ID: 528695
Sample Name: EzCOXP6oxy
Cookbook: default.jbs
Time: 17:08:11
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

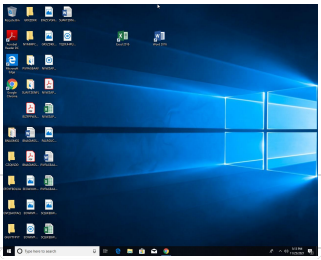
Windows Analysis Report EzCOXP6oxy

Overview

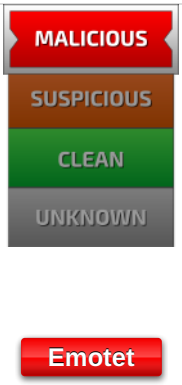
General Information

Sample Name:	EzCOXP6oxy (renamed file extension from none to dll)
Analysis ID:	528695
MD5:	0c32d4334246cc…
SHA1:	eec70a7ff5e0ed8..
SHA256:	c4e9dbb3e3b37e..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection



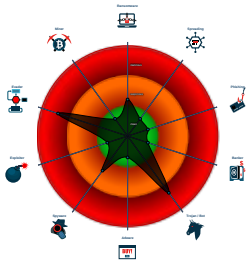
Emotet

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Sigma detected: Emotet RunDLL32 …
- Changes security center settings (no…
- Machine Learning detection for samp…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- svchost.exe (PID: 4596 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- loaddll32.exe (PID: 6828 cmdline: loaddll32.exe "C:\Users\user\Desktop\EzCOXP6oxy.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 5880 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\EzCOXP6oxy.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6656 cmdline: rundll32.exe "C:\Users\user\Desktop\EzCOXP6oxy.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6240 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\EzCOXP6oxy.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3996 cmdline: rundll32.exe C:\Users\user\Desktop\EzCOXP6oxy.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4036 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Nqaukzzzqxw\injbvoyze.mwd",xjdXnltVst MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 4820 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Nqaukzzzqxw\injbvoyze.mwd",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- SgrmBroker.exe (PID: 6812 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 3640 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 2528 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 1296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6032 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4776 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5880 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6888 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW"
  ],
  "C2 list": [
    "51.178.61.60:443",
    "168.197.250.14:80",
    "45.79.33.48:8080",
    "196.44.98.190:8080",
    "177.72.80.14:7080",
    "51.210.242.234:8080",
    "185.148.169.10:8080",
    "142.4.219.173:8080",
    "78.47.204.80:443",
    "78.46.73.125:443",
    "37.44.244.177:8080",
    "37.59.209.141:8080",
    "191.252.103.16:80",
    "54.38.242.185:443",
    "85.214.67.203:8080",
    "54.37.228.122:443",
    "207.148.81.119:8080",
    "195.77.239.39:8080",
    "66.42.57.149:443",
    "195.154.146.35:443"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.289870644.0000000004C20000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.810681340.0000000005590000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.810823822.00000000056B0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.807533185.0000000000EC0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.293225547.0000000004E00000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.rundll32.exe.56b0000.14.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.5440000.8.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.ba0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.4ba0000.4.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.4e00000.6.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 29 entries				

Sigma Overview

System Summary:

Sigma detected: Emotet RunDLL32 Process Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Emotet

System Summary:

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

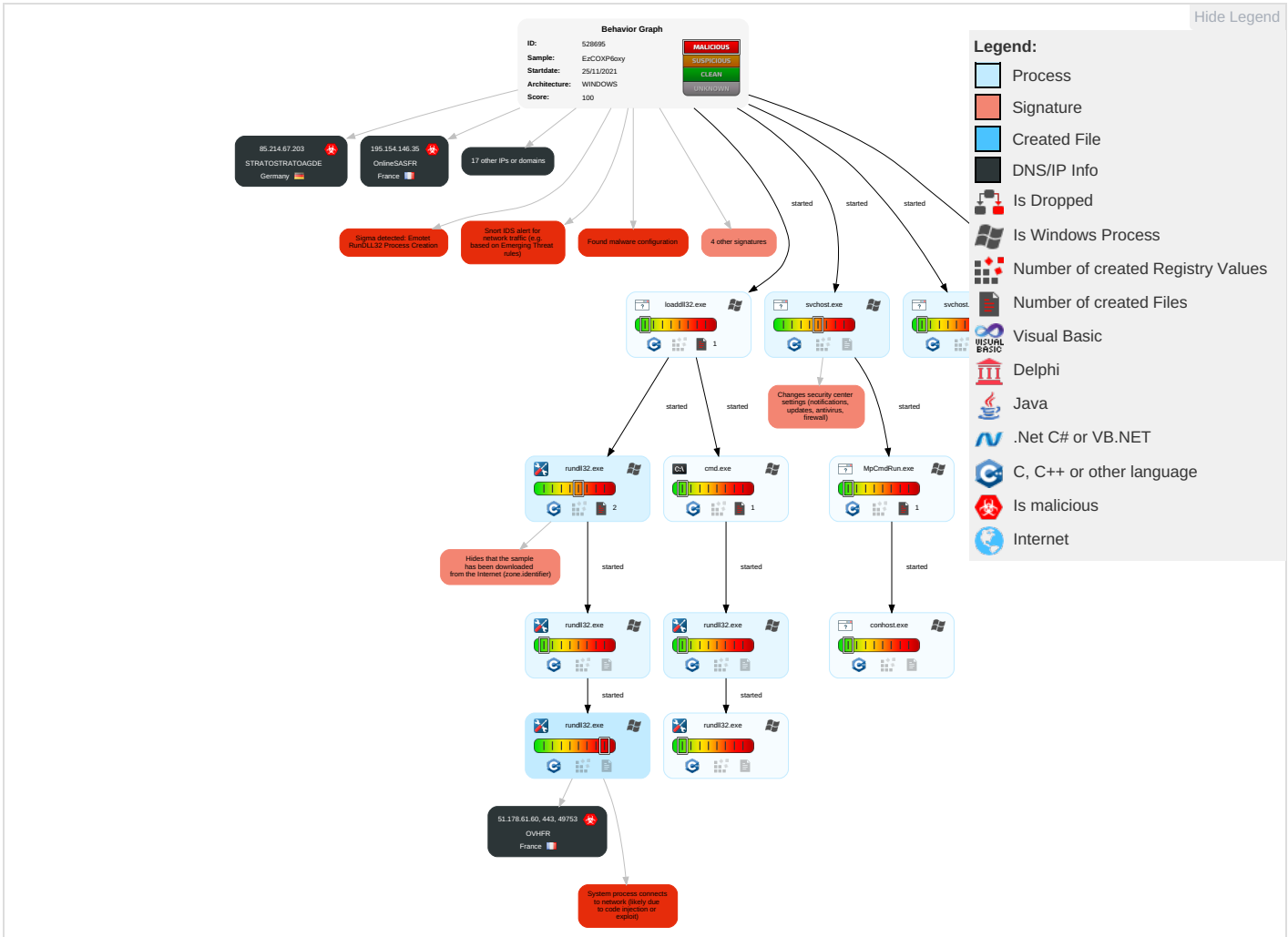
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 1 2	Masquerading 2	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eave Insec Netw Comr
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 4 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Explo Redir Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Explo Track Local

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	System Information Discovery 2 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

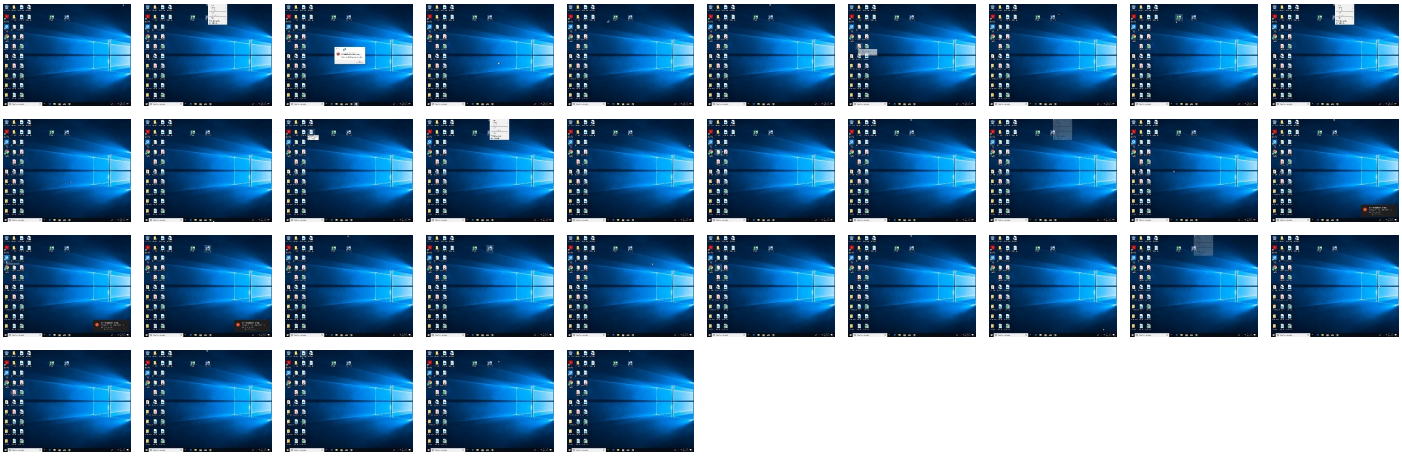
Behavior Graph



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
EzCOXP6oxy.dll	24%	Virustotal		Browse
EzCOXP6oxy.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.55c0000.13.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.56e0000.15.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4cd0000.5.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.5130000.5.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4e90000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.57f0000.17.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.5310000.7.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4550000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.bd0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.5470000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.54d0000.11.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4ff0000.11.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.10e0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4ae0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.4af0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4e30000.7.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.4c50000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://51.178.61.60/icsZGkxVGlJGXERpNMAkbBhZsRBvNu	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://51.178.61.60/icsZGkxVGlJGXERpNMAkbBhZsRBvNu	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.81.119	unknown	United States		20473	AS-CHOOPAUS	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
37.59.209.141	unknown	France		16276	OVHFR	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternet SABR	true
45.79.33.48	unknown	United States		63949	LINODE-APLinodeLLCUS	true
54.37.228.122	unknown	France		16276	OVHFR	true
185.148.169.10	unknown	Germany		44780	EVERSCALE-ASDE	true
142.4.219.173	unknown	Canada		16276	OVHFR	true
54.38.242.185	unknown	France		16276	OVHFR	true
195.154.146.35	unknown	France		12876	OnlineSASFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNET AR	true
51.178.61.60	unknown	France		16276	OVHFR	true
177.72.80.14	unknown	Brazil		262543	NewLifeFibraBR	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
51.210.242.234	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528695
Start date:	25.11.2021
Start time:	17:08:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EzCOXP6oxy (renamed file extension from none to dll)
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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@23/1@0/20
EGA Information:	Failed
HDC Information:	• Successful, ratio: 93% (good quality ratio 89.4%) • Quality average: 81.5% • Quality standard deviation: 25.6%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:09:54	API Interceptor	7x Sleep call for process: svchost.exe modified
17:10:07	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.148.81.119	C1Q17Dg4RT.dll	Get hash	malicious	Browse	
	MakbLShaqA.dll	Get hash	malicious	Browse	
	MakbLShaqA.dll	Get hash	malicious	Browse	
	tUJXpPwU27.dll	Get hash	malicious	Browse	
	pYebrdRKvR.dll	Get hash	malicious	Browse	
	pPX9DaPVYj.dll	Get hash	malicious	Browse	
	wUKXjICs5f.dll	Get hash	malicious	Browse	
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	
	qrb6jVwzoe.dll	Get hash	malicious	Browse	
	1711.doc	Get hash	malicious	Browse	
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	
	wNjqkrm8pH.dll	Get hash	malicious	Browse	
	5YO8hZg21O.dll	Get hash	malicious	Browse	
	dUGnMYeP1C.dll	Get hash	malicious	Browse	
	yFAXc9z51V.dll	Get hash	malicious	Browse	
	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FlyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
196.44.98.190	C1Q17Dg4RT.dll	Get hash	malicious	Browse	
	MakbLShaqA.dll	Get hash	malicious	Browse	
	MakbLShaqA.dll	Get hash	malicious	Browse	
	tUJXpPwU27.dll	Get hash	malicious	Browse	
	pYebrdRKvR.dll	Get hash	malicious	Browse	
	pPX9DaPVYj.dll	Get hash	malicious	Browse	
	wUKXjICs5f.dll	Get hash	malicious	Browse	
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	
	qrb6jVwzoe.dll	Get hash	malicious	Browse	
	1711.doc	Get hash	malicious	Browse	
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	
	wNjqkrm8pH.dll	Get hash	malicious	Browse	
	5YO8hZg21O.dll	Get hash	malicious	Browse	
	dUGnMYeP1C.dll	Get hash	malicious	Browse	
	yFAXc9z51V.dll	Get hash	malicious	Browse	
	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FlyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
78.46.73.125	C1Q17Dg4RT.dll	Get hash	malicious	Browse	
	MakbLShaqA.dll	Get hash	malicious	Browse	
	MakbLShaqA.dll	Get hash	malicious	Browse	
	tUJXpPwU27.dll	Get hash	malicious	Browse	
	pYebrdRKvR.dll	Get hash	malicious	Browse	
	pPX9DaPVYj.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	wUKXjICs5f.dll	Get hash	malicious	Browse	
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	
	qrb6jVwzoe.dll	Get hash	malicious	Browse	
	1711.doc	Get hash	malicious	Browse	
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	
	wNjqkrm8pH.dll	Get hash	malicious	Browse	
	5YO8hZg21O.dll	Get hash	malicious	Browse	
	dUGnMYeP1C.dll	Get hash	malicious	Browse	
	yFAXc9z51V.dll	Get hash	malicious	Browse	
	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FIyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	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
	piPvSLcFXV.exe	Get hash	malicious	Browse	• 88.99.210.172
	fkYZ7hyvnD.exe	Get hash	malicious	Browse	• 116.202.14.219
	.#U266bvmail-478314QOZVOYBY30.htm	Get hash	malicious	Browse	• 168.119.38.214
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 78.47.204.80
	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 78.47.204.80
AS-CHOOPAUS	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
	Jx35I5pwgd	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 66.42.57.149
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 66.42.57.149
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 66.42.57.149
	AWB_NO_9284730932.exe	Get hash	malicious	Browse	• 45.32.28.45
EcobandGH	C1Q17Dg4RT.dll	Get hash	malicious	Browse	• 196.44.98.190
	MakbLShaqA.dll	Get hash	malicious	Browse	• 196.44.98.190
	MakbLShaqA.dll	Get hash	malicious	Browse	• 196.44.98.190
	tUJXpPwU27.dll	Get hash	malicious	Browse	• 196.44.98.190
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 196.44.98.190
	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 196.44.98.190
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 196.44.98.190
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 196.44.98.190
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 196.44.98.190
	1711.doc	Get hash	malicious	Browse	• 196.44.98.190
	n6J7QJs4bk.dll	Get hash	malicious	Browse	• 196.44.109.73
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	• 196.44.98.190
	wNjqkrm8pH.dll	Get hash	malicious	Browse	• 196.44.98.190
	5YO8hZg21O.dll	Get hash	malicious	Browse	• 196.44.98.190
	dUGnMYeP1C.dll	Get hash	malicious	Browse	• 196.44.98.190
	yFAXc9z51V.dll	Get hash	malicious	Browse	• 196.44.98.190
	9fC0as7YLE.dll	Get hash	malicious	Browse	• 196.44.98.190
	FIyE6huzxV.dll	Get hash	malicious	Browse	• 196.44.98.190
	V0gZWRXv8d.dll	Get hash	malicious	Browse	• 196.44.98.190
	t5EuQW2GUF.dll	Get hash	malicious	Browse	• 196.44.98.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	C1Q17Dg4RT.dll	Get hash	malicious	Browse	• 51.178.61.60
	MakbLShaqA.dll	Get hash	malicious	Browse	• 51.178.61.60
	MakbLShaqA.dll	Get hash	malicious	Browse	• 51.178.61.60
	lhvzcskYLPyellowfacebrownietacohead.dll	Get hash	malicious	Browse	• 51.178.61.60
	vacehcp3Zv.dll	Get hash	malicious	Browse	• 51.178.61.60
	SecuriteInfo.com.Drixed-FJX5EDC20B587B4.1828.dll	Get hash	malicious	Browse	• 51.178.61.60
	SecuriteInfo.com.Suspicious.Win32.Save.a.20268.dll	Get hash	malicious	Browse	• 51.178.61.60
	PSVSotIVGj.dll	Get hash	malicious	Browse	• 51.178.61.60
	ivXBh7Nwmt.dll	Get hash	malicious	Browse	• 51.178.61.60
	34PZXoE0JJ.dll	Get hash	malicious	Browse	• 51.178.61.60
	jPzSCuyellowfacebrownietacohead.dll	Get hash	malicious	Browse	• 51.178.61.60
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 51.178.61.60
	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 51.178.61.60
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 51.178.61.60
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 51.178.61.60
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 51.178.61.60
	ReadMe[2021.11.22_12-15].vbs	Get hash	malicious	Browse	• 51.178.61.60
	cTplVWrqRR.dll	Get hash	malicious	Browse	• 51.178.61.60
	NErdgsNsKR.vbs	Get hash	malicious	Browse	• 51.178.61.60
	F.A.Q[2021.11.22_12-15].vbs	Get hash	malicious	Browse	• 51.178.61.60

Dropped Files

No context

Created / dropped Files

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe

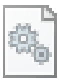
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.164856548166835
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3z9W+kw:j+s+v+b+P+m+0+Q+q+uW+kw
MD5:	3A0984010B462F7305085D71C9C31A20
SHA1:	DBBF15BBAC84EF3F70211EDB78135FBE8D3115D5
SHA-256:	67AFE58FA33A4D5AF793FB84CA55E9D3F896870EB7DA3005E791414602E54E61
SHA-512:	DD44B663C0E821F84E8DF91570875CC8A4696C59D3691CEEFFAB19B802783681415DC522E9A0A98C4CDA45318FF550FACAB430DAA75EF30EBD613241EC44A0B
Malicious:	false
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:. 4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7. 0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.907614584137073
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 94.34% • InstallShield setup (43055/19) 4.05% • Windows Screen Saver (13104/52) 1.23% • Generic Win/DOS Executable (2004/3) 0.19% • DOS Executable Generic (2002/1) 0.19%
File name:	EzCOXP6oxy.dll
File size:	668672
MD5:	0c32d4334246cc061e80fc9cf0780a58
SHA1:	eec70a7ff5e0ed8adb1bba38021dc2fdf0b1081d
SHA256:	c4e9dbb3e3b37e36574a8d963f3ba83d61beceedfb640e9 592b0a416396ca46e
SHA512:	9b43a99ea386c9203fe9269cc125c95be37a474058b997 794dc62913e1b7efdccba5c6c06d51e3daa943bb6369a4 3c7f30364966670a0f56eb75ddaf9fd126cc
SSDEEP:	12288:ZLqntrsKNni3jR34UrmTMQFQIBd+5UZF/imMG:Z2trTZwF34LTkpkom5
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......Je.....T...T...T)..T...T)..T...T...T%..T.VST...T.VET...T.VBT...T.VLT...T.VTT...T.VRT...T.VWT...TRich...T.......................

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1003ff7f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x619E9E08 [Wed Nov 24 20:18:16 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General

OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	cb788e621f390567a1ec94b8d2369e89

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5487c	0x54a00	False	0.557670559453	data	6.55778526171	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x56000	0x15e5e	0x16000	False	0.312466708097	data	5.09346151604	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6c000	0x2a394	0x26800	False	0.943314985795	data	7.9074320255	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x97000	0x7160	0x7200	False	0.260450932018	data	3.9170647287	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9f000	0xab2e	0xac00	False	0.364280523256	data	5.0366284188	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

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
11/25/21-17:09:18.160157	TCP	2404336	ET CNC Feodo Tracker Reported CnC Server TCP group 19	49753	443	192.168.2.3	51.178.61.60

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 51.178.61.60

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49753	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 16:09:18 UTC	0	OUT	GET /icsZGkxVGlJGXERpNMAkbBhZsRBvNu HTTP/1.1 Cookie: VzjNaqMqfocdBX=JqOFPJj7PozLdKilb0Q3hTC9S0ITJTlgaaPM+YcmQ+fGgQl2sU3kSVveu+UxKl7l5E+Vn1v6pOOBNhr6RStkjXoxolELe8X2rLolboD84KIbkDlniHtSL4LHWkLSPni84AFgz3zocxEbBvWcJ4AIekqVpd4PNQbkLSdE6RHCposw2iNPMgXzABlR4bdx4TfSbUboMCHHuhHdRCg++6AooUBOAMfdms1jbZdvw1sJsdZ86jaS+IXQjmI/Fz4GX2r0Zs0TBoVdanVa0yqw Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache
2021-11-25 16:09:19 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 16:09:19 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-11-25 16:09:19 UTC	0	IN	Data Raw: 33 34 31 0d 0a ee 6f c5 06 87 59 74 05 7c 6e c9 65 93 59 ab 70 dd a9 ca 63 16 27 a3 02 b8 71 37 d1 1c ae 34 1a 1f a9 57 b4 e6 44 4f 99 b7 bc a6 48 70 a2 66 2d 59 59 52 58 d5 0e d6 00 f3 01 6b d8 4b 01 e8 20 c0 70 a3 a3 a5 77 b0 d2 30 d7 b9 b9 fb a9 2a ab 7f 0c 09 73 81 58 95 fb c5 c1 bc 86 8f 50 f3 af d7 7d ca 6e 23 e1 85 25 31 f5 de 9e c3 b1 00 bd 31 be f8 97 c2 5c ad 30 6f 3c a9 9e aa c7 3d a6 c5 dd 7d b3 cc 06 a3 92 81 c0 2f 4e 35 ee 2e 1b bf a9 c3 59 1d 52 be 22 e1 d4 ed ca a7 3d 21 d2 fd 55 0b 23 18 5a 92 b0 85 d9 6b 9d 29 81 53 20 77 b4 1c 28 22 8a 45 d6 88 11 5b bc 02 30 69 16 f3 23 af d6 1c 12 8d cd fc 2a c3 81 14 71 95 56 08 69 e8 64 89 77 b2 38 b4 1f 0a 63 c0 10 03 d3 2b d4 fb c3 a6 fb d8 74 85 ab 32 d6 8c 1e a5 0c 78 9c 6d 3f 41 cb eb be 81 74 Data Ascii: 341oYt|neYpc'q74WDOHpf-YYRXkK pw0*sXP}n#%11\0o<=}/N5.YR"=!U#Zk)S w("E[0i#*qVidw8c+t2xm?At

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: svchost.exe PID: 4596 Parent PID: 572

General

Start time:	17:09:05
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: loaddll32.exe PID: 6828 Parent PID: 4880

General

Start time:	17:09:05
Start date:	25/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\EzCOXP6oxy.dll"
Imagebase:	0xf80000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: SgrmBroker.exe PID: 6812 Parent PID: 572

General

Start time:	17:09:05
Start date:	25/11/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff66e040000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5880 Parent PID: 6828

General

Start time:	17:09:06
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\EzCOXP6oxy.dll",#1
Imagebase:	0xd80000
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: svchost.exe PID: 3640 Parent PID: 572

General

Start time:	17:09:06
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 3996 Parent PID: 6828

General

Start time:	17:09:06
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\EzCOXP6oxy.dll,Control_RunDLL
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.293225547.0000000004E00000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.293389274.0000000004FC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.293071133.0000000004BA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.291762953.0000000000CB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.292938916.0000000004AB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.293307621.0000000004E60000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6656 Parent PID: 5880

General

Start time:	17:09:06
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\EzCOXP6oxy.dll",#1
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.289870644.0000000004C20000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6240 Parent PID: 6656

General

Start time:	17:09:07
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\EzCOXP6oxy.dll",Control_RunDLL
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 4036 Parent PID: 3996

General

Start time:	17:09:07
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Nqaukzzzqxw\injbvoyze.mwd",xjdXnltVst
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.293302673.0000000000BA0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4820 Parent PID: 4036

General

Start time:	17:09:08
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Nqaukzzzqxw\injbvoyze.mwd" ,Control_RunDLL
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.810681340.0000000005590000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.810823822.00000000056B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.807533185.0000000000EC0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.810439352.0000000005440000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.810235719.00000000051E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.810948594.00000000057C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.809655568.0000000004AC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.810054913.0000000005100000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.810559507.00000000054A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6032 Parent PID: 572

General

Start time:	17:09:13
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 4776 Parent PID: 572

General

Start time:	17:09:29
Start date:	25/11/2021

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5880 Parent PID: 572

General

Start time:	17:09:43
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6888 Parent PID: 572

General

Start time:	17:09:52
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: MpCmdRun.exe PID: 2528 Parent PID: 3640

General

Start time:	17:10:07
Start date:	25/11/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff6c9780000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 1296 Parent PID: 2528

General

Start time:	17:10:07
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis