ID: 553359
Sample Name: nIQCsrVbbw
Cookbook: default.jbs
Time: 18:58:28
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

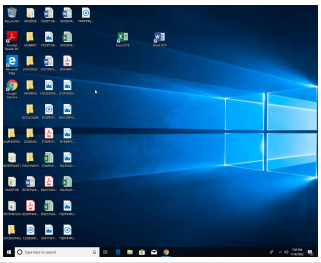
Windows Analysis Report nIQCsrVbbw

Overview

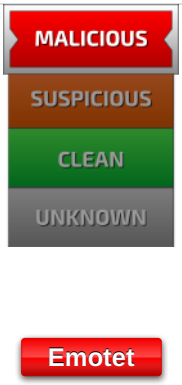
General Information

Sample Name:	nIQCsrVbbw (renamed file extension from none to dll)
Analysis ID:	553359
MD5:	06b75d254c6844..
SHA1:	af4b4dccf317dbe..
SHA256:	b0e46325319e75..
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection



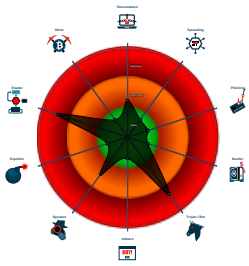
Emotet

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…
- Uses 32bit PE files
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Deletes files inside the Windows fold…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6748 cmdline: loaddll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6764 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6784 cmdline: rundll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 2484 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6772 cmdline: regsvr32.exe /s C:\Users\user\Desktop\nIQCsrVbbw.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 6844 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6816 cmdline: rundll32.exe C:\Users\user\Desktop\nIQCsrVbbw.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4872 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Uibizbzyxusffon\lvdcgmwj.xbl",PtnVsXFQteN MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6012 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Uibizbzyxusffon\lvdcgmwj.xbl",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 6632 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6748 -s 512 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 7056 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2920 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1768 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 3876 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 476 -p 6748 -ip 6748 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6636 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6980 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7080 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2064 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s BITS 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": [
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW",
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.361373048.0000000000881000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.369867351.0000000005381000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.306596758.0000000003330000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.376038820.000000000D51000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.369320365.00000000051C1000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.4860000.8.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.1140000.2.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.3330000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.5380000.9.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.51c0000.5.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 44 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:

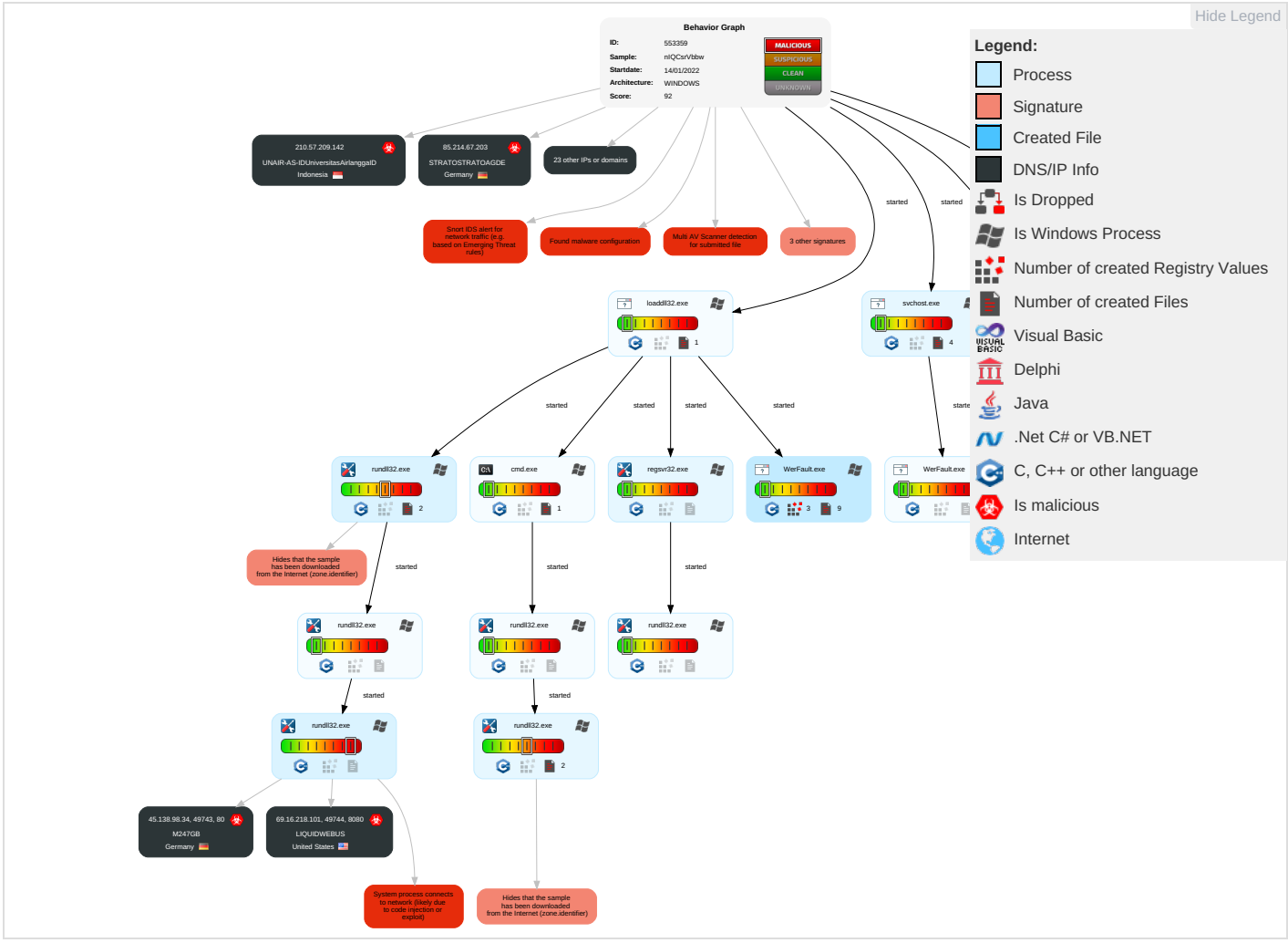
Yara detected Emotet

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 3 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Security Software Discovery 5 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	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

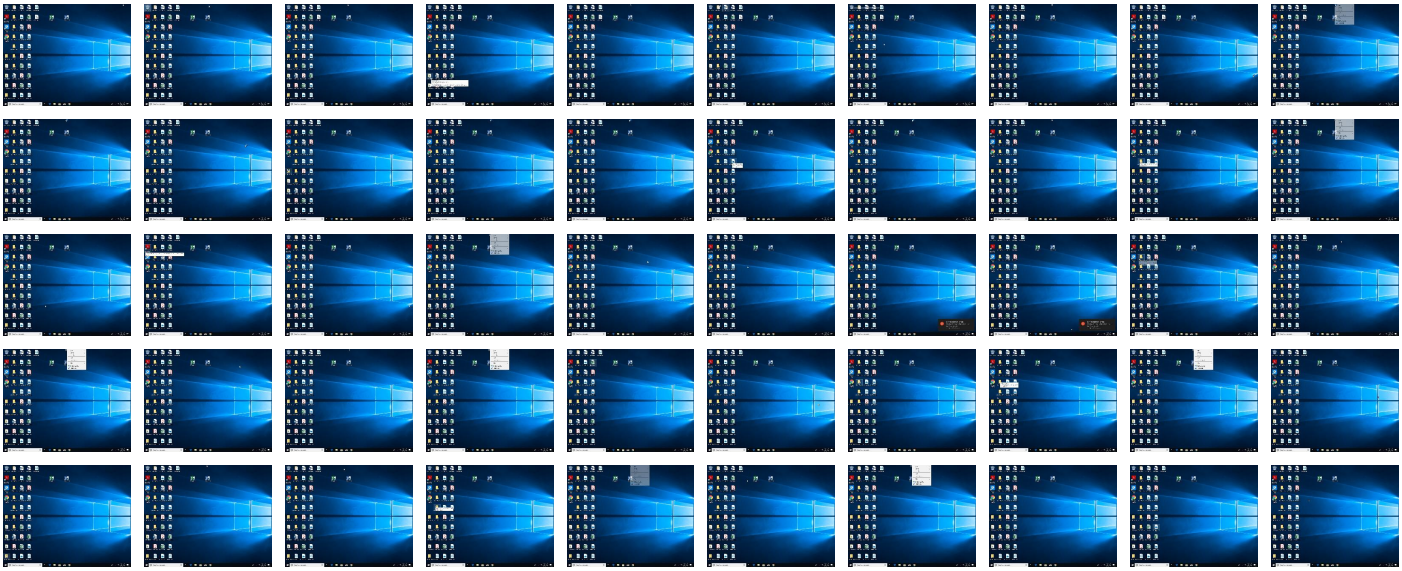
Behavior Graph



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
nIQCsrVbbw.dll	16%	Virustotal		Browse
nIQCsrVbbw.dll	16%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.d00000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.2.loaddll32.exe.d50000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.11d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.5380000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.51c0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.3410000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.12a0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.1190000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.1390000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.1270000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.d50000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.5320000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.5090000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.loaddll32.exe.d50000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.1140000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.1170000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.5060000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.5350000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.560000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4830000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.7c0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
2.2.regsvr32.exe.3330000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.d00000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.52f0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4860000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.d00000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.4b70000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.4c90000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.880000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.bc0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.5190000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.56f0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.56c0000.10.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/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
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553359
Start date:	14.01.2022
Start time:	18:58:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nIQCsrVbbw (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:	mal92.troj.evad.winDLL@29/14@0/28
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 99.3% (good quality ratio 92.4%) • Quality average: 70.9% • Quality standard deviation: 27.1%
HCA Information:	• Successful, ratio: 80% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:00:45	API Interceptor	9x 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\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24859478426505882
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4l:BJiRdwfu2SRU4l
MD5:	51DC402A9F6C81E0BED7BE8CD9693A66
SHA1:	0860EAFD248F50CE399F8BE75302C69B9AC2186B
SHA-256:	AD6EA2A2ACEB0426A47FA5716F3F8A683FA9C5497ED8B73C9273746BAC5B030C
SHA-512:	BD128F1262BF2AAB7A90E9824DED287F376666D570FEC5714BF74D9BE7B44F22E45AB09825A255AAE7F0CC0564ABD9B7E9DB9FC6F1C36CDDCA23215BCF0AA5F0
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 0xb577f95a, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2506719702516563
Encrypted:	false
SSDEEP:	384:s+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:zSB2nSB2RSjlK/+mLesOj1J2
MD5:	D3944AD90064A7E4584F2DB27C5ADC86
SHA1:	2E44696DFB217829BFF20523DC3B477A0811F074
SHA-256:	934257669376A2690EB42234D498CF5709DFDDA7130025751526D7F382C2B793
SHA-512:	EE003A63F02462D270612ABB17874E8CDC0DC5E3024CE48F5B1E898E480D42305AA7E1A6F796D07FCBD58B18F969266E341DD0A34C494C51FC1E6A82F3AB40D
Malicious:	false
Preview:	.w.Z... .....e.f.3...w.....&.....w.....z..h.(.....3...w.....B.....@..... ....3...w..... .....v.....z.u.....8.3.....z.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07672007947968082
Encrypted:	false
SSDEEP:	3:Wl/ll7EvvyBhI+j8l/bJdAtiGmmhttoll3Vkttlmlnl:2liaBhDj8t4VRhQ3
MD5:	6C470310ECBB4F35FA720C7BC188746B
SHA1:	2C392A6FDBF24BB955C99B1FEB373CA48642D8C5
SHA-256:	B896754FCB6CC2860AABDB82A1AC5DE93ECA2410EA5A3497B0FD38C21A779E66
SHA-512:	3D9C4281529A6DDF4B5DB8721903C37ED4C5587419EC07DEAECF9E1F1B584BA3F380981719D6C52BB0996F2A6D67A86AD441A199C6F8F261B70245F3255E74A
Malicious:	false
Preview:	..E.....3...w.....z.....w.....w.....w....:O....w.....8.3.....z.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_7d3365b34093db6d884642e334bbbe4e6283fce_7cac0383_1858c648\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7987766774476208
Encrypted:	false
SSDEEP:	96:9RrdnYyXy9haol7JfapXIQcQSc6mcEUcw3/s+a+z+HbHgLVG4rmMoVaz2PnmnPej:VnjHsieryj7q/u7saS274ltW
MD5:	030E2D9BBA13D29640FC53D6F406D48D
SHA1:	AA68FC7ECDD6942B61FC27365E34E791BD2ED08F
SHA-256:	B67B89C0D3FA51AB3D8C74CDEE6DB758AB665E338104A154E864C1936481F936

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_7d3365b34093db6d884642e334bbbe4e6283fce_7cac0383_1858c648\Report.wer	
SHA-512:	86ACB807926A2A764A5199C4DD58239C5854E36B954DB8946168C9EEDD111E31B19CB26C9897B2632F7EB6237A35923A731E37BEE9E59E681D56F3DA11A098C
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.=.1.3.2.8.6.6.8.9.2.0.8.5.1.0.3.9.8.3.....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.=.f.a.9.3.b.7.5.b.-.d.4.6.d.-.4.c.b.8.-.9.4.5.b.-.8.c.1.c.1.5.2.3.b.5.3.4.....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.=.a.8.a.9.3.b.3.a.-.a.a.4.9.-.4.9.c.8.-.9.0.3.1.-.b.6.6.6.5.a.c.8.1.1.5.4.....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.a.5.c.-.0.0.0.1.-.0.0.1.c.-.e.8.9.2.-.6.b.e.9.b.b.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\WER44E1.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51348
Entropy (8bit):	3.0619519178684405
Encrypted:	false
SSDEEP:	1536:RnHX0mJFybvGHRd10T2LcYzr1pib0lqtWBKXTdPjQjC:RnHX0mJFybvGHRd10T2LcYzr1Mb0lqt3
MD5:	6B1E58957A41AF1EC4FC58CA70BD59CD
SHA1:	C8412D5B6DE309505D5E562B31460A21A87744C2
SHA-256:	63051A2FC6AC62D918072A5CD2184BE7A278D034871139ED77865C9FAAF787B0
SHA-512:	5F3DC03B5B8EAB0857CEB652D50A4A7F7B386E61DA52B9B56E2969129AA4B4DA44D88399D43444A2318D31C9ED2CC3B7CC8497B4B2B602F4E5C9070BBCF556F8
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\WER48CA.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6947815228058167
Encrypted:	false
SSDEEP:	96:9GiZYWXbIfriyY7YFTWkiH6YEZpmtoijOO+hwjqRaljS9x4kIvv3:9jZDXos+oaaljux4Tvv3
MD5:	45928CC03A93897925D4ED016E93C10C
SHA1:	FCE2AFF07EF67490416298A848BB5E7F99E235A9
SHA-256:	D3006E019A2F2729BFF81B10D0F7CAA814DD6959425E1F4F6BDFE9812AF5D50E
SHA-512:	04530BCAFB114F0005E8F02F2044E5D028EE0D0269B1B2F3CF2B7E8FDA8E1521675B53A1CAD9E53B3C55D865EB1DC13C0716C5AAFC28EF0E3C97346C2CC551A0
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:\ProgramData\Microsoft\Windows\WER\Temp\WERB61B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Jan 15 03:00:09 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	45464
Entropy (8bit):	2.0702878641495355
Encrypted:	false
SSDEEP:	192:g317XMoyAKOuWtzZoPJZ2a2LYw/ZILmCEi7zYGbI0dG4Woq:C7pfuWVZoPGvLYw/eLmXi7zYGbII
MD5:	BD343ADAD03C9995B4EA2C3EB1373745
SHA1:	240981625408A7E4800196D0BED975AE1E97C531
SHA-256:	94000B5C993375C966E713E7886E9CD1B9F018FDA7958DF6959130753E26CB55
SHA-512:	B683B8879B180766802B02E0C94B93D2A28267F602D305FB7A095EE435DB8033D55AD9681C8D94208FD14DA1BFFA620163AE1E3A726639B459A4CB033DCB095A
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB61B.tmp.dmp	
Preview:	MDMP..... .....8.a.....$...T.....%.....`.....8.....T.....x.....d.....U.....B..... ...GenuineIntelW.....T.....\....8.a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .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\WERBC85.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):	8352
Entropy (8bit):	3.699125370720691
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiHR6HRbx6YF8SURbgmfzSwGmCpBh89bvmsftFm:RrlsNix6xbx6YeSURbgmfzSwTvFfO
MD5:	DA7CFC33DFCE8DABA83C4EA42ADF32C6
SHA1:	63D2E474088C182A4711071B217918858C89EA71
SHA-256:	95967CA4FB21A290203A7574A307999BDE48EC81A80D9C1EBEBB427EC77A6436
SHA-512:	EDC65F6F32A9DBE2BAB9D3C3D3E3A166FD47F8FAC68700FE3CABF7F6BD1261D0A45CF765037197ACCBA9343549B9CA0AA70A97ADF78A3422C13E75B766640 8E
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.>.6.7.4.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF45.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):	4.471806726263325
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRJgtWI9gjeWSC8BU8fm8M4J2+WZF1+q84pvEKcQIcQw0cQd:uITfjHjfSN3JAx5EKkw0fd
MD5:	662A1A367461BA31DB23340401FD97AB
SHA1:	523C2303A37800C0E8A73B16DC5EE89FA379130E
SHA-256:	917F8CDCF7BF4FDAC65412CFBE5C28FBE72D4D28A2B8E48E8712252A697CC62C
SHA-512:	16A4238C54AC27E4719D0900BCCB823D38A882CE07E42B0BD21DE4A7902A20E0515FA3D0BE11BEDAAFA21FAD4C77D0BD2FA5B46683239EFC113EBE51572A1 A0
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="1342810" />.. <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:\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):	3.1244568012511515
Encrypted:	false
SSDEEP:	6:kKu0k8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:209kPlE99SNxAhUeYlUSA/t
MD5:	7F09ADF005426F52A243F8841E74EFE3
SHA1:	DBF5C90A9BBAE8BFA3C60F2F1B7E0B4C58254C71
SHA-256:	C3D2BE8AB9CD6874A1D13CCAFCEB3FE354986399118D9756427EB9C40DE192FC
SHA-512:	90D651BBDD3482441168A16CE9318BE8936D24C43A46BD9B15CB20D7BF6D5EE7E699110F4578CDDF55F7C05B36D4AA26751E11CA87C3C355836F321D7E3FA3(B
Malicious:	false
Preview:	p..... .....}9.....(..... ....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
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA(A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

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):	4.264668857187777
Encrypted:	false
SSDEEP:	12288:352KJvR+Eb3Bmgn1HZfkx3kDKj64WZpJYZE7Yc7GpqP4BxzSq/bdL:p2KJvR+Eb3BmgnTo
MD5:	E6298D490A541EF8F687C9FE5B0DFC20
SHA1:	AC6036A760334F24CBC3B7FECC0C9102778FB889
SHA-256:	D39DE5CA4FB67686131204CFB251D3C5DA07CA486AC985C85C4548D527B33660
SHA-512:	AED007A7A5970462C141C11BEB66F0A4D60581FDC928E945EAFAC86700C540F8D8B49BDD3407EB222A610956B3700DA06312744C22C54C8ED865F301969597FE
Malicious:	false
Preview:	regfZ...Z...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.rmtmf]h..... ....c]..... .....

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):	3.3825589105427794
Encrypted:	false
SSDEEP:	192:Y9wUv1du5m0KCYO5FSEsWftx19xgoJ4XSaJNSdkyFn6yvRrsfmWfYjdsiDoXzCF:Ojw5Rftx19PJ4XS7FFn7RZd1DoXzCF
MD5:	B55740C905DEDF938ECE9AA720F2D7AF
SHA1:	8AAAF759CF0C4BE4B0F7EBC792C35397A58A33BD
SHA-256:	2D1F3529349467CCF6270C3D0955E5371A66958620B99777B362F22AC547A828
SHA-512:	5047D80FA3EBFCB5BB948803F15E22537B93C01B72B67CFDF39FBB47AFBC653CD78EEAAD43C368B5DEFCD04A43DE1440C5CC250F08850291C5F544EFBA97C 40
Malicious:	false

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Preview:	regfY...Y...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.rmtmf]h..... ....c]HvLE.>.....Y.....(.Z...=....1.....0.....hbin.....p.\..,.....nk,..j..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..j..... ....Z.....Root.....lf.....Root....nk ..j.....}..... .....*.....DeviceCensus..... vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.767603370761852
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:	nIQCsrVbbw.dll
File size:	588288
MD5:	06b75d254c6844f78c7d7eefa5b1243e
SHA1:	af4b4dccf317dbeeab97868a9514a7c9e496c8d3
SHA256:	b0e46325319e75a2490a73045a60030961851c07d266df73d7e048799e133ec7
SHA512:	afe13aee5ffa87d65a2d39a2b9aae1fcbc222e843497bf00744d82a543078235a4d648b78a9e66142d952650bb36ca319176ec445346e4ed4aef59fd7dd5200
SSDEEP:	6144:cNU5LwA22222GgngDrDRVyYli/ci2tEGW78ODQiEJtvOSk5DKXOW14IkFxVFgY4E:x5w7YM/cYVV7EOOpOJyvnHtytFyQ
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

Static PE Info

General

Entrypoint:	0x1002eaac
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x61E03DE6 [Thu Jan 13 14:57:42 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	7f57698bb210fa88a6b01b1feaf20957

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x45bb9	0x45c00	False	0.379756804435	data	6.37093799262	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x47000	0x9c10	0x9e00	False	0.357397151899	data	5.22179618791	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x51000	0x3735c	0x33800	False	0.741035535498	data	6.11335979295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0x3410	0x3600	False	0.306640625	data	4.34913645958	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8d000	0x8c34	0x8e00	False	0.346308318662	data	4.00973830682	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-19:00:14.694584	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49743	80	192.168.2.3	45.138.98.34
01/14/22-19:00:15.994724	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49744	8080	192.168.2.3	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: 6748 Parent PID: 4636

General

Start time:	18:59:28
Start date:	14/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll"
Imagebase:	0x1220000
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: 00000000.00000000.376038820.0000000000D51000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.379371136.0000000000D51000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.397131962.0000000000D00000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.376003738.0000000000D00000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.379329782.0000000000D00000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6764 Parent PID: 6748

General

Start time:	18:59:29
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\nIQCsrVbbw.dll",#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 6772 Parent PID: 6748

General

Start time:	18:59:29
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\nIQCsrVbbw.dll
Imagebase:	0xae0000
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: 00000002.00000002.306596758.0000000003330000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.306669964.0000000003411000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6784 Parent PID: 6764

General

Start time:	18:59:29
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll",#1
Imagebase:	0x13c0000
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: 00000003.00000002.361373048.0000000000881000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.359468675.00000000007C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6816 Parent PID: 6748

General

Start time:	18:59:29
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nIQCsrVbbw.dll,DllRegisterServer
Imagebase:	0x13c0000
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: 00000005.00000002.368368956.0000000004831000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.367128450.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.367810302.0000000001270000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.367757114.0000000001171000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.368438775.0000000004860000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.367845396.00000000012A1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.367713608.0000000001140000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.367919454.0000000001390000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.367465277.0000000000BC1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6844 Parent PID: 6772

General

Start time:	18:59:30
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\nIQCsrVbbw.dll",DllRegisterServer
Imagebase:	0x13c0000
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: svchost.exe PID: 7056 Parent PID: 572

General

Start time:	18:59:42
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 2920 Parent PID: 572

General

Start time:	18:59:53
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 2484 Parent PID: 6784

General

Start time:	18:59:53
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\nIQCsrVbbw.dll",DllRegisterServer
Imagebase:	0x13c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.369867351.0000000005381000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.369320365.00000000051C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.370265294.00000000056C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.369446130.00000000052F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.368922473.0000000004B71000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.369147966.0000000005060000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.370426063.00000000056F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.369281669.0000000005190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.369637751.0000000005350000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.368222308.00000000011D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.369552219.0000000005321000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.369203622.0000000005091000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4872 Parent PID: 6816

General

Start time:	18:59:58
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Uibizbzyxusffon\lvdcgmwj.xbl",PtnVsXFQteN
Imagebase:	0x13c0000
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: 0000000D.00000002.370663067.0000000001190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.376060277.0000000004C91000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6012 Parent PID: 4872

General

Start time:	19:00:00
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Uibizbzyxusffon\lvdcgmwj.xbl",DllRegisterServer
Imagebase:	0x13c0000
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: svchost.exe PID: 1768 Parent PID: 572

General

Start time:	19:00:01
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: WerFault.exe PID: 3876 Parent PID: 1768

General

Start time:	19:00:02
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 476 -p 6748 -ip 6748
Imagebase:	0x1120000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 6632 Parent PID: 6748

General

Start time:	19:00:06
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6748 -s 512
Imagebase:	0x1120000
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: svchost.exe PID: 6636 Parent PID: 572

General

Start time:	19:00:06
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6980 Parent PID: 572

General

Start time:	19:00:27
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 7080 Parent PID: 572

General

Start time:	19:00:41
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 2064 Parent PID: 572

General

Start time:	19:01:09
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis