ID: 553389
Sample Name: YBfn5E3Dlw
Cookbook: default.jbs
Time: 19:48:48
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

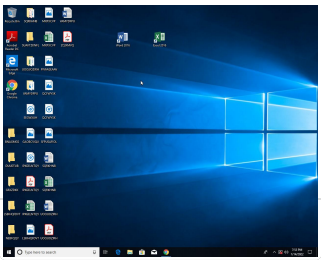
Windows Analysis Report YBfn5E3Dlw

Overview

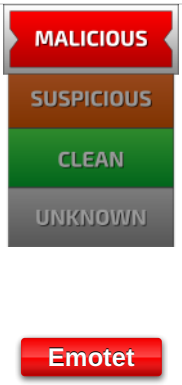
General Information

Sample Name:	YBfn5E3Dlw (renamed file extension from none to dll)
Analysis ID:	553389
MD5:	038f9a9d5b96733.
SHA1:	3b8a4b81f0b0651.
SHA256:	d46762ba155e33..
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection



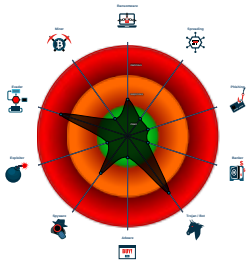
Emotet

Score:	92
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: Suspicious Call by …
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Contains functionality to query locale…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6260 cmdline: loaddll32.exe "C:\Users\user\Desktop\YBfn5E3Dlw.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 2240 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\YBfn5E3Dlw.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6072 cmdline: rundll32.exe "C:\Users\user\Desktop\YBfn5E3Dlw.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 4180 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\YBfn5E3Dlw.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 6500 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Dfktehrjwgeevy\pakqi.bja",rArKTBwXKBsr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
          - rundll32.exe (PID: 6664 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Dfktehrjwgeevy\pakqi.bja",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 5396 cmdline: regsvr32.exe /s C:\Users\user\Desktop\YBfn5E3Dlw.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 6436 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\YBfn5E3Dlw.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1320 cmdline: rundll32.exe C:\Users\user\Desktop\YBfn5E3Dlw.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 6552 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6260 -s 552 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6888 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5628 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6260 -ip 6260 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 1368 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5416 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7132 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "45.138.98.34:80",
    "69.16.218.101:8080",
    "51.210.242.234:8080",
    "185.148.168.220:8080",
    "142.4.219.173:8080",
    "54.38.242.185:443",
    "191.252.103.16:80",
    "104.131.62.48:8080",
    "62.171.178.147:8080",
    "217.182.143.207:443",
    "168.197.250.14:80",
    "37.44.244.177:8080",
    "66.42.57.149:443",
    "210.57.209.142:8080",
    "159.69.237.188:443",
    "116.124.128.206:8080",
    "128.199.192.135:8080",
    "195.154.146.35:443",
    "185.148.168.15:8080",
    "195.77.239.39:8080",
    "207.148.81.119:8080",
    "85.214.67.203:8080",
    "190.90.233.66:443",
    "78.46.73.125:443",
    "78.47.204.80:443",
    "37.59.209.141:8080",
    "54.37.228.122:443"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.680031217.0000000002AE1000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.687070469.0000000000B50000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.684992268.0000000003450000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000002.703964616.0000000002AB0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.687871792.0000000005661000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rundll32.exe.59f0000.10.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.5630000.6.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.4720000.4.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.2ab0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.5690000.8.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 43 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

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)

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

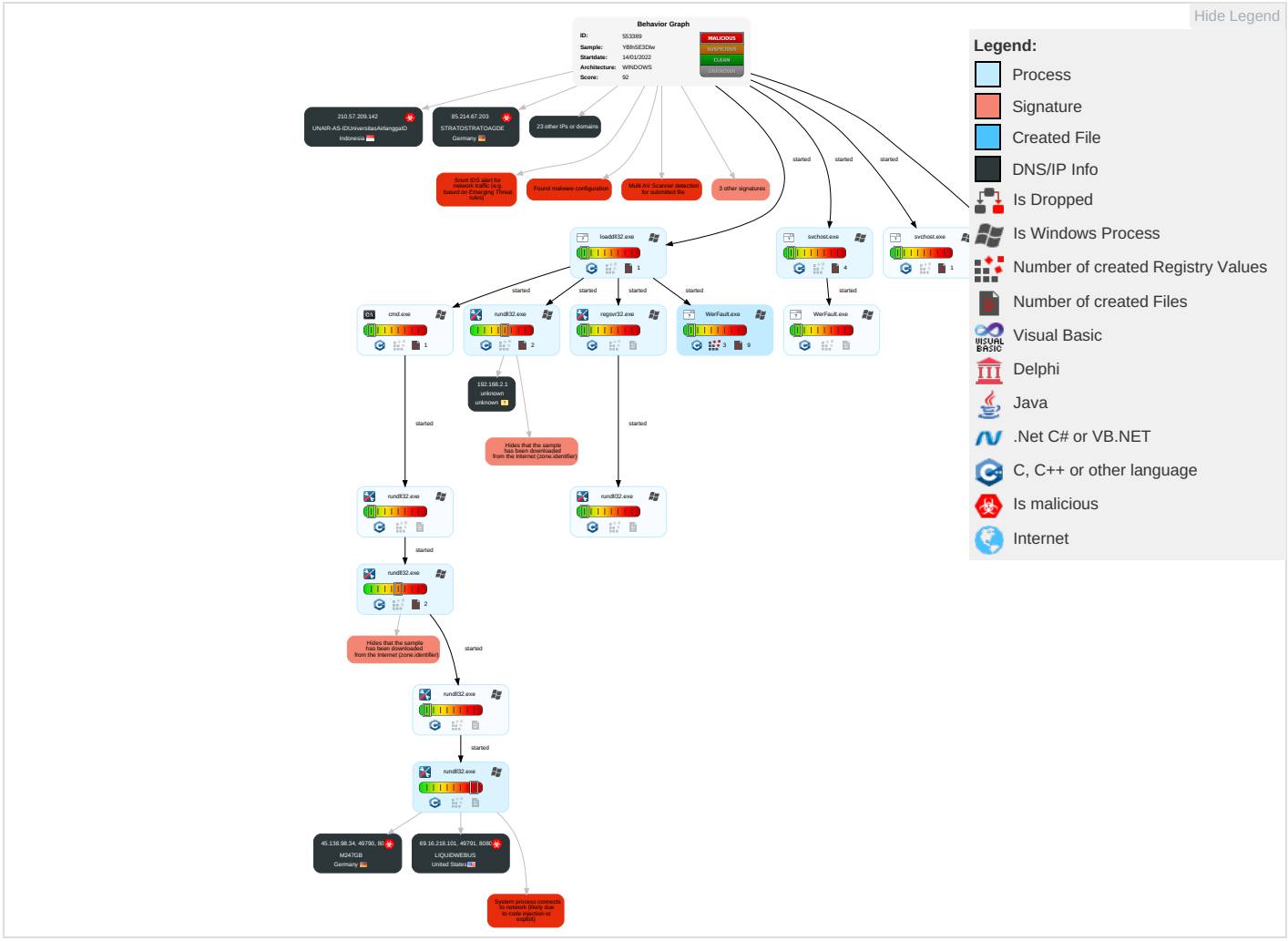
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Native API 2	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Input Capture 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Obfuscated Files or Information 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	System Information Discovery 2 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Security Software Discovery 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Regsvr32 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

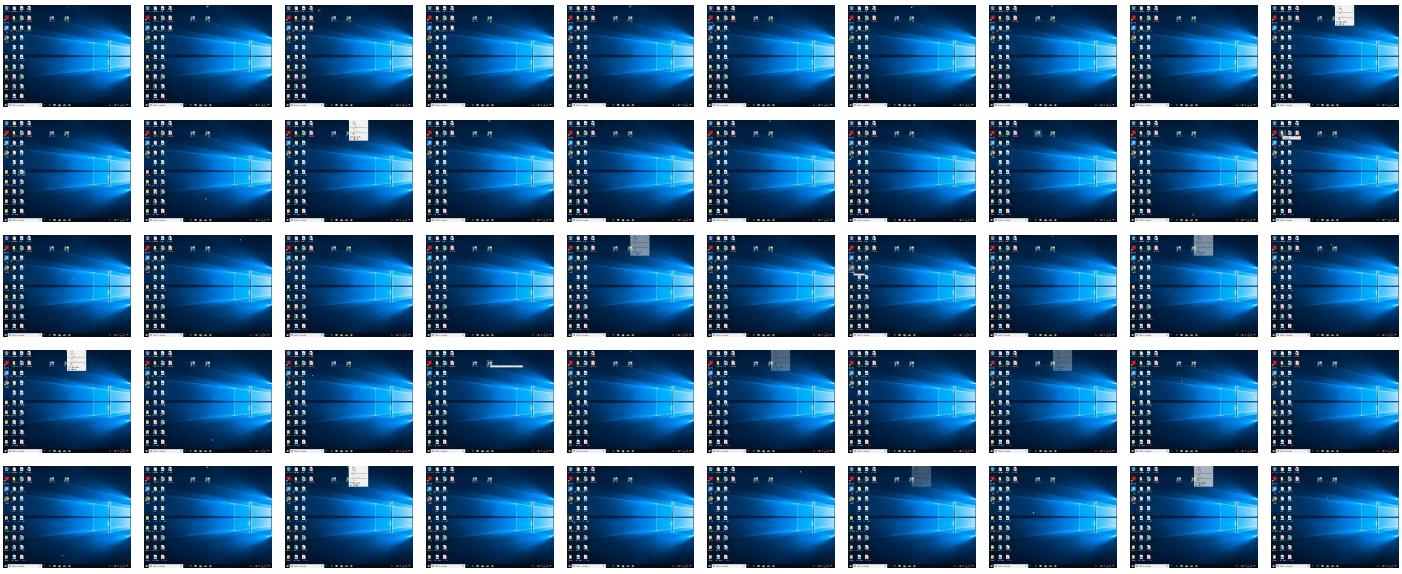
Behavior Graph



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
YBfn5E3Dlw.dll	14%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
YBfn5E3Dlw.dll	16%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.b50000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.2.loaddll32.exe.2ab0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.56c0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.1270000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.59f0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.2.loaddll32.exe.2ae0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.loaddll32.exe.2ae0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.12a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.3450000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.5420000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.5500000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.loaddll32.exe.2ab0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.b80000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.53f0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.5660000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.11c0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4780000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.3600000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.47b0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.loaddll32.exe.2ab0000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4f0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.5a20000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.4750000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.loaddll32.exe.2ae0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.4720000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.5690000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.b20000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.5630000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
2.2.regsvr32.exe.c60000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.54d0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.11f0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.980000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.81.119	unknown	United States		20473	AS-CHOOPAUS	true
104.131.62.48	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternet SABR	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNET AR	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
185.148.168.15	unknown	Germany		44780	EVERSCALE-ASDE	true
51.210.242.234	unknown	France		16276	OVHFR	true
217.182.143.207	unknown	France		16276	OVHFR	true
69.16.218.101	unknown	United States		32244	LIQUIDWEBUS	true
159.69.237.188	unknown	Germany		24940	HETZNER-ASDE	true
45.138.98.34	unknown	Germany		9009	M247GB	true
116.124.128.206	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
37.59.209.141	unknown	France		16276	OVHFR	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
185.148.168.220	unknown	Germany		44780	EVERSCALE-ASDE	true
54.37.228.122	unknown	France		16276	OVHFR	true
190.90.233.66	unknown	Colombia		18678	INTERNEXASAESPCO	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
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
128.199.192.135	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553389
Start date:	14.01.2022
Start time:	19:48:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	YBfn5E3Dlw (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:	26
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:	mal92.troj.evad.winDLL@26/10@0/28
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 98.9% (good quality ratio 92.4%) • Quality average: 70.5% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 76% • 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
19:50:46	API Interceptor	7x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_12a180e49793e381a8b848106c2e1caa7a6a4277_7cac0383_18a51c8a\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_12a180e49793e381a8b848106c2e1caa7a6a4277_7cac0383_18a51c8a\Report.wer	
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7981757905947282
Encrypted:	false
SSDEEP:	96:kc4SgFonYyBy9haol7Jf0pXIQcQSc6mcEUcw3/s+a+z+HbHgpVG4rmMoVazWbSmj:eunLHsieryjpq/u7saS274ItW
MD5:	F6F986B555349D70EC66E15ABCC41890
SHA1:	5C2EF2932A1F16307AC18951CBACD3F50151C05F
SHA-256:	4D9F534FD2F77A71E36EA3A820599F7C5B4489D1D32039948B965D53AD59414E
SHA-512:	2A217B88926A7AB47A31A6F472CBF54173675B9502AF968B4BA16FFB2A0C0463CB2F7BB6023111D76890DBD98470A914D42751D7A0F3ECB4204486BCEFD65831
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.5.9.7.9.5.1.6.4.8.8.5.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.f.d.3.1.0.f.2.-.f.9.e.1.-.4.a.d.7.-.a.1.b.3.-.1.2.6.2.3.e.d.3.f.e.2.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.2.e.c.b.1.7.f.-.0.a.4.4.-.4.7.8.e.-.b.e.a.d.-.e.f.e.0.6.4.4.7.9.0.3.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.7.4.-.0.0.0.1.-.0.0.1.b.-.2.2.e.d.-.a.d.7.e.7.7.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.2././.1.3.:.0.9.:.0.7.:.1.6.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER355.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Jan 14 18:49:56 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	44300
Entropy (8bit):	2.1290506370949975
Encrypted:	false
SSDEEP:	192:NedqBIhNxjO5mYROQaPYfEgZGvI0yrfZPZ/PZw/WcmW0v7kcF4Nw7WZNVNF:4ta5rBDYvRgxDw/zmWY7kcF5WXV7
MD5:	7D5D469A218004033CF0ED3664400CB8
SHA1:	C4EE2D5FE696E1BD6F71C0E0DD8DA2F3490A1A5E
SHA-256:	6EFF54679F3143D50E0ABD570796F215A314A2C9944755DF38223084BEEFEC85
SHA-512:	9E70894E19311018AAD958273E4D0EE97C063967501794D2F81F8243E1591C17310F2836761C28BCA875B2CAFB035E9C50D945CF0410355529C502B196EEA970
Malicious:	false
Preview:	MDMP..... .....a.....$...T.....%.....`.....8.....T.....x.....d.....U.....B..... ...GenuineIntelW.....T.....t.....a.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER961.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8348
Entropy (8bit):	3.701420415223348
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiYR6OAx6YrJSUXy1gmfdSwGs+pBs89bakKhsf3N+m:RrlsNi26OAx6YlSUXy1gmfdSwCakKaf9
MD5:	0E3B556676E1972AF45F6860569A4348
SHA1:	CCA48B9EBB72F6FD774F8A5B325A3F3E01F2CACC
SHA-256:	75B3330CE4091AB2C41009973760A92D19547054C547DA848BB949965346C191
SHA-512:	AA446E322338003BA84B921EBBB6EB3F7B7E8618994D96CFB0E0EEF8A8C98B3A33B4D6E0CEFA8362F80E04857643EEBB071D126D5CBF04F1CD544F0EA7CD6E0F
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.2.6.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE44.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4598
Entropy (8bit):	4.473108429492209
Encrypted:	false
SSDEEP:	48:cvIwSD8zs3JgtWl924WSC8BVp8fm8M4J2+SZFL+q84pzLTKcQIcQw0Vd:uITfZhxSN/OJQfxXKkw0Vd
MD5:	032926C5777B8A0C1B4AE5FD2E6341A0

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE44.tmp.xml	
SHA1:	40E9C560877A7DFD13F7B873DB21A94969A4A750
SHA-256:	8A52CE09864457C05D2CFFC21719F2D4FBD93C39AC133CE67772F37C1192E695
SHA-512:	789F99617C9DA1188FFABCB71B4DAC6B055BBBE16F83B0962FF121CAD9A81EFA03196AD58FAD7C61FFE7A82FC65E6AF7AA0B5D1283E03CF5BEC27BE3E7BF3A98
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1342320" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF761.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54270
Entropy (8bit):	3.039245433474246
Encrypted:	false
SSDEEP:	1536:bNHszwoPun9zObOA3An2NH8eII/TlS6KzOojlp2mpoc:bNHszwoPun9zObOA3An2NH8eII/To6KV
MD5:	E774D2B8707457EEF38FFCD785616182
SHA1:	D5368EC392C150B5C1D2C5601A775ACD0A3F0E1D
SHA-256:	77A23CBC153EFAC355ADC08F9839A27BE6B22F69C013158BD4140162E57F60DD
SHA-512:	DAA572285A4531933A3C0605EE7B40B05E793008F187AB2F7D4588BB970B39EB1561C5A95C5AAB74A77AB9A63A7DD1F29C3CA41D8B4E579E1EF1BB630D8993C9
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF61.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.694806766675773
Encrypted:	false
SSDEEP:	96:9GiZYWlEgJhIqYBYwOW5VHZYEZZmtk0iOlBIHwQAKnaF1BCBwHIA+P3:9jZDl8qWXZHdZnaF1BCBlpP3
MD5:	548F7476594C65B2D9A44ADBE265DD3B
SHA1:	4D81020E8B908AA93E7BBF9B4727F6F4EE2EA264
SHA-256:	C6AF5658B1289EA4A6A4A33E9CD9BFB885277974F2741F5D2EDC54DF3F3F340B
SHA-512:	3015496AA8DB2EEF81C8B3E35CE453A080293518DE509B6B9D2BC4BA83C58FE0E33A114D12F94387F70DF3C92D62C27F650090FE2B4923706581A26245B5A4D5
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
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..?I....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):	3.1084656046114056
Encrypted:	false
SSDEEP:	6:kKkahk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:h9kPlE99SNxAhUeYlUSA/t
MD5:	F265C930EF44E6ACBA853DC0EF3CCA52
SHA1:	98DBD62394E3FAD572DEAABAD08BF56A2F355F03
SHA-256:	A51CCED759A41167FA135BF13E26467986C030908DB1B708157F0BD073DA6EDD
SHA-512:	78A8EB17A923CC0C607BB055AD87B3979E992A165A324E1ABD09BAB284A57B30686C21879DC90C9389EA7F771D8B5AA5767FF5B890DEB6C5B7A631530934D73
Malicious:	false
Preview:	p..... .....(..w...(..... .....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\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.23652836958112
Encrypted:	false
SSDEEP:	12288:Al/ULFzTnZ67Hr5Kem9F7r66iL9Cvdq6KsqEFm4OrTkkiyrI:y/ULFzTnZ6br5K33i
MD5:	0F7E9389B8352594A1D1DA63202D5E76
SHA1:	B8D01D1CAB800DBB068758A3FDA30883C526A6B3
SHA-256:	C688CB041A1A6F2729B4E4EDBACD0CDC07632B2136EF3D45501BEB791B1D9620
SHA-512:	4B3AAE60BEA27A4586D32A6C4F63D490BA206EFA136C5792A598756B929EDC42F7B384A068CB3FB653DEE7EB83CF454F20FA5C6AE4BB8719BDD14051E38929(B
Malicious:	false
Preview:	regfH...H...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.]..w..... ....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.7219597294472537
Encrypted:	false
SSDEEP:	384:z8f5K5lcv4KgnVVeeDzei1NKZtjaT8GRFwWno:QhK+g/eeDzesNYtjnGRFwW
MD5:	E0EE0560CE5C8770F5E1AE82080874B1
SHA1:	DBB38E3F880FC4E4EC56BBDA55EB1E633C274E75
SHA-256:	35AE4F85D7E0B29E096DB29EAF98B81BE8536CF0734CEDDD3847B7CC5D65DD7A
SHA-512:	7A6C835174199EA9864D4FF672FD07F707B87CF29D280FD1F0CD4B9DA043021D488B1868BDAD3EBB6E847D10B3435F077D445EFE1220BF8F9C26E98CB8503AE
Malicious:	false
Preview:	regfG...G...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.]..w..... ....HvLE.>.....G.....?.G...7...N_.M.....hbin.....p.\.,.....nk,...w..... .....&...{ad79c032-a2ea-f756-e377-72 fb9332c3ae}.....nk ....w..... ....Z.....Root.....lf.....Root....nk ....w..... .....*.....DeviceCensus..... vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	
Entropy (8bit):	6.767616444278102
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 98.32% • Windows Screen Saver (13104/52) 1.29% • 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:	YBfn5E3Dlw.dll
File size:	588288
MD5:	038f9a9d5b96733a9b3030cfbe4e4535
SHA1:	3b8a4b81f0b06514188e4f935d5f4b0858b93806
SHA256:	d46762ba155e3345baf5d9e9453e6cd8e0647438693abddf34f98ae8d6bd436a
SHA512:	3f9aea01963c0d9daa7739277fea7af2b3fe86c41a211fb73b2a35e9506856da91bc334a7c4e63ae83094fe696a8b45e8e5050240a1545e5f891fa4c22512671
SSDEEP:	6144:cNU5LwA22222GgngDrDRVyYli/ci2tEGW78ODQiERtvOSk5DKXOW14lkFxVFgY4E:x5w7YM/cYVV7EWOpOJyvnHtytFyQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.....^F.....^P.n....^W.t....^Y.....^A.....^G.....^B.....Rich.....PE..L..

File Icon

Icon Hash:	71b018ccc6577131

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-19:50:18.278585	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49790	80	192.168.2.4	45.138.98.34
01/14/22-19:50:19.639317	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49791	8080	192.168.2.4	69.16.218.101

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6260 Parent PID: 5916

General

Start time:	19:49:43
Start date:	14/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\YBfn5E3Dlw.dll"
Imagebase:	0xef0000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.680031217.0000000002AE1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.703964616.0000000002AB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.679124499.0000000002AE1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.704266978.0000000002AE1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.679046535.0000000002AB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.679999425.0000000002AB0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 2240 Parent PID: 6260

General

Start time:	19:49:44
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\YBfn5E3Dlw.dll",#1
Imagebase:	0x11d0000
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: regsvr32.exe PID: 5396 Parent PID: 6260

General

Start time:	19:49:44
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\YBfn5E3Dlw.dll
Imagebase:	0xcf0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.670153557.0000000000C61000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.670105180.0000000000980000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6072 Parent PID: 2240

General

Start time:	19:49:44
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\YBfn5E3Dlw.dll",#1
Imagebase:	0x12f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.670630923.0000000001270000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.670654175.00000000012A1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 1320 Parent PID: 6260

General

Start time:	19:49:45
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YBfn5E3Dlw.dll,DllRegisterServer
Imagebase:	0x12f0000
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: 00000004.00000002.717791244.00000000047B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.717740715.0000000004780000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.716834900.00000000011C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.716329937.0000000000B21000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.717660130.0000000004720000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.715971380.00000000004F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.716952958.00000000011F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.717702240.0000000004751000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6436 Parent PID: 5396

General

Start time:	19:49:46
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\YBfn5E3Dlw.dll",DllRegisterServer
Imagebase:	0x12f0000
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: 4180 Parent PID: 6072

General

Start time:	19:49:46
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\YBfn5E3Dlw.dll",DllRegisterServer
Imagebase:	0x12f0000
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: 00000007.00000002.684992268.0000000003450000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687871792.0000000005661000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687254093.0000000005501000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.686420197.00000000053F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688080295.0000000005690000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687539122.0000000005630000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688465307.00000000059F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688659098.0000000005A21000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688152191.00000000056C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.686930115.00000000054D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.685377727.0000000003601000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.686624450.0000000005421000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: svchost.exe PID: 6888 Parent PID: 568

General

Start time:	19:49:50
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
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: WerFault.exe PID: 5628 Parent PID: 6888

General

Start time:	19:49:50
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6260 -ip 6260
Imagebase:	0xd70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6500 Parent PID: 4180

General

Start time:	19:49:51
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Dfktehrjwgeevy\pakqi.bja", rArKTBwXKBsr
Imagebase:	0x12f0000
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.00000002.687070469.0000000000B50000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.687321793.0000000000B81000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: WerFault.exe PID: 6552 Parent PID: 6260

General

Start time:	19:49:52
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6260 -s 552
Imagebase:	0xd70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 6664 Parent PID: 6500

General

Start time:	19:49:53
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Dfktehrjwgeevy\pakqi.bja", DllRegisterServer
Imagebase:	0x12f0000
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: 1368 Parent PID: 568

General

Start time:	19:50:07
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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: 5416 Parent PID: 568

General

Start time:	19:50:31
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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: 7132 Parent PID: 568

General

Start time:	19:50:44
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Disassembly

Code Analysis