ID: 524857
Sample Name: yFAXc9z51V
Cookbook: default.jbs
Time: 00:57:18
Date: 19/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report yFAXc9z51V

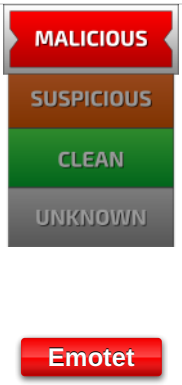
Overview

General Information

Sample Name:	yFAXc9z51V (renamed file extension from none to dll)
Analysis ID:	524857
MD5:	fee9ba8d79bcbc5..
SHA1:	82eb29987e6ed5..
SHA256:	3e8acc4d85b6ffc…
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:

Detection

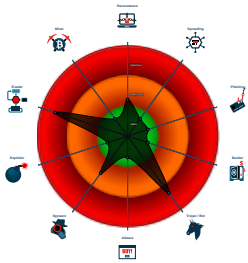


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…

Classification



Process Tree

- **System is w10x64**
- svchost.exe (PID: 3604 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- loaddll32.exe (PID: 924 cmdline: loaddll32.exe "C:\Users\user\Desktop\yFAXc9z51V.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6648 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\yFAXc9z51V.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5564 cmdline: rundll32.exe "C:\Users\user\Desktop\yFAXc9z51V.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6904 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\yFAXc9z51V.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2336 cmdline: rundll32.exe C:\Users\user\Desktop\yFAXc9z51V.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6976 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Wlimfwutowthen\gdntcqg.ebr",vQmrKt MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6768 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Wlimfwutowthen\gdntcqg.ebr",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2528 cmdline: rundll32.exe C:\Users\user\Desktop\yFAXc9z51V.dll,abziuleoxsborpb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6200 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\yFAXc9z51V.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 160 cmdline: rundll32.exe C:\Users\user\Desktop\yFAXc9z51V.dll,aejkroaebsbxdnkhb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 7156 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\yFAXc9z51V.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7148 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\yFAXc9z51V.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 6656 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6108 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6236 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6896 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 4036 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6428 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5496 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 3928 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 4332 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1060 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5980 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4424 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.388952908.000000000295A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.414340731.00000000033AA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000009.00000002.390623075.00000000028BA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.363481536.0000000002AFA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000001.00000002.390502900.000000000097D000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.2b14358.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.28d41f8.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.2ad5298.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.2974250.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.2b14358.0.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)

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

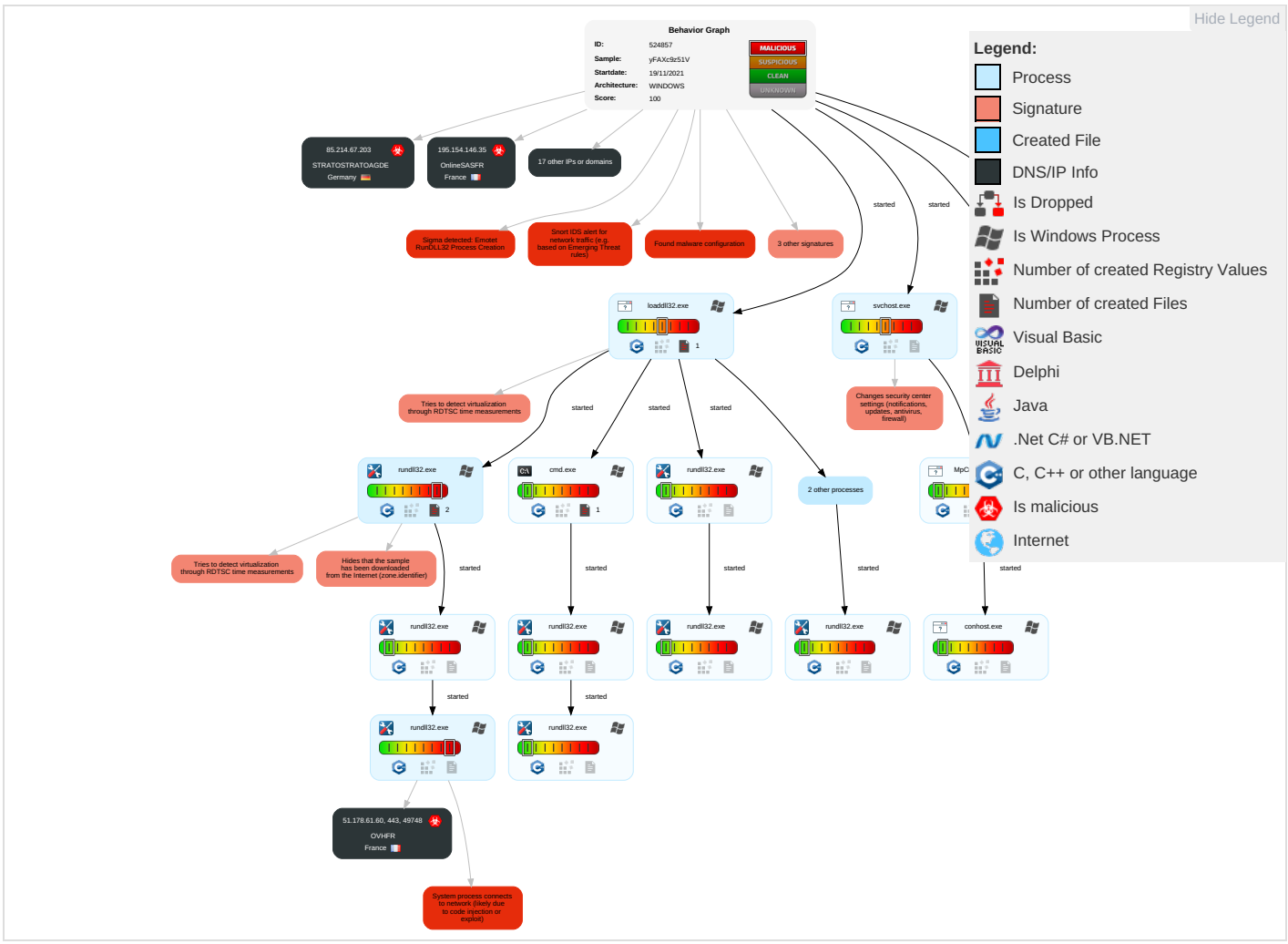
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Con
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 1 1 2	Masquerading 2 1	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 Con
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 5 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress T Transfer
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	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 2	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 Channels
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 Commur
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 1 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Common Used Po
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 Protocols

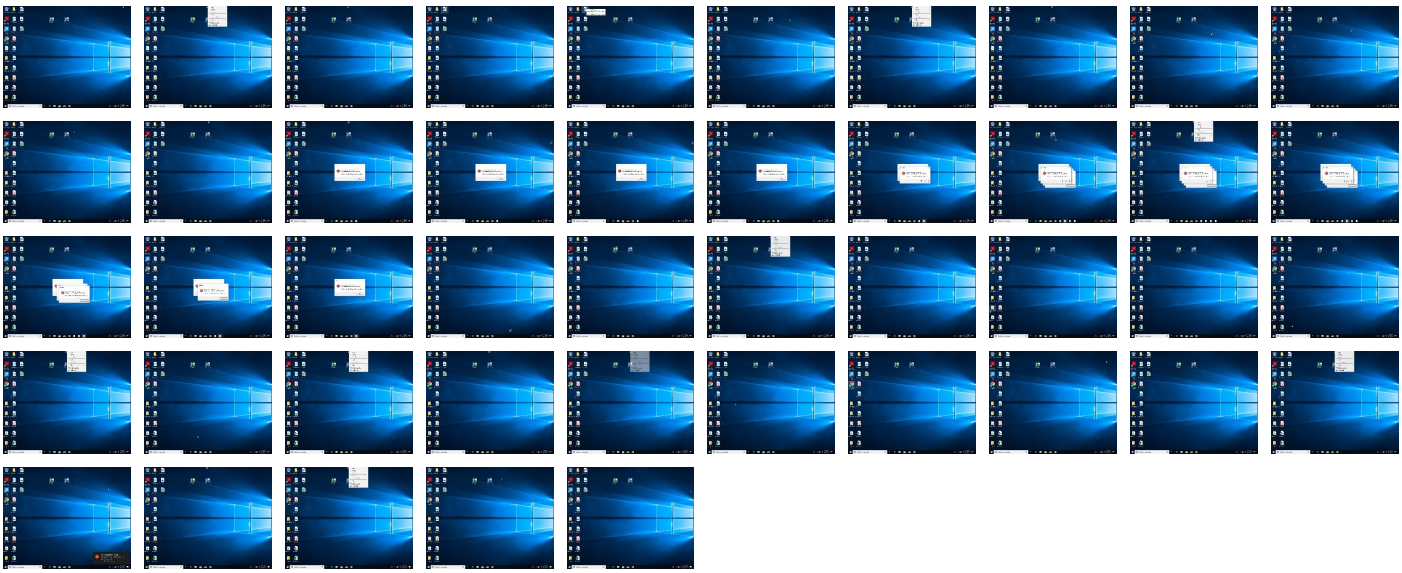
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
yFAXc9z51V.dll	24%	Virustotal		Browse
yFAXc9z51V.dll	23%	ReversingLabs	Win32.Infostealer.Convagent	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.3250000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.4220000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.2.loaddll32.exe.c50000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.2ad5298.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.2c30000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.2d40000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.2790000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
19.2.rundll32.exe.4040000.0.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.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://51.178.61.60/RUMPKfyWvwh	0%	Avira URL Cloud	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/RUMPKfyWvwh	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:	524857
Start date:	19.11.2021
Start time:	00:57:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yFAXc9z51V (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:	34
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@37/8@0/20
EGA Information:	Failed
HDC Information:	• Successful, ratio: 42.9% (good quality ratio 37.8%) • Quality average: 67.9% • Quality standard deviation: 31.1%
HCA Information:	• Successful, ratio: 78% • 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
01:00:03	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
01:00:18	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	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FIyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
	8rryPzJR1p.dll	Get hash	malicious	Browse	
	a65FgjVus4.dll	Get hash	malicious	Browse	
	bWjYh6H8wk.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
196.44.98.190	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FIyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	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
	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
EcobandGH	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	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
	ZJOHKItBoJ.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
	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

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1101587720598329
Encrypted:	false
SSDEEP:	12:26SJlzXm/Ey6q9995dq3qQ10nMCldimE8eawHjc48v:26mYl68yLyMCldzE9BHjch
MD5:	DC35AEEFD9A4AC32F636DB97DD77F7B4
SHA1:	92C04E6C2D7192FE98D5EFCB12FCC65E522DFD4E
SHA-256:	A74D363E9CF61A22014B82583FCA514A3BE9F0A2D0788D34EF79F50E31C503AE
SHA-512:	F4CE64CFEAC6715BD85E6E5387AA87E9B2BECF90593F8948AA9774390EB24388E86300CEC81CE72C4D1E48ADB47D56D12B836D1142A98BEECDA17E60FB6C360

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Malicious:	false
Preview:	.....\....O.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....CY1..... .....'..#.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c. k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.,...\....O..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11245296714236776
Encrypted:	false
SSDEEP:	12:GJUzXm/Ey6q9995d51miM3qQ10nMCldimE8eawHza1milbMf:4l68x1tMLyMCldzE9BHza1tlY
MD5:	2983F84BE50E8B7DE67EFCF0E59D1161
SHA1:	3111C2A7E722FE73275E9A2AE8CF32981A3E4367
SHA-256:	0FBB517D446AF3E8A8F6BDAA8BE246867EDDEA8897EBC7E623AEE11CF287104C
SHA-512:	3BD7E3B8F810D85A9AAD482DDB3C0A9E576ED21C4EC82605F902C7D50F4AF69C74BDF8A7A3F2004B3E01A2AFC76B53996982C95272F99F060F9A163F4774EBE D
Malicious:	false
Preview:	.....\....O.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....CY1..... .....#.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l .\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.,...\....#O..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11239433397049552
Encrypted:	false
SSDEEP:	12:GyzXm/Ey6q9995hi1mK2P3qQ10nMCldimE8eawHza1mKOZf:Al68fi1iPLyMCldzE9BHza1W
MD5:	B5565AFBE83FB0B5C53610A7C504D210
SHA1:	869EFD851CD535B035ACB3B45226282CAE014AAF
SHA-256:	1FFFF4A904F4BD62AA4D678D46034F77940F7D2A313804CF1D9FCCC1A52110EA
SHA-512:	C65F60294714D8087854B3260D0407C918B2AE92940B37D413D23E2559BF659BD4DF06E4A49C00282C355F309E98A721555C4C0E6760BE9787B3C581C7D84E0F
Malicious:	false
Preview:	.....\...:.E.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....CY1..... .....#.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.,...\....F..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1101587720598329
Encrypted:	false
SSDEEP:	12:26SJlzXm/Ey6q9995dq3qQ10nMCldimE8eawHjc48v:26mYl68yLyMCldzE9BHjch
MD5:	DC35AEEFD9A4AC32F636DB97DD77F7B4
SHA1:	92C04E6C2D7192FE98D5EFCB12FCC65E522DFD4E
SHA-256:	A74D363E9CF61A22014B82583FCA514A3BE9F0A2D0788D34EF79F50E31C503AE
SHA-512:	F4CE64CFEAC6715BD85E6E5387AA87E9B2BECF90593F8948AA9774390EB24388E86300CEC81CE72C4D1E48ADB47D56D12B836D1142A98BEECDA17E60FB6C3 60
Malicious:	false
Preview:	.....\....O.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....CY1..... .....'..#.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c. k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.,...\....O..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11245296714236776
Encrypted:	false
SSDEEP:	12:GJUzXm/Ey6q9995d51miM3qQ10nMCldimE8eawHza1miIbMf:4l68x1tMLyMCldzE9BHza1tIY
MD5:	2983F84BE50E8B7DE67EFCF0E59D1161
SHA1:	3111C2A7E722FE73275E9A2AE8CF32981A3E4367
SHA-256:	0FBB517D446AF3E8A8F6BDAA8BE246867EDDEA8897EBC7E623AEE11CF287104C
SHA-512:	3BD7E3B8F810D85A9AAD482DDB3C0A9E576ED21C4EC82605F902C7D50F4AF69C74BDF8A7A3F2004B3E01A2AFC76B53996982C95272F99F060F9A163F4774EBE D
Malicious:	false
Preview:	....,..\.....O.....................B.............Zb..@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..CY1...... ....#...........U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l .\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.......P.P.,...\....#O.. ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11239433397049552
Encrypted:	false
SSDEEP:	12:GyzXm/Ey6q9995hi1mK2P3qQ10nMCldimE8eawHza1mKOZf:Al68fi1iPLyMCldzE9BHza1W
MD5:	B5565AFBE83FB0B5C53610A7C504D210
SHA1:	869EFD851CD535B035ACB3B45226282CAE014AAF
SHA-256:	1FFFF4A904F4BD62AA4D678D46034F77940F7D2A313804CF1D9FCCC1A52110EA
SHA-512:	C65F60294714D8087854B3260D0407C918B2AE92940B37D413D23E2559BF659BD4DF06E4A49C00282C355F309E98A721555C4C0E6760BE9787B3C581C7D84E0F
Malicious:	false
Preview:	....,..\...:.E.....................B.............Zb..@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..CY1...... ....#...........U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.......P.P.,...\.....F.. ....

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):	9062
Entropy (8bit):	3.164795917848804
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zjn+I9:j+s+v+b+P+m+0+Q+q+8+w
MD5:	358E84AACB195494C75FAB6D68B99F1A
SHA1:	92E2DD504557E7E15F0C8DBE7E745978BFD6FFCE
SHA-256:	F5AFB444723487FDE4CFD4CCF1536C273796A87371B7E1A160F70706612ABDFB
SHA-512:	8D0A67B410F203A7DC862945830B5F7E91DEF2500FD32DCA1423253246905C76FCBDA1E8EB2D9E4A5AD26582A6B42203F892FE088635516B3275FC2CEF06146A
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_085830_065.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.8155632809083784
Encrypted:	false
SSDEEP:	96:sbCLO2o+ZK5Fu9+/YrmCKvI2l/SkQP46lT24jFzdNMCKdJRej52F+NMCAY5+bUM4:sOLt5kWt28rcCqTNCITCpCVCcCR
MD5:	469DA211A59A2EB76ECA172177D95D00

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211119_085830_065.etl	
SHA1:	CE8D4B0BA25F6C4935EE133D04EA3D115C5B9C1D
SHA-256:	760E93FC4B973D77DE91BD19F204F02F264FCEF7B1ABE581618D21DCBF3B9765
SHA-512:	278BEF860684BF53584AE62FC1C4D0CAE16806102DBEB6E44E3C46641E93D15D6DF0EC5CF2F6900A2461F695D6CDFD57D36CEC5A704981B22302577BCD05B6C
Malicious:	false
Preview:	....l.....x+.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....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._.0.8.5.8.3.0._.0.6.5...e.t.l.....P.P.....x+..... .....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.178854423942452
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:	yFAXc9z51V.dll
File size:	485376
MD5:	fee9ba8d79bcbc58800fda0cafbe5f64
SHA1:	82eb29987e6ed568a5ae01816de7240df1490c0d
SHA256:	3e8acc4d85b6ffc06b18b97a33a43628e8c11bc4dde8648bcc8a2ad9b1154150
SHA512:	fbc664d79a841b054ae60045286871cc3af79be10193562f730245941772241fcd56854c9decb18182832b1db5a2bbfff346e15c0c8af9b25c24bd8fe285062f
SSDEEP:	12288:bdv8jkvzqZvv2wLBVmTi12yD88kYwZ1h1:b2Zvv2ccTi1v0Z1h
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

General

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	0.818520457474	data	7.74949552696	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
11/19/21-00:59:36.582289	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49748	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	49748	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-18 23:59:37 UTC	0	OUT	GET /RUMPKfyWvwh HTTP/1.1 Cookie: gVql=qP2SWVnr/WJG8YP5xSF8G7Rr6KkEKH5oVbT/aPyZcyn9K/saApq06qYJQ7VQDqAGQmsog3CqnGHN9x0QykU5uuVnobYs31akiF1WnncdqfGM3pGgWKZ2r4ogC9SE6Vh2+mnqzNK2/WuhSLvfpxzgrn3BeUCBl3LUqJXa1TfC4xBhYwdQa/6a5jixa5pMiqaToa/047TTwtpTt5xgOLwssCVW5YzKACeEqQfp8YgGPHadd14J0SJTGVNqyFCbrXXoDBPSb3GwjcRynh1BJ5z3u6jM5aWKTd6XgU1rwPi8sKMzrSyB1Zu0v5YluHWstRSulPtNogkEJBlOu+qxuLWX18w= Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache
2021-11-18 23:59:37 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 18 Nov 2021 23:59:37 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-11-18 23:59:37 UTC	0	IN	Data Raw: 32 33 37 0d 0a 5f b0 47 cc 74 f0 42 ef 83 3d 1b 5a 94 05 58 5f e5 ff d9 ee 9d 3d 93 0f fc aa 7c 43 b7 a3 31 3b dc c4 30 ad bf 98 5f a3 13 fe f9 18 d5 08 0a a0 4f 3e b9 75 42 a4 fe 8c 2a 0c 38 b8 d1 64 3a bf fe 4c 2f e4 73 0a 6e 70 05 2f b1 12 84 58 81 88 d6 10 7f f7 d6 5d 79 4e c9 79 51 13 82 bf ea ca 51 f4 00 72 7c 69 70 82 10 9b f7 dc 35 b3 9b ac 28 bb e6 85 fe b5 ba 1c 2b 64 9f af f9 0f 91 74 66 fb d9 a4 7f 62 07 73 f2 dc 75 bf 0d 35 ef be 86 a8 8d b9 35 40 17 06 92 0b 65 87 8e 58 8d fd 05 7f 32 9b ef 84 29 40 6d 6c 34 70 28 82 42 6a 9e 4f 1e a3 86 85 44 82 87 50 5b 96 d8 81 a5 3d c4 70 66 26 42 c2 c4 2d d9 c5 1e 5e b6 6c f5 72 be a3 6f 91 8c d7 91 e1 8c d7 0b 2a 51 e2 47 41 50 62 ce 72 bd 9e 6c 66 e2 f0 d8 2e 55 01 de 4c ee 93 5c 87 35 e8 50 64 cb c5 Data Ascii: 237_GtB=ZX_=|C1;0_O>uB*8d:L/snp/X]yNyQQr|ip5(+dtfbsu55@eX2)@ml4p(BjODP[=pf&B-^lro*QGAPbr lf.UL\5Pd

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: svchost.exe PID: 3604 Parent PID: 572

General

Start time:	00:58:11
Start date:	19/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: loaddll32.exe PID: 924 Parent PID: 5272

General

Start time:	00:58:11
Start date:	19/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\yFAXc9z51V.dll"
Imagebase:	0x290000
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: 00000001.00000002.390502900.000000000097D000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6656 Parent PID: 572

General

Start time:	00:58:11
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6648 Parent PID: 924

General

Start time:	00:58:11
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\yFAXc9z51V.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: 2336 Parent PID: 924

General

Start time:	00:58:12
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\yFAXc9z51V.dll,Control_RunDLL
Imagebase:	0x1f0000
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: 00000004.00000002.365418732.0000000002ABA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 5564 Parent PID: 6648

General

Start time:	00:58:12
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\yFAXc9z51V.dll",#1
Imagebase:	0x1f0000
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: 00000005.00000002.363481536.0000000002AFA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6108 Parent PID: 572

General

Start time:	00:58:12
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6236 Parent PID: 572

General

Start time:	00:58:12
Start date:	19/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 2528 Parent PID: 924

General

Start time:	00:58:16
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\yFAXc9z51V.dll,abziuleoxsborpb
Imagebase:	0x1f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.388952908.000000000295A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 160 Parent PID: 924

General

Start time:	00:58:23
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\yFAXc9z51V.dll,aejkroaebsbxdnkhb
Imagebase:	0x1f0000
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: 00000009.00000002.390623075.00000000028BA000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 6896 Parent PID: 572

General

Start time:	00:58:30
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:	0x7ff70d6e0000
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: 6904 Parent PID: 5564

General

Start time:	00:58:41
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\yFAXc9z51V.dll",Control_RunDLL
Imagebase:	0x1f0000
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: 6976 Parent PID: 2336

General

Start time:	00:58:43
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Wlimfwutowthen\gdntcqg.ebr",vQmrKt
Imagebase:	0x1f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.414340731.00000000033AA000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: SgrmBroker.exe PID: 4036 Parent PID: 572

General

Start time:	00:58:53
Start date:	19/11/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7f54e0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6200 Parent PID: 2528

General

Start time:	00:58:54
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\yFAXc9z51V.dll",Control_RunDLL
Imagebase:	0x1f0000
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: 7156 Parent PID: 160

General

Start time:	00:59:00
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\yFAXc9z51V.dll",Control_RunDLL
Imagebase:	0x1f0000
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: 7148 Parent PID: 924

General

Start time:	00:59:00
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\yFAXc9z51V.dll",Control_RunDLL
Imagebase:	0x1f0000
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: 6428 Parent PID: 572

General

Start time:	00:59:01
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:	0x7ff70d6e0000
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: svchost.exe PID: 4332 Parent PID: 572

General

Start time:	00:59:06
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: 6768 Parent PID: 6976

General

Start time:	00:59:12
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Wlimfwutowthen\gdntcqg.ebr",Control_RunDLL
Imagebase:	0x1f0000
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: 00000013.00000002.808384988.00000000026E7000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 1060 Parent PID: 572

General

Start time:	00:59:43
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: 5980 Parent PID: 572

General

Start time:	01:00:00
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: MpCmdRun.exe PID: 5496 Parent PID: 6428

General

Start time:	01:00:02
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:	0x7ff6eaa50000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 3928 Parent PID: 5496

General

Start time:	01:00:03
Start date:	19/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4424 Parent PID: 572

General

Start time:	01:00:15
Start date:	19/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
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