ID: 553353
Sample Name: nV5Wu77N8J
Cookbook: default.jbs
Time: 18:49:15
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

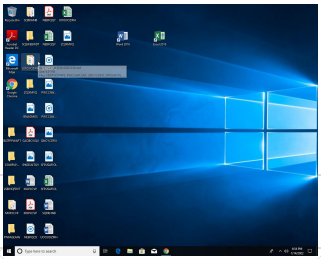
Windows Analysis Report nV5Wu77N8J

Overview

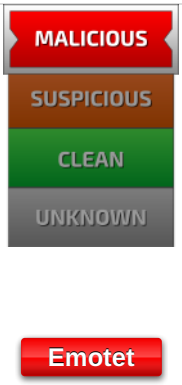
General Information

Sample Name:	nV5Wu77N8J (renamed file extension from none to dll)
Analysis ID:	553353
MD5:	a0306b7a6a1202..
SHA1:	ee7d221826a725..
SHA256:	9b1ca060b5a969..
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

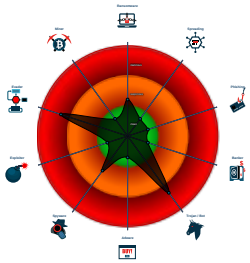


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7128 cmdline: loaddll32.exe "C:\Users\user\Desktop\nV5Wu77N8J.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 7148 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\nV5Wu77N8J.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3296 cmdline: rundll32.exe "C:\Users\user\Desktop\nV5Wu77N8J.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6344 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nV5Wu77N8J.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 7160 cmdline: regsvr32.exe /s C:\Users\user\Desktop\nV5Wu77N8J.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 6192 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nV5Wu77N8J.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6244 cmdline: rundll32.exe C:\Users\user\Desktop\nV5Wu77N8J.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5356 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Bdaefwhkzqb\lrinxnmhyts.ogu",XLurkV MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6040 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Bdaefwhkzqb\lrinxnmhyts.ogu",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 3660 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7128 -s 568 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5672 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6676 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6712 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 7128 -ip 7128 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 808 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7064 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4296 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": [
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW",
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.718929777.0000000003501000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000E.00000002.1188125968.00000000049D1000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000E.00000002.1190726376.00000000059A0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.718904101.00000000034D0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.719243124.0000000005161000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 45 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.rundll32.exe.55b0000.12.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.5030000.4.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.4770000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.53b0000.4.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.de0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 71 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:

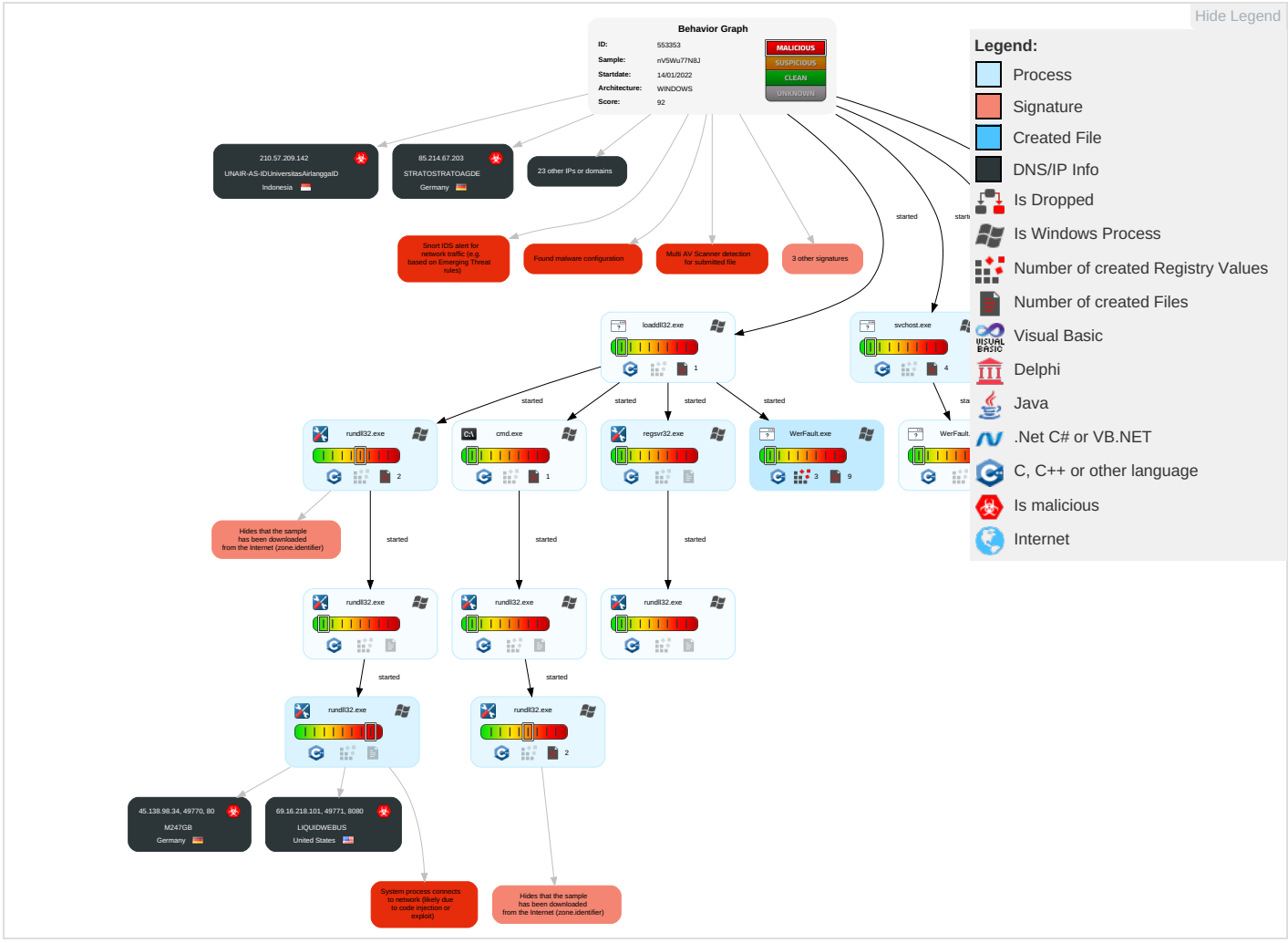
Yara detected Emotet

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 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
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

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 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

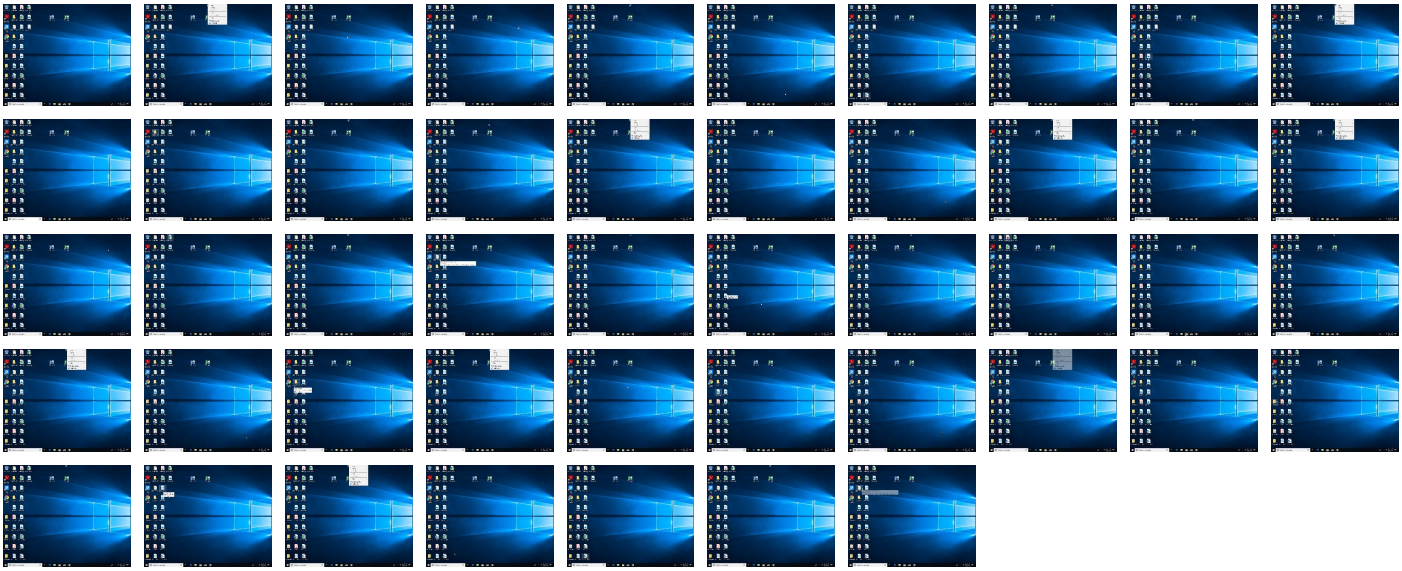
Behavior Graph



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
nV5Wu77N8J.dll	17%	Virustotal		Browse
nV5Wu77N8J.dll	14%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.5030000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.55b0000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.5510000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.53e0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.de0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.4780000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.52a0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.53b0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4cb0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.52d0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.2e30000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.4770000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.loaddll32.exe.de0000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.de0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.e10000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.56f0000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.5570000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.5540000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.49d0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.5a20000.20.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.59d0000.19.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.2510000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
3.2.rundll32.exe.4740000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.4750000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.5300000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.4c80000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
2.2.regsvr32.exe.2540000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.52a0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.55e0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.57a0000.16.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.5a50000.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.57d0000.17.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.52f0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5210000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.3500000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.5140000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.5060000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.5270000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.5110000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.e10000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.49a0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.59a0000.18.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.34d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.5160000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5130000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.52b0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.5270000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.56c0000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.5240000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.2e00000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

No Antivirus matches

URLs

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal

Analysis ID:	553353
Start date:	14.01.2022
Start time:	18:49:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nV5Wu77N8J (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:	27
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@27/10@0/27
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 31.9% (good quality ratio 30%) • Quality average: 74.1% • Quality standard deviation: 26.4%
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
18:51:13	API Interceptor	7x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_12a180e49793e381a8b848106c2e1caa7a6a4277_7cac0383_0ffd4626\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):	0.7958908003747792
Encrypted:	false
SSDEEP:	96:gtrh2nYyay9haol7Jf0pXIQcQSc6mcEUcw3/s+a+z+HbHg1VG4rmMoVazWvMOpNZ:gdunoHsieryjNq/u7seS274ItW
MD5:	CC2ED1887CF43DF87605ACE581A8646C
SHA1:	550A0F8D4875DDE3241376F32EA4319F995E80AA
SHA-256:	2A1C0F968CC272E23942C7A0DE2550330F1D6BAA7B5D7CDB3D0C9EDF63E4704D
SHA-512:	A05A8654EBB4CDEAA2C964D7880CC6640A68CF90BE7EB2CE7110CF774751F2FA6546123E45FF9763CD84B39B5C79B07F085D870C3A4B24F92863B9ECF2B1A7E
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.5.6.2.4.0.2.0.6.0.7.4.9.....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.=.5.7.b.5.1.f.7.2.-.7.4.5.f.-.4.6.c.a.-.9.4.6.d.-.0.f.2.2.d.a.9.f.6.1.f.e.....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.=.8.e.d.6.1.2.2.8.-.d.a.4.6.-.4.e.3.3.-.a.1.3.6.-.9.d.3.d.a.e.5.6.8.a.e.f.....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.8.-.0.0.0.1.-.0.0.1.b.-.0.8.4.5.-.4.1.2.c.6.f.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\WER2F33.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Jan 14 17:50:41 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	44328
Entropy (8bit):	2.1255697233673803
Encrypted:	false
SSDEEP:	192:6vUl/5hbOiYNH+PieACib4nfnzOgPUEYMw/xZUWbKboJyrPun+MN:8biiYH+aaOgTYMw/kWbKboQMN
MD5:	DC01F206F671FB8F58F9AA9658616573
SHA1:	698402D4CB0A56F16C96CC6FF9C7B2CC51C8D6F1
SHA-256:	43038B7DC644076824E4557DE0C176126850EE890D718752E4997773D5948B2C
SHA-512:	5887CCEE773D35B702C9AF1A452D57C7C288A8E63141269152E4556787331FCD37A7B60B7F77E92B740B69409D5416CC87030CCE2E898ED17A5E0901EB784EC
Malicious:	false
Preview:	MDMP..... .....a.....$...T.....%.....`.....8.....T.....(.....x.....d.....U.....B..... ..GenuineIntelW.....T.....a.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.. .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER357E.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):	3.698245170232573
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNieg6HDG6Yr8SUJzzgmfdSwGY+pB289bqHsfBdum:RrlsNix6HDG6YgSUJzzgmfdSwAqMf7
MD5:	7E0377FAAB1AD65AB85DA6CD5994D55C
SHA1:	BAE2C81841F7387CEF5D048B0822AD874695907B
SHA-256:	D187E67B5FFD076BFFCB4C6A7A3C0ACC88655A148F03ADFEDF52B2F2917884CF
SHA-512:	C203C207A0759E8037725128528C0E628973195243726B8FE4A122C3288D821AA40DC2E15BA5DC97CAF5A8110F94EBAFDB8093890785450 27B3EF494F809039C
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER357E.tmp.WERInternalMetadata.xml	
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.>.7.1.2.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER37B8.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54294
Entropy (8bit):	3.065453431295334
Encrypted:	false
SSDEEP:	768:NZHDXSE66uT4rWXV/ZKGzWZXf+tJYRzdvs1sj+nKztt4o:NZHDXruT4rWX1ZKGz2Pz3s1sjmYtt3
MD5:	9349FAC214CA4C81AB05C77F4A2C7D4D
SHA1:	3AAEB9C25AF62BDCC9495E193D9352D5A98454DE
SHA-256:	A5673DCE88CE81C3441A2D16BF605813E6F99D24354F81F24CC9C333E15133CE
SHA-512:	119E25AF4398FEABC300138E337B697DC9AF0DD61D2D9DA2139F227C2C366D35C785896C4C47027421DCB949377989B61AD3BFCBBA1200877C9E91F158D6A81
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\WER380F.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):	4.472230205116493
Encrypted:	false
SSDEEP:	48:cvIwSD8zs3JgtWI9i8WSC8B5T8fm8M4J2+SZFriK+q84pz/KcQIcQw0Fd:uITfZJ1SN4JQaKx/Kkw0Fd
MD5:	AD542CDFC04F3D3E21C591306272E1F2
SHA1:	75DCC0382297711450AA500834D42ABD25E00A84
SHA-256:	94CE388EDFAABD0604FF750318ED3358F74120AD6B82D85BADD173DF09C9CC32
SHA-512:	BA14E776E54168A2FE6CB337B251455021408E7D28A199E9E04FB2349C858E3DFBFE7F37486CD15415AB0552DE2631CF09FC813AF9D43E440CCAEFCABDB8472E
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="1342261" />.. <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\WER40B2.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.694612449693779
Encrypted:	false
SSDEEP:	96:9GiZYWvXIp9YRYVLHW2zH3UYEZCftFiSP3DG5wCEBFZUahVHixcZzQIaD3:9jZDk2oDDUSUahVHicZznaD3
MD5:	5F5477C2598625553616383B8D034BF9
SHA1:	93356F37C9678412A30B9CDFEE671FFC31D10926
SHA-256:	E34358D64E33055A271962E7C83522C5557B2420100ADFAF553438CCE8DFAB6D
SHA-512:	57FAFBBDE767CE5B3C0691E6F3802C93986B87710A0A12B23A429D9DE94A8242705779133007B198DA2FDFFE7CCE866E31D0F1CD2E91F57ED4966105BB874BA
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):	3.097530992147587
Encrypted:	false
SSDEEP:	6:kKa0k8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:f9kPlE99SNxAhUeYlUSA/t
MD5:	FE852652A83C35ED73C16EB984F0A0BB
SHA1:	903E0D354606447141921F368FFF881F8B39D314
SHA-256:	544F8EC2994A6E7AE27B6E6716551CED5B9DA560112E0983051DD85BD10A38D3
SHA-512:	262D92433CCBCF768B271A5CD0E0FEA9FFD91773D8BEECE487C9BC110661D0FF92BFDF59C9934F83B897A65B11E885A63361AD24CE9F94C86F7592643C7D94 A
Malicious:	false
Preview:	p..... ....d.Eo...(..... ....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):	4.2353877146837755
Encrypted:	false
SSDEEP:	12288:AXebQWU7wCwgLXGMpf9a2sYrwl8X6ixnD72RGDQfK+kGVZWa:cebQWU7wCwYXGMmuw
MD5:	A0557199ADDFB27CF6464B5654E5A8D2
SHA1:	A1E5B548CF78A926C58CF4F8896D6F5AF36EA689
SHA-256:	57BEABDE5C4A76F562D6BC875F323212DD287C45BB05BAE5B1EAD7E60A1B3A7C
SHA-512:	06DB0E8FA45D8FD906539407ABEC8DE47B01D10FE91FD379BDE0E8ED0242299888405E4ACA66B0856C90EF95559C50B9A8C83B0B347B7F8BDC7D35321F57D5 B
Malicious:	false
Preview:	regfH...H...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmZ^.=o..... ....u..`..... .....

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):	3.717963317220201
Encrypted:	false
SSDEEP:	384:bou5K5Rcv4KgnVVeeDzeu1NKZtjWT8GRFwlnz:UgKCg/eeDzeANYtjzGRFwl
MD5:	6F59FBDE4F71430F9292DA90FE383B99
SHA1:	4726D40666BF4E921633D743DC6763542696A4EC
SHA-256:	BCBC1BEB1BA771B7C4B1C28484C56FACB5D44B9AE7F92AD4585349840177A5B8

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
SHA-512:	2709BD600E9FBAEF8069E1197E29A79AB36F18BA3DAFA11849C9B0CA81EA0B45C4B46E8D896F195207EEC23FFA9D4AD04D03DA4316ED61DE0AA5DDED6E07F9AB
Malicious:	false
Preview:	regfG...G...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmZ^.=o..... .....s..`HvLE.>.....G.....-'_....2....J.....hbin.....p.\.,.....nk,....=o..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ....=o..... ....Z.....Root.....lf.....Root....nk ....=o..... ....*.....DeviceCensus..... ....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.767601853206896
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:	nV5Wu77N8J.dll
File size:	588288
MD5:	a0306b7a6a12022e4fc8e586b0bc90ec
SHA1:	ee7d221826a725a2110bbddbea34bd14522b5ab4
SHA256:	9b1ca060b5a969f03c4c8d99ad487a454742e47fff97343a90afacb5da7d9589
SHA512:	9bf807e5b79ec4d6c24db9106db43d6e4e2211d70caf8ca71101d96001a7fb6c31dad9ac4d72b8e6646e03a7bfa70b296968be6a24f3d11dd8e90090de94d7dc
SSDEEP:	6144:cNU5LwA22222GgngDrDRVyYli/ci2tEGW78ODQiE3tvOSk5DKXOW14IkFxVFgY4E:x5w7YM/cYVV7EsOpOJyvnHtytFyQ
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	5.22192082052	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
01/14/22-18:50:50.021159	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49770	80	192.168.2.4	45.138.98.34
01/14/22-18:50:51.303705	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49771	8080	192.168.2.4	69.16.218.101

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 7128 Parent PID: 5400

General

Start time:	18:50:09
Start date:	14/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\nV5Wu77N8J.dll"
Imagebase:	0x1230000
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: 00000000.00000000.720219818.0000000000DE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.720240608.0000000000E11000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.722455601.0000000000E11000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.722263663.0000000000DE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.742599060.0000000000DE0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 7148 Parent PID: 7128

General

Start time:	18:50:10
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\nV5Wu77N8J.dll",#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 7160 Parent PID: 7128

General

Start time:	18:50:10
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\nV5Wu77N8J.dll
Imagebase:	0x20000
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: 00000002.00000002.669938310.0000000002541000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.669913455.0000000002510000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 3296 Parent PID: 7148

General

Start time:	18:50:10
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\nV5Wu77N8J.dll",#1
Imagebase:	0xb00000
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: 00000003.00000002.670020972.0000000004740000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.670044528.0000000004771000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6244 Parent PID: 7128

General

Start time:	18:50:10
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nV5Wu77N8J.dll,DllRegisterServer
Imagebase:	0xb00000
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: 00000004.00000002.719826672.00000000053B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.719773637.00000000052F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.719527275.0000000004CB1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.719898030.0000000005510000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.719919636.0000000005541000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.719503580.0000000004C80000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.719747240.00000000052B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.719938381.0000000005570000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.719857103.00000000053E1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6192 Parent PID: 7160

General

Start time:	18:50:11
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\nV5Wu77N8J.dll",DllRegisterServer
Imagebase:	0xb00000
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: 6344 Parent PID: 3296

General

Start time:	18:50:11
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\nV5Wu77N8J.dll",DllRegisterServer
Imagebase:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.718929777.0000000003501000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.718904101.00000000034D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.719243124.0000000005161000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.719379711.00000000052A1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.719211601.0000000005130000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.719345888.0000000005270000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.719316941.0000000005241000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.719284878.0000000005210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5672 Parent PID: 568

General

Start time:	18:50:23
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5356 Parent PID: 6244

General

Start time:	18:50:34
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Bdaefwhkzqb\lrinxnmhyts.ogu",XLurkV
Imagebase:	0xb00000
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.00000002.723238837.0000000004750000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.723309788.0000000004781000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6676 Parent PID: 568

General

Start time:	18:50:35
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 6712 Parent PID: 6676

General

Start time:	18:50:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 7128 -ip 7128
Imagebase:	0xcc0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6040 Parent PID: 5356

General

Start time:	18:50:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Bdaefwhkzqb\lrinxnmhyts.ogu",DllRegisterServer
Imagebase:	0xb00000
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: 0000000E.00000002.1188125968.00000000049D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1190726376.00000000059A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1190213897.00000000057D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188426833.0000000005110000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188330842.0000000005030000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188469714.0000000005141000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1186610997.0000000002E00000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188598739.00000000052A1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188659452.0000000005301000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188052400.00000000049A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1190813785.0000000005A20000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1190127401.00000000057A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188878871.00000000055E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1186687872.0000000002E31000.00000020.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188363449.0000000005061000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1190848028.0000000005A51000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188631120.00000000052D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188973289.00000000056F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188839400.00000000055B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188934735.00000000056C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1188553677.0000000005270000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.1190787571.00000000059D1000.00000020.00000001.sdmp, Author: Joe Security

File Activities Show Windows behavior

Analysis Process: WerFault.exe PID: 3660 Parent PID: 7128

General

Start time:	18:50:38
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7128 -s 568
Imagebase:	0xcc0000
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: 808 Parent PID: 568

General

Start time:	18:50:40
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 7064 Parent PID: 568

General

Start time:	18:50:58
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 4296 Parent PID: 568

General

Start time:	18:51:11
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Disassembly

Code Analysis