ID: 524862
Sample Name: wNjqkrm8pH
Cookbook: default.jbs
Time: 01:03:13
Date: 19/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

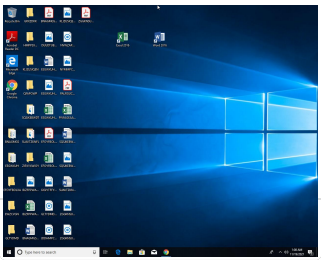
Windows Analysis Report wNjqkrm8pH

Overview

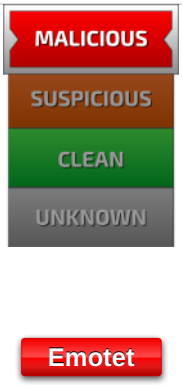
General Information

Sample Name:	wNjqkrm8pH (renamed file extension from none to dll)
Analysis ID:	524862
MD5:	699b39c805f6a36.
SHA1:	04489a4c9d50b6..
SHA256:	142d330305cf2bb.
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

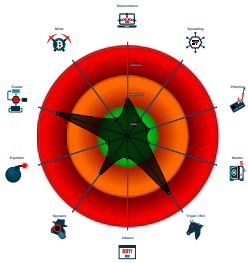


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 …
- Tries to detect virtualization through…
- 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…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6164 cmdline: loaddll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 2804 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5940 cmdline: rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 2944 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6280 cmdline: rundll32.exe C:\Users\user\Desktop\wNjqkrm8pH.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 672 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Hsngzdtsiohsyp\jlodhhplzusb.iie",cwqsUWjgRvl MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 6388 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Hsngzdtsiohsyp\jlodhhplzusb.iie",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6416 cmdline: rundll32.exe C:\Users\user\Desktop\wNjqkrm8pH.dll,abziuleoxsborpb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6828 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6420 cmdline: rundll32.exe C:\Users\user\Desktop\wNjqkrm8pH.dll,aejkroaebsbxdnkhb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 1304 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6848 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 5932 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5416 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2276 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2236 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "Public Key": [
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW",
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0"
  ],
  "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
00000003.00000002.352402052.000000000344A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000002.415487729.000000000117D000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.413760673.0000000000D1A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.426884632.000000000328A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.415304095.00000000032EA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.3304250.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.d341f8.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.3464320.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.d341f8.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.32a6388.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 5 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)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

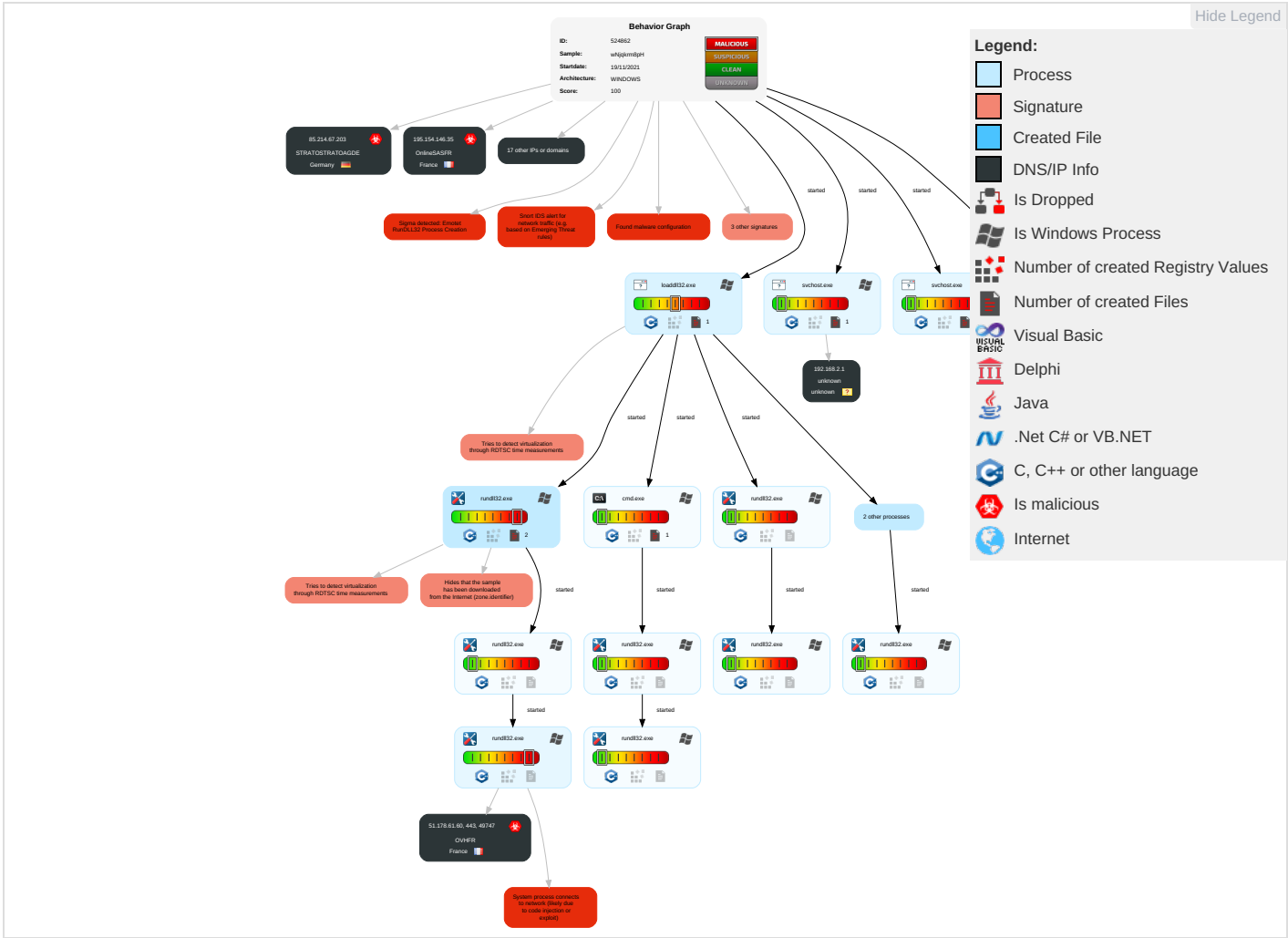
Yara detected Emotet

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	Windows Management Instrumentation	Application Shimming 1	Process Injection 1 1 2	Masquerading 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdr Insecure Network Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Application Shimming 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1 3 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit S Track D 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)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	System Information Discovery 1 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protocol

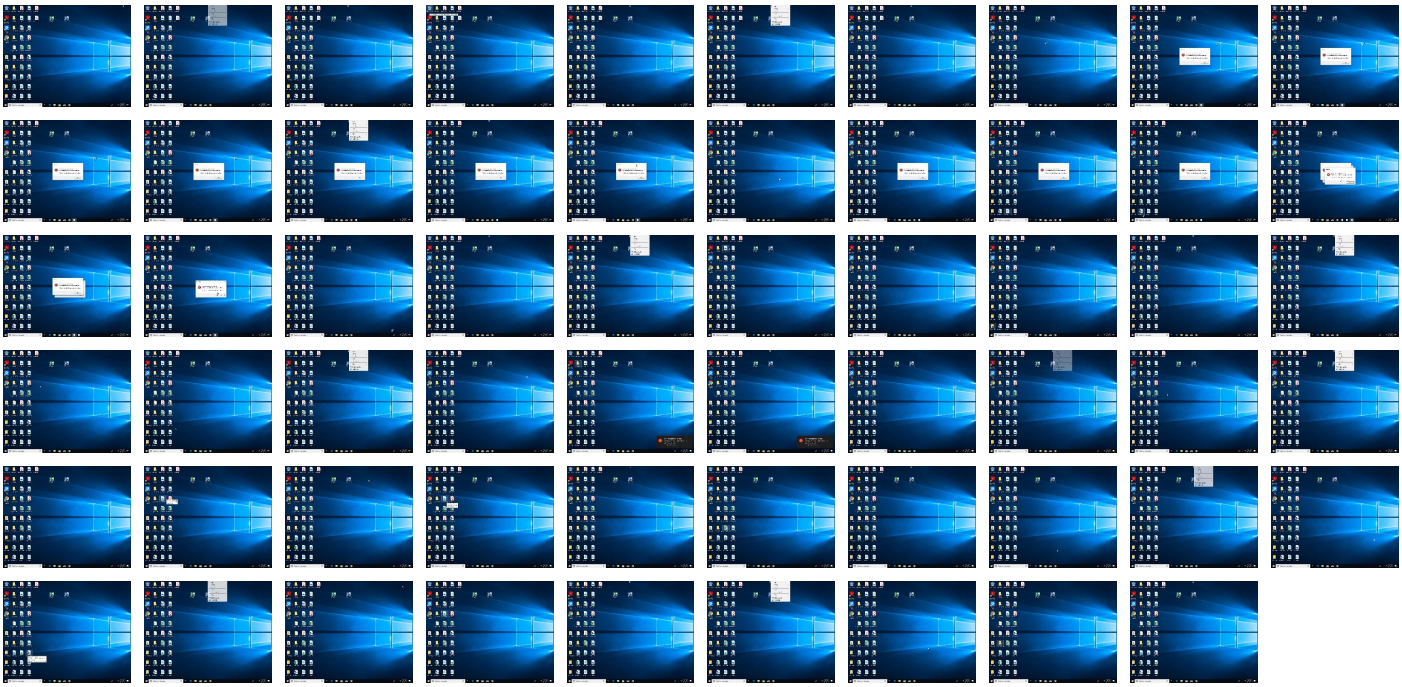
Behavior Graph



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
wNjqkrm8pH.dll	24%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.1040000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.cf0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.b20000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.ea0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.e45298.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.3230000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.1030000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.3230000.0.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.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	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

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	524862
Start date:	19.11.2021
Start time:	01:03:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wNjqkrm8pH (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:	27
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@27/0@0/21
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.6% (good quality ratio 16%) • Quality average: 69.9% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 86% • 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
01:06:37	API Interceptor	8x 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	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	
	8rryPzJR1p.dll	Get hash	malicious	Browse	
	a65FgjVus4.dll	Get hash	malicious	Browse	
	bWjYh6H8wk.dll	Get hash	malicious	Browse	
	ZJOHKItBoJ.dll	Get hash	malicious	Browse	
	eyPPiz3W6u.dll	Get hash	malicious	Browse	
	HjYSwxqyUn.dll	Get hash	malicious	Browse	
	f47YPsvRI3.dll	Get hash	malicious	Browse	
	2n64VXT08V.dll	Get hash	malicious	Browse	
	qUr4bXsweR.dll	Get hash	malicious	Browse	
	52O6evfqQT.dll	Get hash	malicious	Browse	
	ONEitXKvz6.dll	Get hash	malicious	Browse	
	1w9i8K6AzWV5RmHTSn8.dll	Get hash	malicious	Browse	
196.44.98.190	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	
	8rryPzJR1p.dll	Get hash	malicious	Browse	
	a65FgjVus4.dll	Get hash	malicious	Browse	
	bWjYh6H8wk.dll	Get hash	malicious	Browse	
	ZJOHKItBoJ.dll	Get hash	malicious	Browse	
	eyPPiz3W6u.dll	Get hash	malicious	Browse	
	HjYSwxqyUn.dll	Get hash	malicious	Browse	
	f47YPsvRI3.dll	Get hash	malicious	Browse	
	2n64VXT08V.dll	Get hash	malicious	Browse	
	qUr4bXsweR.dll	Get hash	malicious	Browse	
	52O6evfqQT.dll	Get hash	malicious	Browse	
	ONEitXKvz6.dll	Get hash	malicious	Browse	
	1w9i8K6AzWV5RmHTSn8.dll	Get hash	malicious	Browse	
78.46.73.125	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	
	8rryPzJR1p.dll	Get hash	malicious	Browse	
	a65FgjVus4.dll	Get hash	malicious	Browse	
	bWjYh6H8wk.dll	Get hash	malicious	Browse	
	ZJOHKItBoJ.dll	Get hash	malicious	Browse	
	eyPPiz3W6u.dll	Get hash	malicious	Browse	
	HjYSwxqyUn.dll	Get hash	malicious	Browse	
	f47YPsvRI3.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2n64VXT08V.dll	Get hash	malicious	Browse	
	qUr4bXsweR.dll	Get hash	malicious	Browse	
	52O6evfqQT.dll	Get hash	malicious	Browse	
	ONEitXKvz6.dll	Get hash	malicious	Browse	
	1w9i8K6AzWV5RmHTSn8.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	5YO8hZg21O.dll	Get hash	malicious	Browse	• 78.47.204.80
	dUGnMYeP1C.dll	Get hash	malicious	Browse	• 78.47.204.80
	yFAXc9z51V.dll	Get hash	malicious	Browse	• 78.47.204.80
	9fC0as7YLE.dll	Get hash	malicious	Browse	• 78.47.204.80
	FIyE6huzxV.dll	Get hash	malicious	Browse	• 78.47.204.80
	V0gZWRXv8d.dll	Get hash	malicious	Browse	• 78.47.204.80
	t5EuQW2GUF.dll	Get hash	malicious	Browse	• 78.47.204.80
	uh1WyesPlh.dll	Get hash	malicious	Browse	• 78.47.204.80
	8rryPzJR1p.dll	Get hash	malicious	Browse	• 78.47.204.80
	a65FgjVus4.dll	Get hash	malicious	Browse	• 78.47.204.80
	bWjYh6H8wk.dll	Get hash	malicious	Browse	• 78.47.204.80
	ZJOHKItBoJ.dll	Get hash	malicious	Browse	• 78.47.204.80
	eyPPiz3W6u.dll	Get hash	malicious	Browse	• 78.47.204.80
	HjYSwxqyUn.dll	Get hash	malicious	Browse	• 78.47.204.80
	f47YPsvRI3.dll	Get hash	malicious	Browse	• 78.47.204.80
	2n64VXT08V.dll	Get hash	malicious	Browse	• 78.47.204.80
	qUr4bXsweR.dll	Get hash	malicious	Browse	• 78.47.204.80
	52O6evfqQT.dll	Get hash	malicious	Browse	• 78.47.204.80
	ONEitXKvz6.dll	Get hash	malicious	Browse	• 78.47.204.80
	F2433DFBA69148A0C3A5A5951D360B6C3C045090DE06F.exe	Get hash	malicious	Browse	• 5.9.162.45
AS-CHOOPAUS	5YO8hZg21O.dll	Get hash	malicious	Browse	• 66.42.57.149
	dUGnMYeP1C.dll	Get hash	malicious	Browse	• 66.42.57.149
	yFAXc9z51V.dll	Get hash	malicious	Browse	• 66.42.57.149
	9fC0as7YLE.dll	Get hash	malicious	Browse	• 66.42.57.149
	FIyE6huzxV.dll	Get hash	malicious	Browse	• 66.42.57.149
	V0gZWRXv8d.dll	Get hash	malicious	Browse	• 66.42.57.149
	t5EuQW2GUF.dll	Get hash	malicious	Browse	• 66.42.57.149
	uh1WyesPlh.dll	Get hash	malicious	Browse	• 66.42.57.149
	8rryPzJR1p.dll	Get hash	malicious	Browse	• 66.42.57.149
	a65FgjVus4.dll	Get hash	malicious	Browse	• 66.42.57.149
	bWjYh6H8wk.dll	Get hash	malicious	Browse	• 66.42.57.149
	ZJOHKItBoJ.dll	Get hash	malicious	Browse	• 66.42.57.149
	eyPPiz3W6u.dll	Get hash	malicious	Browse	• 66.42.57.149
	HjYSwxqyUn.dll	Get hash	malicious	Browse	• 66.42.57.149
	f47YPsvRI3.dll	Get hash	malicious	Browse	• 66.42.57.149
	2n64VXT08V.dll	Get hash	malicious	Browse	• 66.42.57.149
	qUr4bXsweR.dll	Get hash	malicious	Browse	• 66.42.57.149
	52O6evfqQT.dll	Get hash	malicious	Browse	• 66.42.57.149
	ONEitXKvz6.dll	Get hash	malicious	Browse	• 66.42.57.149
	F2433DFBA69148A0C3A5A5951D360B6C3C045090DE06F.exe	Get hash	malicious	Browse	• 149.28.253.196
EcobandGH	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
	uh1WyesPlh.dll	Get hash	malicious	Browse	• 196.44.98.190
	8rryPzJR1p.dll	Get hash	malicious	Browse	• 196.44.98.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	a65FgjVus4.dll	Get hash	malicious	Browse	• 196.44.98.190
	bWjYh6H8wk.dll	Get hash	malicious	Browse	• 196.44.98.190
	ZJOHKltBoJ.dll	Get hash	malicious	Browse	• 196.44.98.190
	eyPPiz3W6u.dll	Get hash	malicious	Browse	• 196.44.98.190
	HjYSwxqyUn.dll	Get hash	malicious	Browse	• 196.44.98.190
	f47YPsvRI3.dll	Get hash	malicious	Browse	• 196.44.98.190
	2n64VXT08V.dll	Get hash	malicious	Browse	• 196.44.98.190
	qUr4bXsweR.dll	Get hash	malicious	Browse	• 196.44.98.190
	52O6evfqQT.dll	Get hash	malicious	Browse	• 196.44.98.190
	ONEitXKvz6.dll	Get hash	malicious	Browse	• 196.44.98.190
	1w9i8K6AzWV5RmHTSn8.dll	Get hash	malicious	Browse	• 196.44.98.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	5YO8hZg21O.dll	Get hash	malicious	Browse	• 51.178.61.60
	dUGnMYeP1C.dll	Get hash	malicious	Browse	• 51.178.61.60
	yFAXc9z51V.dll	Get hash	malicious	Browse	• 51.178.61.60
	9fC0as7YLE.dll	Get hash	malicious	Browse	• 51.178.61.60
	FIyE6huzxV.dll	Get hash	malicious	Browse	• 51.178.61.60
	V0gZWRXv8d.dll	Get hash	malicious	Browse	• 51.178.61.60
	t5EuQW2GUF.dll	Get hash	malicious	Browse	• 51.178.61.60
	uh1WyesPlh.dll	Get hash	malicious	Browse	• 51.178.61.60
	8rryPzJR1p.dll	Get hash	malicious	Browse	• 51.178.61.60
	a65FgjVus4.dll	Get hash	malicious	Browse	• 51.178.61.60
	bWjYh6H8wk.dll	Get hash	malicious	Browse	• 51.178.61.60
	ZJOHKltBoJ.dll	Get hash	malicious	Browse	• 51.178.61.60
	eyPPiz3W6u.dll	Get hash	malicious	Browse	• 51.178.61.60
	02D6463C8D80183F843D874AB427C11FC47B6B9CE4726.exe	Get hash	malicious	Browse	• 51.178.61.60
	HjYSwxqyUn.dll	Get hash	malicious	Browse	• 51.178.61.60
	f47YPsvRI3.dll	Get hash	malicious	Browse	• 51.178.61.60
	2n64VXT08V.dll	Get hash	malicious	Browse	• 51.178.61.60
	qUr4bXsweR.dll	Get hash	malicious	Browse	• 51.178.61.60
	52O6evfqQT.dll	Get hash	malicious	Browse	• 51.178.61.60
	ONEitXKvz6.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):	7.178846163511901
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.40% • Clipper DOS Executable (2020/12) 0.20% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	wNjqkrm8pH.dll
File size:	485376
MD5:	699b39c805f6a366707eb9a0e580bc0d

General

SHA1:	04489a4c9d50b62a9ff16f5baa67f568b2eb46ed
SHA256:	142d330305cf2bba895b000b9c7c2da6c6b38cb728d3fb347da8dd9f0bed4845
SHA512:	840b88d0d294b84b46e15eb6f6172171e370cc91d1dce89daa8d5dd5b9133683797b382fc61545c9fb73d4278819c48322c8063ccf6711611fc0442ae79ba31f
SSDEEP:	12288:bdv8jkvzqZvv2wLBymTi12yD88kYwZ1h1:b2Zvv2c1Ti1v0Z1h
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10015826
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61964C08 [Thu Nov 18 12:50:16 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:	261bae8b02d2e7bf979e55d76b9dc786

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3930c	0x39400	False	0.530729735262	data	6.66187646144	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3b000	0x13cfe	0x13e00	False	0.464512087264	data	5.41556152438	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4f000	0x252c	0x1800	False	0.223795572917	data	3.845062089	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x52000	0x24410	0x24600	False	0.818513745704	data	7.74948390886	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x77000	0x33a0	0x3400	False	0.71484375	data	6.58405020621	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

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
11/19/21-01:05:43.275474	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49747	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

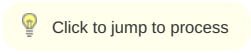
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49747	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-19 00:05:44 UTC	0	OUT	GET /BJKdnuOnKNLLGEDBpJpeXPiWYvJQgGvoYhhdIpnN HTTP/1.1 Cookie: kpcXAWpZfRkJEAy=i+5bJ+1ZInDjvfPM+1JhKt+KWj8rVMERTO3MBxIOillAvxAx2ioHmQPbtLgNLA6EGF RwLshnv6kCnZWyIXAgbMZzd1u5zeY7pIcnc7NYlk4ptgX0JiJVkIXW1dfaYySomVYPcSiwpIcomQgIb/a5XevS7QE2 etUd+zxfOWZFj62QjzAO7FAj4VKuBSkPo+IBUjmiQKTNcL09qokscyBsIQcAMaCCPfrdl8uN2W5z+g+7 Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache
2021-11-19 00:05:44 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Nov 2021 00:05:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-11-19 00:05:44 UTC	0	IN	Data Raw: 33 65 66 0d 0a 64 ca 1e 80 24 75 d9 5f ee 00 12 92 90 60 fe f8 4d d1 a6 22 5d 8c 03 6e 4b a1 65 50 63 f0 b0 2c 53 25 07 40 a3 d4 75 42 b0 75 c8 40 29 fa 6d bd 0e 24 50 70 4b a0 6d 4a 27 64 30 32 1c a5 25 f6 a7 bb 80 a9 b6 03 92 b0 86 98 93 28 65 f6 fe 17 3c 99 d3 e1 42 66 bc 20 1d de 33 25 a4 8e 5c 71 33 e9 ca 67 9b 05 79 4c cf b2 00 84 fa c7 cc 22 0c b8 4d ea ea 2b 14 fa 7a f2 30 5f e2 99 0e b9 6b 60 ce 5f b4 b8 2b 21 87 95 68 af c6 3e b3 b9 ae f2 90 f2 ba 41 bc dc 54 85 fb 2b 24 b4 82 48 be e2 65 61 34 59 b3 40 c2 f7 db 69 ed 16 4d 8a f2 1f 59 b0 eb 38 4b c6 36 68 f8 75 17 c3 98 f6 b0 3c cc b2 08 8a bd 1c 2f b7 cf a2 d1 fe e9 df 23 dd 25 e4 6f ab 7c be 65 6e 4f 19 56 78 f9 f1 73 7d 71 19 7c 8d 08 35 28 57 9f f0 2d 2b 35 7e 87 17 f5 5a f0 0e f3 d7 86 b1 Data Ascii: 3efd$u_`M"]nKePc,S%@uBu@)m$PpKmJ'd02%(e<Bf 3%\q3gyL"M+z0_k`_+!h>AT+$Hea4Y@iMY8 K6hu</#%o|enOVxs}q|5(W-+5~Z

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6164 Parent PID: 4864

General

Start time:	01:04:10
Start date:	19/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll"
Imagebase:	0xe10000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
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: 00000000.00000002.415487729.000000000117D000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2804 Parent PID: 6164

General

Start time:	01:04:10
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.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: rundll32.exe PID: 6280 Parent PID: 6164

General

Start time:	01:04:11
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\wNjqkrm8pH.dll,Control_RunDLL
Imagebase:	0x1150000
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: 00000002.00000002.352283785.0000000000E2A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 5940 Parent PID: 2804

General

Start time:	01:04:11
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",#1
Imagebase:	0x1150000
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: 00000003.00000002.352402052.000000000344A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6416 Parent PID: 6164

General

Start time:	01:04:15
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\wNjqkrm8pH.dll,abziuleoxsborpb
Imagebase:	0x1150000
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: 00000004.00000002.415304095.00000000032EA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6420 Parent PID: 6164

General

Start time:	01:04:23
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\wNjqkrm8pH.dll,aejkroaebsbxdnkhb
Imagebase:	0x1150000
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: 00000005.00000002.413760673.0000000000D1A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 2944 Parent PID: 5940

General

Start time:	01:04:38
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",Control_RunDLL
Imagebase:	0x1150000
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: 672 Parent PID: 6280

General

Start time:	01:04:38
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Hsngzdtsiohsyp\jlodhhplzusb.iie",cwqsUWjgRvl
Imagebase:	0x1150000
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: 00000007.00000002.426884632.000000000328A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6828 Parent PID: 6416

General

Start time:	01:04:56
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",Control_RunDLL
Imagebase:	0x1150000
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: 1304 Parent PID: 6420

General

Start time:	01:05:05
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",Control_RunDLL
Imagebase:	0x1150000
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: 6848 Parent PID: 6164

General

Start time:	01:05:06
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\wNjqkrm8pH.dll",Control_RunDLL
Imagebase:	0x1150000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 5932 Parent PID: 572

General

Start time:	01:05:12
Start date:	19/11/2021
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: rundll32.exe PID: 6388 Parent PID: 672

General

Start time:	01:05:13
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Hsngzdtsiohsyp\jlodhhplzusb.iie",Control_RunDLL
Imagebase:	0x1150000
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: 0000000E.00000002.816631755.0000000000C67000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 5416 Parent PID: 572

General

Start time:	01:05:48
Start date:	19/11/2021
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: 2276 Parent PID: 572

General

Start time:	01:06:12
Start date:	19/11/2021
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: 2236 Parent PID: 572

General

Start time:	01:06:35
Start date:	19/11/2021
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

Disassembly

Code Analysis