrcTDkV.exe	Get hash	malicious	Browse	• 149.28.253.196
	SOO6hKZ7M0.exe	Get hash	malicious	Browse	• 149.28.253.196
	SOO6hKZ7M0.exe	Get hash	malicious	Browse	• 149.28.253.196
	f4gxrcTDkV.exe	Get hash	malicious	Browse	• 149.28.253.196
	l6erIt5Uil.exe	Get hash	malicious	Browse	• 149.28.253.196
	l6erIt5Uil.exe	Get hash	malicious	Browse	• 149.28.253.196
	B4A1AFA93C65EBA3AB6EFEB4624DCC8D65DBDEFEFE682.exe	Get hash	malicious	Browse	• 149.28.253.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fXlJhe5OGb.exe	Get hash	malicious	Browse	• 149.28.253.196
	vgVQ5S6MxN.exe	Get hash	malicious	Browse	• 149.28.253.196

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	EaCmG75WxF.exe	Get hash	malicious	Browse	• 149.28.253.196
	EaCmG75WxF.exe	Get hash	malicious	Browse	• 149.28.253.196
	EzCOXP6oxy.dll	Get hash	malicious	Browse	• 66.42.57.149
	IkroV40UrZ.dll	Get hash	malicious	Browse	• 66.42.57.149
	C1Q17Dg4RT.dll	Get hash	malicious	Browse	• 66.42.57.149
	MakbLShaqA.dll	Get hash	malicious	Browse	• 66.42.57.149
	MakbLShaqA.dll	Get hash	malicious	Browse	• 66.42.57.149
	OPKyR75fJn.exe	Get hash	malicious	Browse	• 149.28.253.196
	Ljm7n1QDZe	Get hash	malicious	Browse	• 68.232.173.117
	Jx35l5pwgd	Get hash	malicious	Browse	• 66.42.54.65
	tUJXpPwU27.dll	Get hash	malicious	Browse	• 66.42.57.149
	LZxr7xI4nc.exe	Get hash	malicious	Browse	• 149.28.253.196
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	• 149.28.253.196
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 149.28.253.196
	asbestos_safety_and_eradication_agency_enterprise_agreement 41573 .js	Get hash	malicious	Browse	• 45.76.154.237
	23062BA932165210EBB3FFCD15474E79F19E6AD74869F.exe	Get hash	malicious	Browse	• 149.28.253.196
	DA8063D9EB60622915D492542A6A8AE318BC87B4C5F89.exe	Get hash	malicious	Browse	• 155.138.201.103
	asbestos_safety_and_eradication_agency_enterprise_agreement 64081 .js	Get hash	malicious	Browse	• 45.76.154.237
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 66.42.57.149
	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 66.42.57.149
HETZNER-ASDE	EaCmG75WxF.exe	Get hash	malicious	Browse	• 5.9.162.45
	8p2NlqFgew.exe	Get hash	malicious	Browse	• 49.12.42.56
	EaCmG75WxF.exe	Get hash	malicious	Browse	• 5.9.162.45
	EzCOXP6oxy.dll	Get hash	malicious	Browse	• 78.47.204.80
	IkroV40UrZ.dll	Get hash	malicious	Browse	• 78.47.204.80
	C1Q17Dg4RT.dll	Get hash	malicious	Browse	• 78.47.204.80
	ff0231.exe	Get hash	malicious	Browse	• 5.9.96.94
	MakbLShaqA.dll	Get hash	malicious	Browse	• 78.47.204.80
	MakbLShaqA.dll	Get hash	malicious	Browse	• 78.47.204.80
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 88.99.22.5
	OPKyR75fJn.exe	Get hash	malicious	Browse	• 5.9.162.45
	meerkat.arm7	Get hash	malicious	Browse	• 148.251.220.118
	oQANZnrt9d	Get hash	malicious	Browse	• 135.181.142.151
	tUJXpPwU27.dll	Get hash	malicious	Browse	• 78.47.204.80
	LZxr7xI4nc.exe	Get hash	malicious	Browse	• 5.9.162.45
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	• 5.9.162.45
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 5.9.162.45
	23062BA932165210EBB3FFCD15474E79F19E6AD74869F.exe	Get hash	malicious	Browse	• 5.9.162.45
	exe.exe	Get hash	malicious	Browse	• 116.202.203.61
	J73PTzDghy.exe	Get hash	malicious	Browse	• 94.130.138.146

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	EaCmG75WxF.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	fpvN6iDp5r.msi	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	EaCmG75WxF.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Se adjunta el pedido, proforma.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	Statement.html	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	Michal November 23, 2021.html	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	survey-1384723731.xls	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	Wfedtqxbgeorkwcgiehsnsjbdjghrpjtlr.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	survey-1378794827.xls	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	mN2NobuuDv.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	cs.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	ORDINE + DDT A.M.F SpA.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	mal1.html	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	DOC5629.htm	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	Racun je u prilogu.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	exe.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	INF-BRdocsx.NDVDELDKRS.msi	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45
	2GEg45PlG9.exe	Get hash	malicious	Browse	• 149.28.253.196 • 5.9.162.45

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_duLT5gkRjy.exe_1716a7dbaca25d22b8ce403b85cf2c886155787b_b69a8483_0f8f88d3\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.0267413680848108
Encrypted:	false
SSDEEP:	192:c/IiK8oB+HBUZMXAjmH6v8/u7sZS274ltp1:cgiUB2BUZMXAj18/u7sZX4ltp
MD5:	9791D257D822DD8019C1C1BEFBFE0783
SHA1:	583B3EE02BC9562DC54A72DD591E673E24A8B66A
SHA-256:	37F9FE2C1EFBFD972E7CED4ACAFB817ED25F9BA27190691205311A3973372C9B
SHA-512:	EDEB1E8982642E2DF92E8A8B9E93939012569DD76140009D53480B979840FD67F798CBE9B93D468A64013AD6C5E2A3B26FADB91C65AA9808B7D9F2599FA73A8
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.3.6.7.0.0.7.4.9.3.2.6.4.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.2.3.6.7.0.1.0.4.9.3.2.4.3.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.2.a.0.0.7.a.c.-.b.d.b.c.-.4.3.e.b.-.b.a.0.d.-.b.4.0.d.9.0.e.6.2.3.9.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.9.f.f.2.8.5.9.-.0.e.5.d.-.4.6.7.3.-.b.0.7.3.-.a.8.0.7.7.f.9.e.b.5.1.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.d.u.L.T.5.g.k.R.j.y...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.c.c.-.0.0.0.1.-.0.0.1.7.-.1.1.d.9.-.2.8.9.5.6.c.e.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.c.8.5.b.f.e.1.d.6.f.e.f.d.b.d.a.c.0.f.9.1.5.3.d.0.2.f.9.b.5.5.0.0.0.0.0.9.0.4.!.0.0.0.0.3.0.f.4.9.d.0.f.3.d.4.6.c.c.9.c.c.f.8.7.3.3.2.4.7.a.0.7.0.9.5.5.5.a.d.2.0.9.9.f.!.d.u.L.T.5.g.k.R.j.y...e.x.e.....T.a.r.g.e.t.A.p.p.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7933.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Nov 26 02:23:28 2021, 0x1205a4 type
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7933.tmp.dmp	
Size (bytes):	131814
Entropy (8bit):	1.9804120841231585
Encrypted:	false
SSDEEP:	384:WiL1p0Q6GlRScvwmIEGVQMW/wraE7twJuQeToI1UJTqeDKOKF:L6GWcvw9EGVQUraEGssIdyKOC
MD5:	CD7BD168A73892B70C6E43607A74B806
SHA1:	9FD336BDCAAE2D099311BA3E1180A6F3CFC27BC1
SHA-256:	D3D80F7D4301E3CB2BA187FA536EFE2AC1AE85F0CA2108F4FEA24B4C1F51E771
SHA-512:	116361494615758O3FB1620EC75E2DBFFA976A528F5CC75217A386B9B78CA67AE2348274846CC191A19823E3CD5FBEBB35ACB901E3377E4581C6AD9A85A001D1
Malicious:	false
Reputation:	low
Preview:	MDMP..... ..... E.a.....D.....,...L.....Q.....T.....8.....T.....K..6.....x#.....d%.....U.....B.....%..... .GenuineIntelW.....T.....E.a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER80A6.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8296
Entropy (8bit):	3.7008050316408068
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiDd6GKC6YgDSUdoJgmffSVCprB89b/Asf+1m:RrlsNi56G/6YUSUdoJgmffSD/Tft
MD5:	DE019634757A2E498589659AABE2FA25
SHA1:	C9FEF1E6A406C902924989176DE108134D3BC0F9
SHA-256:	8DBAD734D69208DDC814C03F34B460BA87FAE5456C55A61FE221B38E2F9AE649
SHA-512:	2813EB0BB2DE93A09654AA10DE0A7BAD1147E14E3CEAF7CDAE5CCDA59B1AF572425E721A3779F5775E4F41B946E33A6FE116E8E22EC45DE96A9CD48F70E40B47
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.0.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8328.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4563
Entropy (8bit):	4.475311563035437
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUJgtWI9+AWSC8B08fm8M4JnCfBifsFy7+q8OxuDOl+mtdF0q03d:uITfSt5SNnJnC8NXQjmtdF0q03d
MD5:	1AB2EC2741530EB35DE688CF7BB89B06
SHA1:	067F6C95C9B2F97CFCC061D40B70DDE4D4C24564
SHA-256:	FD2F2AA348EDA2BC9759C175309B360CA294EFA0E1787D0F589846CB53214793
SHA-512:	FF0F60EB939DE7A449388D90BFDA99ADC36EB6ACC1B16B233880009016FF53962C47B3EE10CB63C0C58CECBB6AC417140FE0467040D4F27C6719CF3828BBB87
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1270774" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.277985648101297
Encrypted:	false

C:\Windows\appcompat\Programs\Amcache.hve	
SSDEEP:	12288:d5ujz4qQswYDf9MTryEn6zDoTd00Fg6cYKuvrlRIw4oYqFvKEf:Pmz4qQswYDf9MTTWC0o
MD5:	6E2BD6B0FBF1D4BA46D0FC6C25511830
SHA1:	4194EA0B60BD71B986E5DA6D7CEF76CA3093B0C9
SHA-256:	5DF90C277F31BB2E17449C2803535D49FB975B0272839C8FE771623FA04A3644
SHA-512:	B71C2002477740638312055B55999CF2A3066D09D6B5DC5869E91B011F4715B21B838FDDB64223EDF36168CFB5ED4BB11F0BA5C00AD06948B2F10407B93E44078
Malicious:	false
Reputation:	low
Preview:	regfX...X...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm./..l..... .....N..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	4.07512415013091
Encrypted:	false
SSDEEP:	384:JVSKQpIFg53EDxxkeRu3xxvYdnq9SaPDSpafYzI+yD+hBzpfIVjQOU6XadYV7i+t:JEKe3Gxkau3xdYduSaPupafYzTyDefIX
MD5:	A3C48A0B657AB5E9A93804801E47146B
SHA1:	8BCE5C32FEB8733974C2027DF0FAEB88A05E15A9
SHA-256:	1FB6140D42DB3FE71530F5DFEB7E5B429F56293008EA1AC5158235207267C568
SHA-512:	2B76B6C020F6605A913D566E7B4CDCDAE55CC443778D01CB7F1AB17431E8FD3DE55AF3599E17BFCBFAB4D12A9BC7A491466B4A85409E1BB4874585932151077E
Malicious:	false
Reputation:	low
Preview:	regfW...W...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm./..l..... .....N..HvLE.^.....W.....y./.V/....nn.....0.....hbin.....p.\.....nk,.....l..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .....l..... .....8~..... .....Z.....Root.....lf.....Root....nk .....l..... .....*.....DeviceCensus..... .....vk.....WritePermissions

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.685246086092563
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:	duLT5gkRjy.exe
File size:	1552896
MD5:	d42456f7afc812628a9ff67d8c9340eb
SHA1:	30f49d0f3d46cc9ccf8733247a0709555ad2099f
SHA256:	a5b981c10065983578a2bca4399f901bd5a4e87b4ebe2d05c1f9971fb9fb36ac
SHA512:	02de7cd71c5155ac5d08f7e432f5f3a138a6800d74479c4696cf877bbcf8fc99bbbf972a50991ca978b5416b89d76b6ab652a9d7315bc61b1baf23aacfdbd755
SSDEEP:	24576:+CjpXA4U35ozW03XRp/hESVE5uU2xbVN6pZVnoYLRZgUQs8n:rpTJxPNlcPVnoYLRZvz8n
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....@.....-.....+.w.....+.....*.....-.....&.....*.....(...../...../.7.....*.....+.....

File Icon

Icon Hash:	c8d8d8b6f0f83c58

Static PE Info

General

Entrypoint:	0x4e5eb3
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F64CF [Thu Nov 25 10:26:23 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	d69e4c13e25f0ad622344ac56118c0df

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1122a1	0x112400	False	0.505059964676	data	6.55728577412	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.ogtrfyj	0x114000	0x580a	0x5a00	False	0.466579861111	data	5.981573238	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x11a000	0x2b7b2	0x2b800	False	0.447607983118	data	5.81232244285	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x146000	0x77a4	0x2e00	False	0.252802309783	data	3.89020136245	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ogtrfyj	0x14e000	0x50	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14f000	0x2c550	0x2c600	False	0.68740096831	data	6.50827273455	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x17c000	0x8098	0x8200	False	0.705498798077	data	6.64096530369	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	China	
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
Nov 25, 2021 18:23:23.197443008 CET	192.168.2.7	8.8.8.8	0x1b0c	Standard query (0)	www.listincode.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:24.350204945 CET	192.168.2.7	8.8.8.8	0x2312	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:23:23.218777895 CET	8.8.8.8	192.168.2.7	0x1b0c	No error (0)	www.listincode.com		149.28.253.196	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:24.388041973 CET	8.8.8.8	192.168.2.7	0x2312	No error (0)	iplogger.org		5.9.162.45	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.listincode.com
- iplogger.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49736	149.28.253.196	443	C:\Users\user\Desktop\duLT5gkRjy.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 17:23:24 UTC	0	OUT	GET / HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36 Host: www.listincode.com Cache-Control: no-cache
2021-11-25 17:23:24 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 17:23:24 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 2 Connection: close X-Powered-By: PHP/5.6.40 Access-Control-Allow-Origin: *
2021-11-25 17:23:24 UTC	0	IN	Data Raw: 47 42 Data Ascii: GB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49737	5.9.162.45	443	C:\Users\user\Desktop\duLT5gkRjy.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-11-25 17:23:24 UTC	0	OUT	GET /1GWfv7 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36 Host: iplogger.org Cache-Control: no-cache
2021-11-25 17:23:24 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 17:23:24 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=84.17.52.63; expires=Wed, 18-Jul-2029 05:49:51 GMT; Max-Age=241187187; path=/ Set-Cookie: timezone=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/ Cache-Control: no-store, no-cache, must-revalidate Expires: Thu, 25 Nov 2021 17:23:24 +0000 Answers: whoami: dd7a5982e8b1de9b0cc7da7fe0ec7879c44089276a00308f59743c09424407f5 Strict-Transport-Security: max-age=31536000; preload X-Frame-Options: DENY
2021-11-25 17:23:24 UTC	1	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: duLT5gkRjy.exe PID: 5068 Parent PID: 5916

General

Start time:	18:23:21
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\duLT5gkRjy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\duLT5gkRjy.exe"
Imagebase:	0x1350000
File size:	1552896 bytes
MD5 hash:	D42456F7AFC812628A9FF67D8C9340EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Socelars, Description: Yara detected Socelars, Source: 00000001.00000002.266028618.000000000146A000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Socelars, Description: Yara detected Socelars, Source: 00000001.00000000.250943662.000000000146A000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Socelars, Description: Yara detected Socelars, Source: 00000001.00000000.244816151.000000000146A000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Socelars, Description: Yara detected Socelars, Source: 00000001.00000000.251852996.000000000146A000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

Analysis Process: WerFault.exe PID: 4060 Parent PID: 5068

General

Start time:	18:23:26
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5068 -s 1932
Imagebase:	0xad0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis