ID: 553359
Sample Name: nIQCsrVbbw.dll
Cookbook: default.jbs
Time: 19:14:26
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

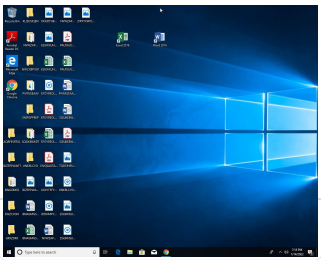
Windows Analysis Report nIQCsrVbbw.dll

Overview

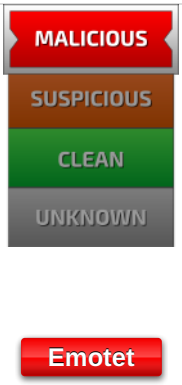
General Information

Sample Name:	nIQCsrVbbw.dll
Analysis ID:	553359
MD5:	06b75d254c6844..
SHA1:	af4b4dccf317dbe..
SHA256:	b0e46325319e75..
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

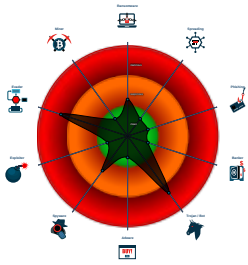


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- 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…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7120 cmdline: loaddll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 4892 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5580 cmdline: rundll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 7040 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 3100 cmdline: regsvr32.exe /s C:\Users\user\Desktop\nIQCsrVbbw.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 6716 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nIQCsrVbbw.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6504 cmdline: rundll32.exe C:\Users\user\Desktop\nIQCsrVbbw.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3604 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gwwrzypqggddo\faunqcxbnkzdy.fxb",DpwIzoKqIHOYx MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 3396 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Gwwrzypqggddo\faunqcxbnkzdy.fxb",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 5444 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7120 -s 512 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4000 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 4664 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 484 -p 7120 -ip 7120 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5884 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2504 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7076 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6432 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
0000000B.00000002.692416013.00000000054F0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.318376552.0000000004F91000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.322328065.0000000002D20000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.692912261.0000000005AA0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.693049451.0000000005B80000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 55 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.4d20000.4.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.5d80000.18.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.4d80000.4.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.5aa0000.14.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.4ee0000.6.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 85 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

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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:

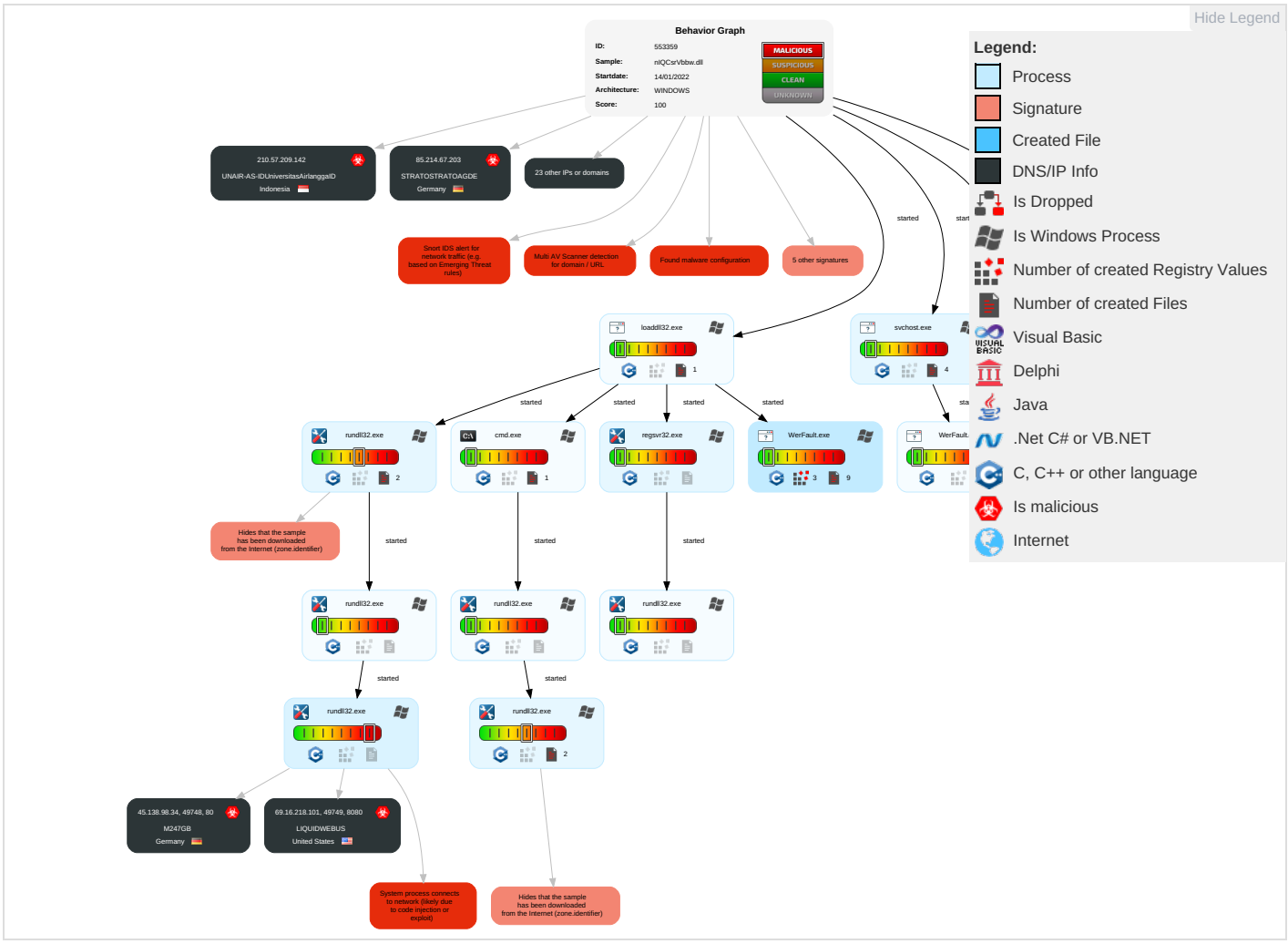
Yara detected Emotet

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 1	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 1	Exfiltration Over Bluetooth	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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
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

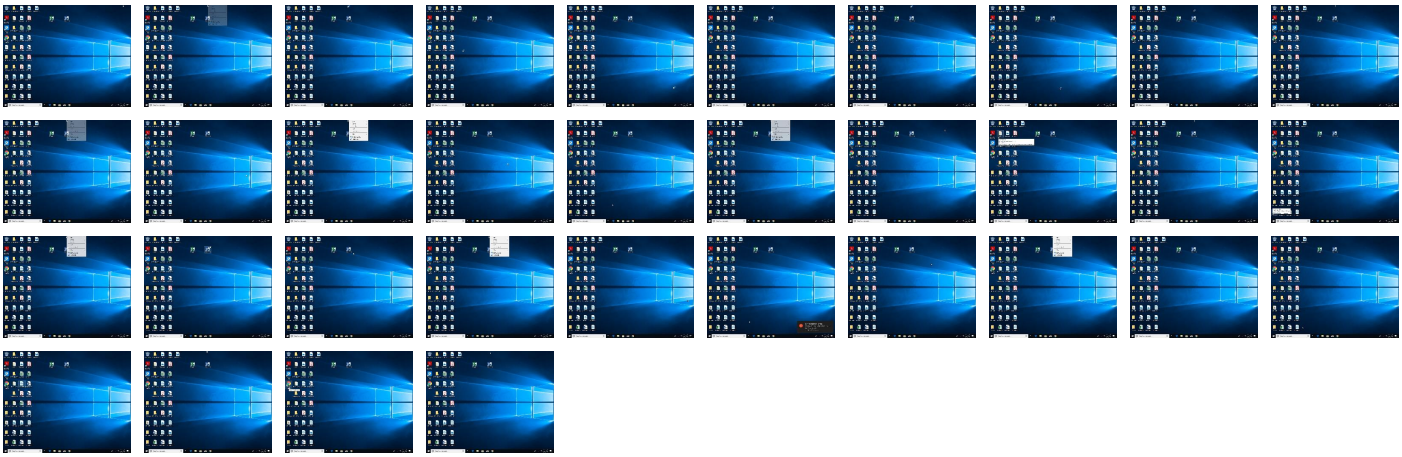
Behavior Graph



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

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.rundll32.exe.4ee0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5aa0000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
1.0.loaddll32.exe.2980000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5680000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.52b0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4f60000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.4c40000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.4c70000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.4580000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.4d80000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.4480000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5bb0000.17.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.2980000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2d20000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.56b0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.51f0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.4f40000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5d80000.18.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.2e20000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.5320000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.2eb0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5db0000.19.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.59c0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.52e0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.4f70000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5410000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.6000000.20.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.5350000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.4d50000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5ad0000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.3280000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4d20000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
1.0.loaddll32.exe.27a0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.46c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.4c80000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.51c0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4f90000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.dd0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4700000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.4c70000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.4c50000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.2d20000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.6030000.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.4c40000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
3.2.regsvr32.exe.4930000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.4f10000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.4f00000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4f30000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.27a0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.4db0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5650000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.54f0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5b80000.16.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5440000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.56e0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.loaddll32.exe.27a0000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.32b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5520000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5990000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
1.0.loaddll32.exe.2980000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		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://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://69.16.218.101:8080/GBwdsVvnKKEsOdMLrBySKnfjLZwMjZtlJDuPNHQIXAc1	0%	Avira URL Cloud	safe	
http://https://45.138.98.34:80/pzThWGIkVuQKGXKeHBqdbAz#	100%	Avira URL Cloud	malware	
http://https://69.16.218.101:8080/GBwdsVvnKKEsOdMLrBySKnfjLZwMjZtlJDuPNHQIXAc	0%	Avira URL Cloud	safe	
http://https://45.138.98.34/	11%	Virustotal		Browse
http://https://45.138.98.34/	100%	Avira URL Cloud	malware	
http://https://69.16.218.101:8080/GBwdsVvnKKEsOdMLrBySKnfjLZwMjZtlJDuPNHQIXAcY	0%	Avira URL Cloud	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://69.16.218.101:8080/GBwdsVvnKKEsOdMLrBySKnfjLZwMjZtlJDuPNHQIXAcDk6	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://69.16.218.101:8080/GBwdsVvnKKEsOdMLrBySKnfjLZwMjZtlJDuPNHQIXAcDk7	0%	Avira URL Cloud	safe	
http://https://69.16.218.101/X.	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://69.16.218.101/	0%	Avira URL Cloud	safe	
http://https://45.138.98.34:80/pzThWGIkVuQKGXKeHBqdbAz	100%	Avira URL Cloud	malware	

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553359
Start date:	14.01.2022
Start time:	19:14:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nIQCsrVbbw.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@27/10@0/27
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 98.3% (good quality ratio 90.6%) • Quality average: 69.3% • Quality standard deviation: 27.6%
HCA Information:	• Successful, ratio: 76% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

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_7d3365b34093db6d884642e334bbbe4e6283fce_7cac0383_14c0c43b\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):	0.798561029081837
Encrypted:	false
SSDEEP:	96:MFHnYyNy9haol7JfapXIQcQSc6mcEUcw3/s+a+z+HbHgLVG4rmMoVazWbSmEBFdJ:0n5Hsieryjbq/u7sBS274ItW
MD5:	47C2236FC7F7FD33768FF717485077EB
SHA1:	324F37B4BEEACEF393D3A17CE93CF532EC4ADC11
SHA-256:	03DD114B8DD767BD30BCAEC649F2F1F9D3955C99237012C1500B926831CA5D3D
SHA-512:	5EBE95C9396B209625AA4EBEBDEB801E37DA2BC78DCF4EE732AFA22D4B693FC0B02DD00106C6F17ADA03CA8260613C338703EAFBCA6093A22CA3A57D3071E46E
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.=.1.3.2.8.6.6.9.0.1.3.9.1.0.5.9.8.1.1.....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.=.4.3.1.1.8.3.9.7.-.1.8.d.2.-.4.a.d.d.-.a.e.d.0.-.b.2.3.a.6.f.c.f.4.c.c.0.....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.=.e.3.f.3.f.c.9.f.-.e.6.5.d.-.4.7.d.3.-.8.d.3.3.-.e.2.c.c.1.7.b.8.c.7.9.8.....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.b.d.0.-.0.0.0.1.-.0.0.1.c.-.7.9.f.6.-.c.6.2.3.b.e.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\WERAAA8.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Jan 15 03:15:40 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	43080
Entropy (8bit):	2.1584854924947634
Encrypted:	false
SSDEEP:	192:pz6BYXiODmYgXplWK4BTD4Tow/5XtmBu4JPKLh1tYrJzT0:JDrImVDw/59mB/PKLt8H
MD5:	71B4C5580B40320A438CFD5FB6318F90
SHA1:	D36630F59F017522FAFA589E0E16E188CAD51E1B
SHA-256:	18DD7914A802132AB3588CEB3B6D018D2E21C3A90B271C1CC59ED4051952A956

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAAA8.tmp.dmp	
SHA-512:	D1E868107DD761437CB82140CAC5022EBB997C88C639330828093CFE3E010AE8C319701499CA693A48B93AC0EA2FA42929704F5BAF0184D17AA832CFB25D22F
Malicious:	false
Preview:	MDMP..... .....\<.a.....$...T.....%.....`.....8.....T.....x.....d.....U.....B..... ...GenuineIntelW.....T.....M<.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\WERB279.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):	3.6991800277798528
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWo6V4jO6YF6cSU2SegmfzSwGiiMCpBd89bf4sfmVm:RrlsNiB6V6O6YzSU2SegmfzSw7iMfrfl
MD5:	90B5BE2F43F15777EB8F5679E2D1ED90
SHA1:	7B32AECF5B9A00734A6819DC3DC5C3642723B061
SHA-256:	B9A979479D191E484C34A2F5DDFFEAFBA1F432ED358D6E1B31C5B68BEFAFEFC8
SHA-512:	CF2F9F9EAA4B480CD420C8324707E4D1194A7DAD9C06BC6370608D5D77659CB4E6C5E54839886FE40D5103A161E4982189EED985614407658709F099B64A607C
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.>.7.1.2.0.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB856.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):	4.472677854908915
Encrypted:	false
SSDEEP:	48:cvIwSD8zsYJgtWI9zeyWSC8BNe8fm8M4J2+WZFcKY+q84pvfWKcQIcQw0kd:uITfeMeTSNnbJAoKY5OKkw0kd
MD5:	604B8C9DCC9B9E290D1D0DF60E50775B
SHA1:	126AC935B694F4056DDE1FC149A0FF553E4A3EBA
SHA-256:	02DFC7906EC712185A60370C253A67F706299AEAF3D8E249B6A77B2F6C248DE9
SHA-512:	804A53955B8B9852D0E3A668193F3D668C319FC4B01CB2B3EE9D1C4573D92C73817A6366D67DA5F6242CD7ABF80B78E39A0899BF1D85CB0ABFA7FD76F9567F8
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="1342826" />.. <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\WERF34C.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54416
Entropy (8bit):	3.0483272458121204
Encrypted:	false
SSDEEP:	1536:OGHf1ARrE94Mc+knmQQHZUsbfnQ2zZP/FseyFX:OGHf1ARrE94Mc+knmQQHZUsbfQ2zZP/G
MD5:	AC6216F35194ED9F55807A18231C72AD
SHA1:	67635A1B75DC59A28B32D6AB995952FBEBD7D505
SHA-256:	984846E6359246613180B05172F4A3FC0C6CDBD7E6EDA1941EC4802E7D8A8E77
SHA-512:	DF12C51D92333EC75D08268FE1398CA9A5D9D14C430F7ADFB6C43D25271B262E2C752E21AFC68FE7D0CD27C355D18A2C7C091D341196DD5425A1B86B6A3122
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\WERFCB3.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	modified
Size (bytes):	13340
Entropy (8bit):	2.6951828158862896
Encrypted:	false
SSDEEP:	96:9GiZYWC28QIY3YrWoniHc2YEZbNtk0iNOJnIwgFaHtVa5qXZyJIUP3:9jZDqwq6gAHXa5qXZy2UP3
MD5:	245D6B6A0941C49EF44FD9032DDC5A3E
SHA1:	12FF2B0A655C324810D4D0F33B231415F1530B00
SHA-256:	0CDF58E4D753E0BC759A2C218AC292EE6B6C8D8F63A55B0AD20764CC6253B08B
SHA-512:	F75E5E3711B0EDD89D929A999F8FAD6F94D20F61D8EDA2060B80DA072778F6D6016A00D61C353217B5298FB8E645F06624C1E2695242E6956591EF01E96C2D5C
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
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.l..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.........N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F..._..z....._...gY..!Z..?l....vp.l.:.d.Z..W.....~...N.._k...&.....$......i.F.d.....D!e.....Y..,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1122616792999316
Encrypted:	false
SSDEEP:	6:kKqk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:y9kPlE99SNxAhUeYlUSA/t
MD5:	C7310ED6A35F0A29E56D62EC65202D14
SHA1:	C0A8D240D5D0EC262CA4730912C319CCB2E50325
SHA-256:	7D6E9CC48DB506283A5F874F529584E3B4797E838B42A8D0853B5DAE4AF058DE
SHA-512:	C5E1299AF504A3F8011486A4BABB8E42C83B4CFFF45D4885C2DA06407163228CA4B95976F0E479CF2989D499C1E06B682FD9E7710B4C52D057266B0364294D81
Malicious:	false
Preview:	p..... .....3....(..... .....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):	4.2704532755425335
Encrypted:	false
SSDEEP:	12288:ieoCpD9D8UfLZ4HkpM7UciLqbrZxV5uVBtgeMNjXlmm4pFXW/mm91:PoCpD9D8UfLZ4Hw8
MD5:	3B45DA502DAB998978618A4F00F4AED7
SHA1:	0CAF7FCB6AF81676CB12AD9478C9A06DD5092907
SHA-256:	AAD5608AD5C838E8F57507D8805B638DAA47B21E7FFE0798C202B9793631F9F2

C:\Windows\appcompat\Programs\Amcache.hve	
SHA-512:	86063FAB9F77DE3B9D15D4F341DA4BDFF90F18843DD5B5B1D7A21CC8D2B80FD131D7C63BC29BF3739EC514EF682CA5F39B2959A5E4F14F5E23BFBA6774A1A0F7
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.rmtm.t.*..... .....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):	3.395491222878325
Encrypted:	false
SSDEEP:	192:Q04s91RaJ6A+KYR5FSEsWftx1gxgoJ4X7aJNSdkyFn6yvRrsfuWfYjdsiDoXzCv:7jJ5Rftx1gPJ4X77FFn7xZd1DoXzCv
MD5:	7EC880F71B2856F603D1F6E3003FF20E
SHA1:	84AE43885AF4178D7AAF9E04C923D048FEF8E86B
SHA-256:	3A317BB8611AB523EA59949CF09F5266F0DA421312DEEBEE5D96EE1AF68571B1
SHA-512:	70E9665AAFEBBEA359B27F4E3DC8C4AD97D4085B71A9A47549D00664BB0F80AD220465F0B178B28552CDBB5CEAEAE2E4856C995F63ACBC929C3237C07C28CEA9
Malicious:	false
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.rmtm.t.*..... ....wHvLE.>.....Y.....L.....t..z.....0.....hbin.....p.\..,.....nk,..t.*.....h..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..t.*..... ....Z.....Root.....lf.....Root....nk ..t.*.....}..... .....*.....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: 7120 Parent PID: 5788

General

Start time:	19:15:25
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:	0x1020000
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: 00000001.00000002.340184392.0000000002981000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.313088625.00000000027A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.313923443.00000000027A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000002.340127468.00000000027A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.314281816.0000000002981000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000001.00000000.313185864.0000000002981000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4892 Parent PID: 7120

General

Start time:	19:15:26
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: 3100 Parent PID: 7120

General

Start time:	19:15:26
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:	0xff0000
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: 00000003.00000002.304136320.0000000004931000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.303858298.0000000000DD0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5580 Parent PID: 4892

General

Start time:	19:15:26
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:	0xb80000
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: 00000004.00000002.313015794.0000000002D20000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.313073617.0000000002E21000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6504 Parent PID: 7120

General

Start time:	19:15:27
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:	0xb80000
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: 00000005.00000002.318376552.0000000004F91000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318188927.0000000004C71000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318296344.0000000004F00000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318566617.0000000005320000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318521400.00000000051F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.317820038.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318320563.0000000004F31000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318160754.0000000004C40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318025809.0000000004701000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318347085.0000000004F60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318598439.0000000005351000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318240143.0000000004D51000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318218247.0000000004D20000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.318476243.00000000051C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6716 Parent PID: 3100

General

Start time:	19:15:28
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:	0xb80000
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: 7040 Parent PID: 5580

General

Start time:	19:15:28
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:	0xb80000
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: 00000007.00000002.319220718.0000000004C50000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.319469836.0000000004F11000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.319637287.00000000052B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.318877954.0000000004580000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.319268493.0000000004C81000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.319350113.0000000004DB1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.319315094.0000000004D80000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.319560099.0000000004F71000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.319417804.0000000004EE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.319512030.0000000004F40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.319678344.00000000052E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.319057129.00000000046C1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 4000 Parent PID: 572

General

Start time:	19:15:31
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
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 4664 Parent PID: 4000

General

Start time:	19:15:32
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 484 -p 7120 -ip 7120
Imagebase:	0xac0000
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: 3604 Parent PID: 6504

General

Start time:	19:15:34
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gwwrzypqggddo\faunqcxbnkzdy.fxb",DpwIzoKqIHOYx
Imagebase:	0xb80000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.322328065.0000000002D20000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.322840736.0000000004481000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 3396 Parent PID: 3604

General

Start time:	19:15:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Gwwrzypqggddo\faunqcxbnkzdy.fxb",DllRegisterServer
Imagebase:	0xb80000
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.00000002.692416013.00000000054F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692912261.0000000005AA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.693049451.0000000005B80000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692792483.0000000005990000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692538587.0000000005681000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692564390.00000000056B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692047710.0000000004C71000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692594246.00000000056E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.693077342.0000000005BB1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.693386084.0000000006031000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692022013.0000000004C40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.693354364.0000000006000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692503192.0000000005650000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.691678754.00000000032B1000.00000020.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692337885.0000000005410000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.693231899.0000000005D80000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692973628.0000000005AD1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692836661.00000000059C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.691624077.0000000003280000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692363013.0000000005441000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.693267062.0000000005DB1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.692450211.0000000005521000.00000020.00000001.sdmp, Author: Joe Security

File Activities Show Windows behavior

Analysis Process: WerFault.exe PID: 5444 Parent PID: 7120

General

Start time:	19:15:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7120 -s 512
Imagebase:	0xac0000
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: 5884 Parent PID: 572

General

Start time:	19:15:39
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: 2504 Parent PID: 572

General

Start time:	19:15:51
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: 7076 Parent PID: 572

General

Start time:	19:16:08
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: 6432 Parent PID: 572

General

Start time:	19:16:24
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

Disassembly

Code Analysis