ID: 531996
Sample Name:
spZRMihlrkFGqYq1f.dll
Cookbook: default.jbs
Time: 16:10:38
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

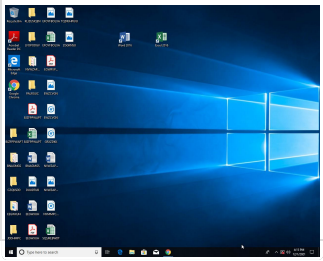
Windows Analysis Report spZRMihlrkFGqYq1f.dll

Overview

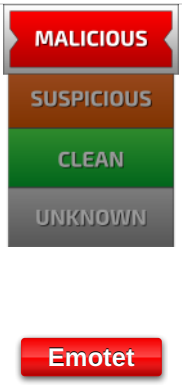
General Information

Sample Name:	spZRMihlrkFGqYq1f.dll
Analysis ID:	531996
MD5:	9f4fa905fd685d2…
SHA1:	e186e0869276d3..
SHA256:	808e8247efd685b.
Infos:	

Most interesting Screenshot:



Detection

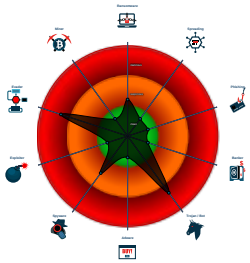


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 …
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query locale…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6816 cmdline: loaddll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6796 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6860 cmdline: rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6880 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6792 cmdline: rundll32.exe C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4928 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Feetevsox\qeijjyafbaho.gis",ayowadvg MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 3476 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Feetevsox\qeijjyafbaho.gis",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 6836 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4864 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6940 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6904 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "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"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.1231555705.0000000003380000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.715083656.00000000042D1000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.1232688117.0000000005A90000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.1232050333.0000000004ED1000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.712245563.00000000046E0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rundll32.exe.5880000.10.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.56b0000.6.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.4910000.9.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.3f80000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.59a0000.13.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 46 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

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)

Stealing of Sensitive Information:

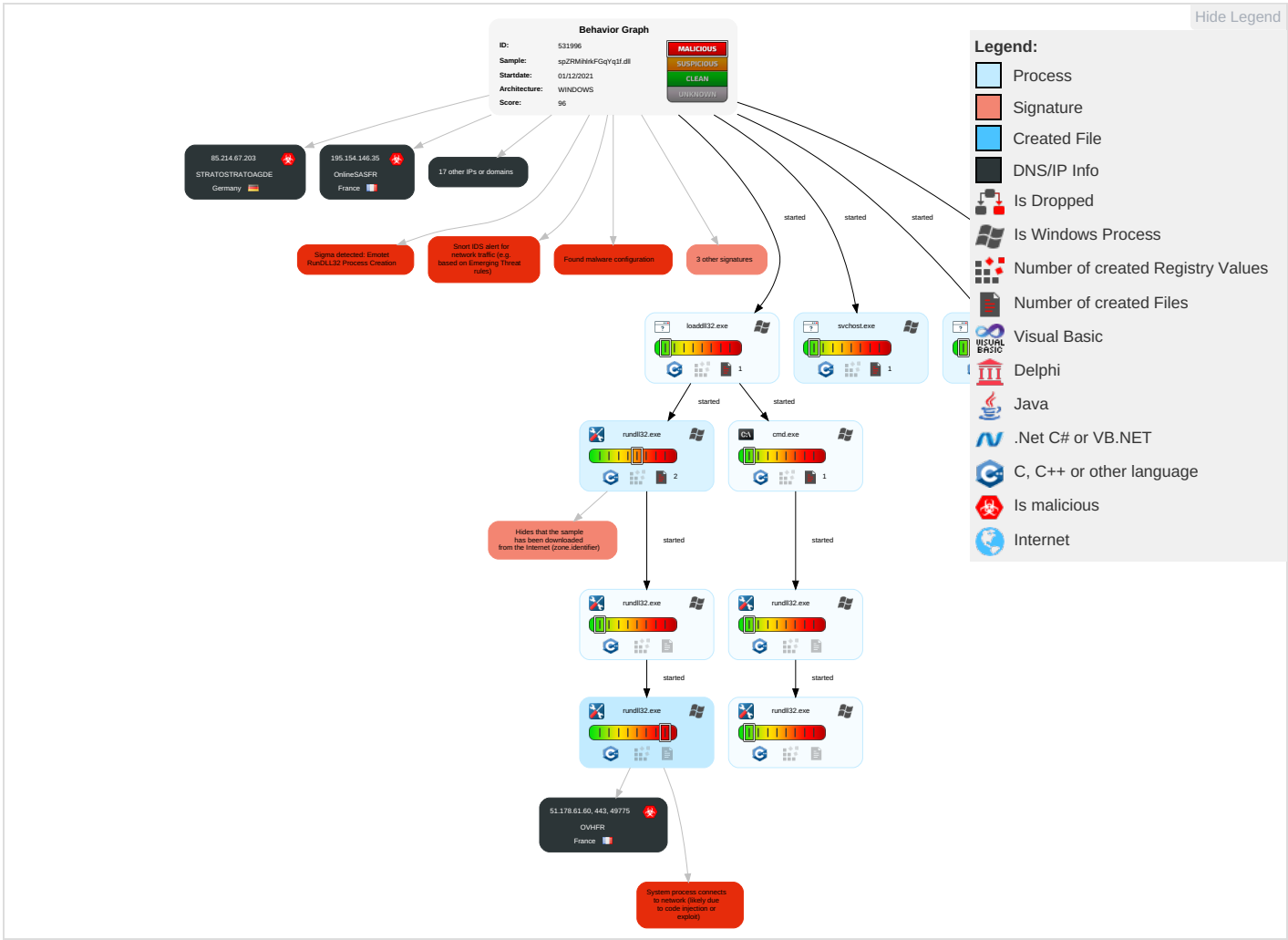
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 1 1 2	Masquerading 2	Input Capture 2	System Time Discovery 2	Remote Services	Input Capture 2	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Security Software Discovery 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Virtualization/Sandbox Evasion 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Application Window 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	Rundll32 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 2 7	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statior

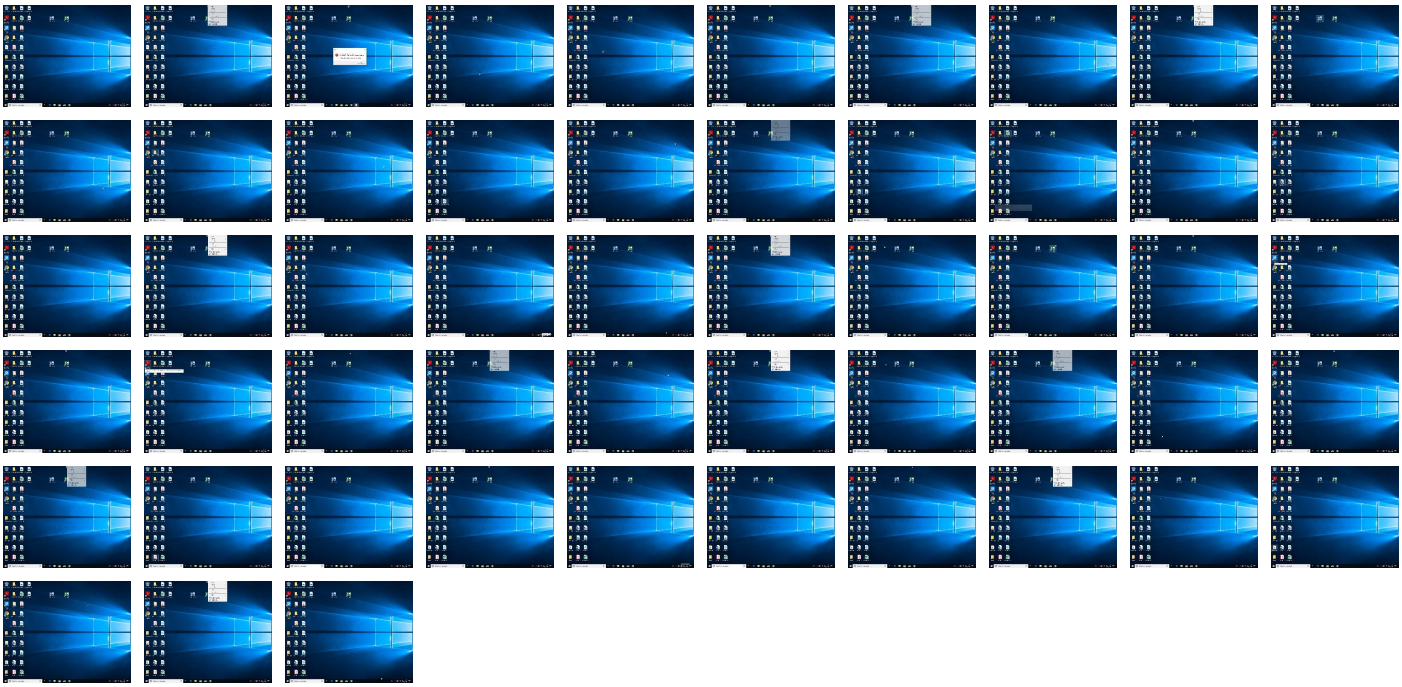
Behavior Graph



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
spZRMihlrkFGqYq1f.dll	43%	Metadefender		Browse
spZRMihlrkFGqYq1f.dll	57%	ReversingLabs	Win32.Trojan.Mansabo	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.4710000.5.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.3fc0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.34d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.58b0000.11.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.4a70000.11.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.59a0000.13.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.4910000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.5bd0000.17.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.56e0000.7.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.42d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4ed0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.4630000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.5840000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.48b0000.7.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.5600000.5.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.30d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.5ac0000.15.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://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://51.178.61.60/ZKzoaCRaSGPOqJVHjhZJzdCfaeZvESlfQfwHxNYMOhGmjZbKSRXfZNvJ	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	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/ZKzoaCRaSGPOqJVHjhZJzdCfaeZvESlfQfwHxNYMOhGmjZbKSRXfZNvJ	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:	531996
Start date:	01.12.2021
Start time:	16:10:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	spZRMihlrkFGqYq1f.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:	19
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:	mal96.troj.evad.winDLL@17/0@0/20
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 99.3% (good quality ratio 91.2%) • Quality average: 75.6% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:12:45	API Interceptor	7x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.148.81.119	gvtdsqavfej.dll	Get hash	malicious	Browse	
	mhOX6jll6x.dll	Get hash	malicious	Browse	
	dguQYT8p8j.dll	Get hash	malicious	Browse	
	jSxIzXfwc7.dll	Get hash	malicious	Browse	
	mhOX6jll6x.dll	Get hash	malicious	Browse	
	X2XCewI2Yy.dll	Get hash	malicious	Browse	
	dguQYT8p8j.dll	Get hash	malicious	Browse	
	HMvjzUYq2h.dll	Get hash	malicious	Browse	
	s9BZBDWmi4.dll	Get hash	malicious	Browse	
	bFx5bZRC6P.dll	Get hash	malicious	Browse	
	c7IUEh66u6.dll	Get hash	malicious	Browse	
	HMvjzUYq2h.dll	Get hash	malicious	Browse	
	s9BZBDWmi4.dll	Get hash	malicious	Browse	
	bFx5bZRC6P.dll	Get hash	malicious	Browse	
	WfCt2B042X.dll	Get hash	malicious	Browse	
	ZKVYER7XcT.dll	Get hash	malicious	Browse	
	2cq85E4EeM.dll	Get hash	malicious	Browse	
	WfCt2B042X.dll	Get hash	malicious	Browse	
	ZKVYER7XcT.dll	Get hash	malicious	Browse	
	6PPJENHoVW.dll	Get hash	malicious	Browse	
196.44.98.190	gvtdsqavfej.dll	Get hash	malicious	Browse	
	mhOX6jll6x.dll	Get hash	malicious	Browse	
	dguQYT8p8j.dll	Get hash	malicious	Browse	
	jSxIzXfwc7.dll	Get hash	malicious	Browse	
	mhOX6jll6x.dll	Get hash	malicious	Browse	
	X2XCewI2Yy.dll	Get hash	malicious	Browse	
	dguQYT8p8j.dll	Get hash	malicious	Browse	
	HMvjzUYq2h.dll	Get hash	malicious	Browse	
	s9BZBDWmi4.dll	Get hash	malicious	Browse	
	bFx5bZRC6P.dll	Get hash	malicious	Browse	
	c7IUEh66u6.dll	Get hash	malicious	Browse	
	HMvjzUYq2h.dll	Get hash	malicious	Browse	
	s9BZBDWmi4.dll	Get hash	malicious	Browse	
	bFx5bZRC6P.dll	Get hash	malicious	Browse	
	WfCt2B042X.dll	Get hash	malicious	Browse	
	ZKVYER7XcT.dll	Get hash	malicious	Browse	
	2cq85E4EeM.dll	Get hash	malicious	Browse	
	WfCt2B042X.dll	Get hash	malicious	Browse	
	ZKVYER7XcT.dll	Get hash	malicious	Browse	
	6PPJENHoVW.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	iU17wh2uUd.exe	Get hash	malicious	Browse	• 149.28.253.196
	iU17wh2uUd.exe	Get hash	malicious	Browse	• 149.28.253.196
	Sz4lxTmH7r.exe	Get hash	malicious	Browse	• 149.28.253.196
	7AF33E5528AB8A8F45EE7B8C4DD24B4014FEAA6E1D310.exe	Get hash	malicious	Browse	• 149.28.253.196
	RFIlSRQKzj.exe	Get hash	malicious	Browse	• 45.32.115.235
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 149.28.253.196
	991D4DC612FF80AB2506510DBA31531DB995FE3F64318.exe	Get hash	malicious	Browse	• 149.28.253.196
	MMUc2aeWxZ.exe	Get hash	malicious	Browse	• 149.28.253.196
	0pvsj0MF1D.exe	Get hash	malicious	Browse	• 149.28.253.196
	Linux_amd64	Get hash	malicious	Browse	• 45.32.162.141
	nkXzJnW7AH.exe	Get hash	malicious	Browse	• 149.28.253.196
	67MPsax8fd.exe	Get hash	malicious	Browse	• 136.244.117.138
	Linux_x86	Get hash	malicious	Browse	• 45.77.44.252
	uI6mJo4TJQ.exe	Get hash	malicious	Browse	• 149.28.253.196
	uI6mJo4TJQ.exe	Get hash	malicious	Browse	• 149.28.253.196
	M2jG6lMe7Y.exe	Get hash	malicious	Browse	• 202.182.120.6
	7LPqKhiPCL.exe	Get hash	malicious	Browse	• 139.180.133.9
	wvYbWkOPqJ.exe	Get hash	malicious	Browse	• 149.28.253.196
	wvYbWkOPqJ.exe	Get hash	malicious	Browse	• 149.28.253.196
	7OoLG7JkFC	Get hash	malicious	Browse	• 44.40.164.168
EcobandGH	gvtdsqavfej.dll	Get hash	malicious	Browse	• 196.44.98.190
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 196.44.98.190
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 196.44.98.190
	jSxIzXfwc7.dll	Get hash	malicious	Browse	• 196.44.98.190
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 196.44.98.190
	X2XCewI2Yy.dll	Get hash	malicious	Browse	• 196.44.98.190
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 196.44.98.190
	HMvjzUYq2h.dll	Get hash	malicious	Browse	• 196.44.98.190
	s9BZBDWmi4.dll	Get hash	malicious	Browse	• 196.44.98.190
	bFx5bZRC6P.dll	Get hash	malicious	Browse	• 196.44.98.190
	c7IUEh66u6.dll	Get hash	malicious	Browse	• 196.44.98.190
	HMvjzUYq2h.dll	Get hash	malicious	Browse	• 196.44.98.190
	s9BZBDWmi4.dll	Get hash	malicious	Browse	• 196.44.98.190
	bFx5bZRC6P.dll	Get hash	malicious	Browse	• 196.44.98.190
	WfCt2B042X.dll	Get hash	malicious	Browse	• 196.44.98.190
	ZKVYER7XcT.dll	Get hash	malicious	Browse	• 196.44.98.190
	2cq85E4EeM.dll	Get hash	malicious	Browse	• 196.44.98.190
	WfCt2B042X.dll	Get hash	malicious	Browse	• 196.44.98.190
	ZKVYER7XcT.dll	Get hash	malicious	Browse	• 196.44.98.190
	6PPJENHoVW.dll	Get hash	malicious	Browse	• 196.44.98.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	fehiVK2JSx.dll	Get hash	malicious	Browse	• 51.178.61.60
	kQ9HU0gKVH.exe	Get hash	malicious	Browse	• 51.178.61.60
	gvtdsqavfej.dll	Get hash	malicious	Browse	• 51.178.61.60
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 51.178.61.60
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 51.178.61.60
	jSxIzXfwc7.dll	Get hash	malicious	Browse	• 51.178.61.60
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 51.178.61.60
	X2XCewI2Yy.dll	Get hash	malicious	Browse	• 51.178.61.60
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 51.178.61.60
	date1%3fBNLv65=pAAS.dll	Get hash	malicious	Browse	• 51.178.61.60
	HMvjzUYq2h.dll	Get hash	malicious	Browse	• 51.178.61.60
	s9BZBDWmi4.dll	Get hash	malicious	Browse	• 51.178.61.60
	bFx5bZRC6P.dll	Get hash	malicious	Browse	• 51.178.61.60
	c7IUEh66u6.dll	Get hash	malicious	Browse	• 51.178.61.60
	HMvjzUYq2h.dll	Get hash	malicious	Browse	• 51.178.61.60

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	s9BZBDWmi4.dll	Get hash	malicious	Browse	• 51.178.61.60
	bFx5bZRC6P.dll	Get hash	malicious	Browse	• 51.178.61.60
	WfCt2B042X.dll	Get hash	malicious	Browse	• 51.178.61.60
	ZKVYER7XcT.dll	Get hash	malicious	Browse	• 51.178.61.60
	2cq85E4EeM.dll	Get hash	malicious	Browse	• 51.178.61.60

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.7859159976425
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 95.51% • InstallShield setup (43055/19) 4.10% • Generic Win/DOS Executable (2004/3) 0.19% • DOS Executable Generic (2002/1) 0.19% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	spZRMihlrkFGqYq1f.dll
File size:	712704
MD5:	9f4fa905fd685d28c4ff28f24ad224a1
SHA1:	e186e0869276d3af6465d7c754b22527c7ac2ced
SHA256:	808e8247efd685bdbae3ea0e55de1e8ed8aecd1359a213b0c6291b73f007fdaf
SHA512:	d8c33eb38fe54e40d463f20b6091c88863f0fadc70382ad826d7c33e61d696af614e9ba8c73f84d4e13fb141289d5bd978451a5565f61e869a054a837fdef5e0
SSDEEP:	12288:WKEUkuAOLka1miSmuYr1V7nAobS3qTHPR101D:TEQLka1nBVDAoS3WvR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.V.8...8...8..I7...8..I7...8...8...:.....8.....8.....48.....8.....8.....8.....8..Rich.8.....PE..L...(..a...

File Icon

Icon Hash:	be71f1aca0b8c0c4

Static PE Info

General

Entrypoint:	0x1003d301
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x61A0C528 [Fri Nov 26 11:29:44 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General

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:	d8c52655a835ecb2c6fea489c7c7674b

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x566b7	0x57000	False	0.574984846444	data	6.6363911364	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x58000	0x188de	0x19000	False	0.30236328125	data	4.88012998463	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x71000	0x2a254	0x27000	False	0.931434044471	data	7.84888321435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x9af8	0xa000	False	0.241723632813	data	3.85640321845	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa6000	0xbd48	0xc000	False	0.347106933594	data	4.87718770475	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
12/01/21-16:12:03.931139	TCP	2404336	ET CNC Feodo Tracker Reported CnC Server TCP group 19	49775	443	192.168.2.4	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	192.168.2.4	49775	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-01 15:12:04 UTC	0	OUT	GET /ZKzoaCRaSGPOqJVHjhZJzdCfaeZvESlfQfwHxNYMOhGmjZbKSRXfZNvJ HTTP/1.1 Cookie: BbabBTNqIR=qrh4znIW0vRoZUgVJJVgzfQvY9C+RpRussFCR/fGFdtMBlPVybXrZsLF92dUNSOaN7UtApP RkIXlq1+7rNMFKl/GD+kwN0+UKJ1vSTU/v1LmGzXvNL9Y6Ncf4sehP3YL6oaRsTpSuU6YzoarwBbK29kvoAsGOYRv6 Xj3viHnIeOCY6VwhklOKsvWD+GGQWp/+KzcLqZXdf6vX1pw51ydx7BZAIYsZ4oO5HPx+C0OX/W7prasTQF+SxpB+l8 kw9kHpKuLSE3MN5eruU/U1ZyDN8wwOUnkB9ePec54mFaBjmfD1QEzkF2yYIRzHwr7O5Mz0xHblcofjcNex7IClSGUV tOK3elw Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache
2021-12-01 15:12:05 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 01 Dec 2021 15:12:05 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-12-01 15:12:05 UTC	0	IN	Data Raw: 33 30 31 0d 0a 20 9b c5 28 57 37 9f 3b 96 c5 45 95 6a a2 15 b8 f4 41 76 33 3b ae 0c 15 49 0c 36 5e b0 1c a1 f1 ce c4 2c 55 d6 d6 fc 1c 98 3c 7e 88 82 5f 6c 2f 4e e2 0f 21 bc e0 f2 81 2a fb 54 ba cc bf 3f fc 78 46 1b 08 69 e2 c9 45 ab 80 93 45 3a b1 42 b0 fc e3 4e d5 c5 bf ab aa a3 1a d4 4c 37 2b d5 91 d5 66 47 03 03 c8 e7 99 d1 79 ba 02 78 00 80 d4 41 66 62 7c e6 70 bd 5a 59 53 09 03 8c 61 da bc e5 49 9b 2e 3c e7 d1 da 37 14 bd 10 da 06 40 80 f1 bb 3a c8 df bd de 88 04 fe 52 5b 0f 7b b3 06 81 84 b9 3d fe 81 b3 67 8a 1a 85 d6 95 9c 9d 82 a0 e1 92 a6 3d f4 20 6e 13 cc 5e ef d7 83 b6 fd 9a 50 74 28 1e 96 17 e7 ac 6f 22 2f c0 1c f0 93 f3 a9 16 9f ec 0c 20 7a 49 68 f1 19 c7 59 c3 a4 f5 cf 06 c8 55 0c 84 b7 3a ce 7b f4 a7 73 e2 8b ce df b1 6f a7 82 10 0a 01 64 Data Ascii: 301 (W7;EjAv3;l6^,U<~_l/N!*T?xFiEE:BNL7+fGyxAfb|pZYSaI.<7@:R[{=g= n^Pt(o"/ zIhYU:{sod

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6816 Parent PID: 5704

General

Start time:	16:11:53
Start date:	01/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll"
Imagebase:	0xd30000
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: cmd.exe PID: 6796 Parent PID: 6816

General

Start time:	16:11:53
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",#1
Imagebase:	0x11d0000
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: 6836 Parent PID: 568

General

Start time:	16:11:54
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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: rundll32.exe PID: 6792 Parent PID: 6816

General

Start time:	16:11:54
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll,Control_RunDLL
Imagebase:	0x10000
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: 00000003.00000002.712245563.00000000046E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.712289758.0000000004711000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.712514212.00000000048B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.712664698.0000000004911000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.712162779.0000000004631000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.712727948.0000000004A40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.711795712.0000000004040000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.711701070.0000000003FC1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.712440145.0000000004880000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.712583531.00000000048E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.712769808.0000000004A71000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.711647577.0000000003F80000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6860 Parent PID: 6796

General

Start time:	16:11:54
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",#1
Imagebase:	0x10000
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: 00000004.00000002.710421091.00000000030D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.710385050.00000000030A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6880 Parent PID: 6860

General

Start time:	16:11:54
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",Control_RunDLL
Imagebase:	0x10000
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: 4928 Parent PID: 6792

General

Start time:	16:11:55
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Feetevsox\qeijjyafbaho.gis",ayowadvg
Imagebase:	0x10000
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: 00000006.00000002.715083656.00000000042D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.714978387.00000000041A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 3476 Parent PID: 4928

General

Start time:	16:11:56
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Feetevsox\qeijjyafbaho.gis",Control_RunDLL
Imagebase:	0x10000
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: 00000007.00000002.1231555705.0000000003380000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232688117.0000000005A90000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232050333.0000000004ED1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232447127.0000000005810000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232307431.0000000005601000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1231756136.00000000034D1000.00000020.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232722292.0000000005AC1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232778778.0000000005BA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232026757.0000000004EA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232814811.0000000005BD1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232471736.0000000005841000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232588764.0000000005970000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232613063.00000000059A1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232537029.00000000058B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232513916.0000000005880000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232107048.0000000004F80000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232396043.00000000056E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1232361987.00000000056B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 4864 Parent PID: 568

General

Start time:	16:12:16
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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: 6940 Parent PID: 568

General

Start time:	16:12:32
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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: 6904 Parent PID: 568

General

Start time:	16:12:43
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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

Disassembly

Code Analysis