ID: 553354
Sample Name: hPJnda9rBy
Cookbook: default.jbs
Time: 18:49:20
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

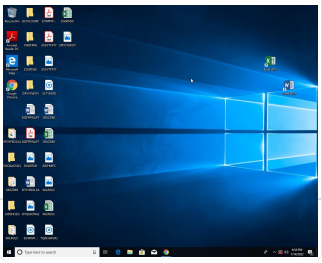
Windows Analysis Report hPJnda9rBy

Overview

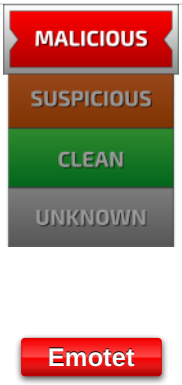
General Information

Sample Name:	hPJnda9rBy (renamed file extension from none to dll)
Analysis ID:	553354
MD5:	56c2941eb73ea5..
SHA1:	8d483f2069955ae.
SHA256:	7caa923401ec9a..
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

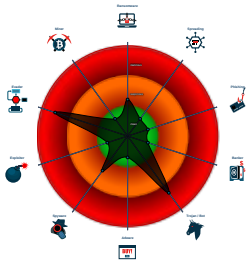


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Changes security center settings (no…
- 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

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6396 cmdline: loaddll32.exe "C:\Users\user\Desktop\hPJnda9rBy.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6436 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\hPJnda9rBy.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6472 cmdline: rundll32.exe "C:\Users\user\Desktop\hPJnda9rBy.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 7132 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\hPJnda9rBy.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6448 cmdline: regsvr32.exe /s C:\Users\user\Desktop\hPJnda9rBy.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 6552 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\hPJnda9rBy.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6524 cmdline: rundll32.exe C:\Users\user\Desktop\hPJnda9rBy.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 468 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vrptpiaqednpvbdv\iiexcwhjvlokrgr.var",pFqaCuAaxr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6384 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Vrptpiaqednpvbdv\iiexcwhjvlokrgr.var",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 6752 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6396 -s 524 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6620 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6656 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6396 -ip 6396 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6868 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7080 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7124 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 988 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6080 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 3688 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6300 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 1704 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 1056 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6724 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2188 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6412 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.249579927.0000000000D40000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.292238203.00000000050F0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.283401737.0000000004C70000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.249666455.0000000000EB1000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.292440539.0000000005360000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.d40000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.5200000.4.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.47b0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.5360000.6.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.5390000.7.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 39 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)

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

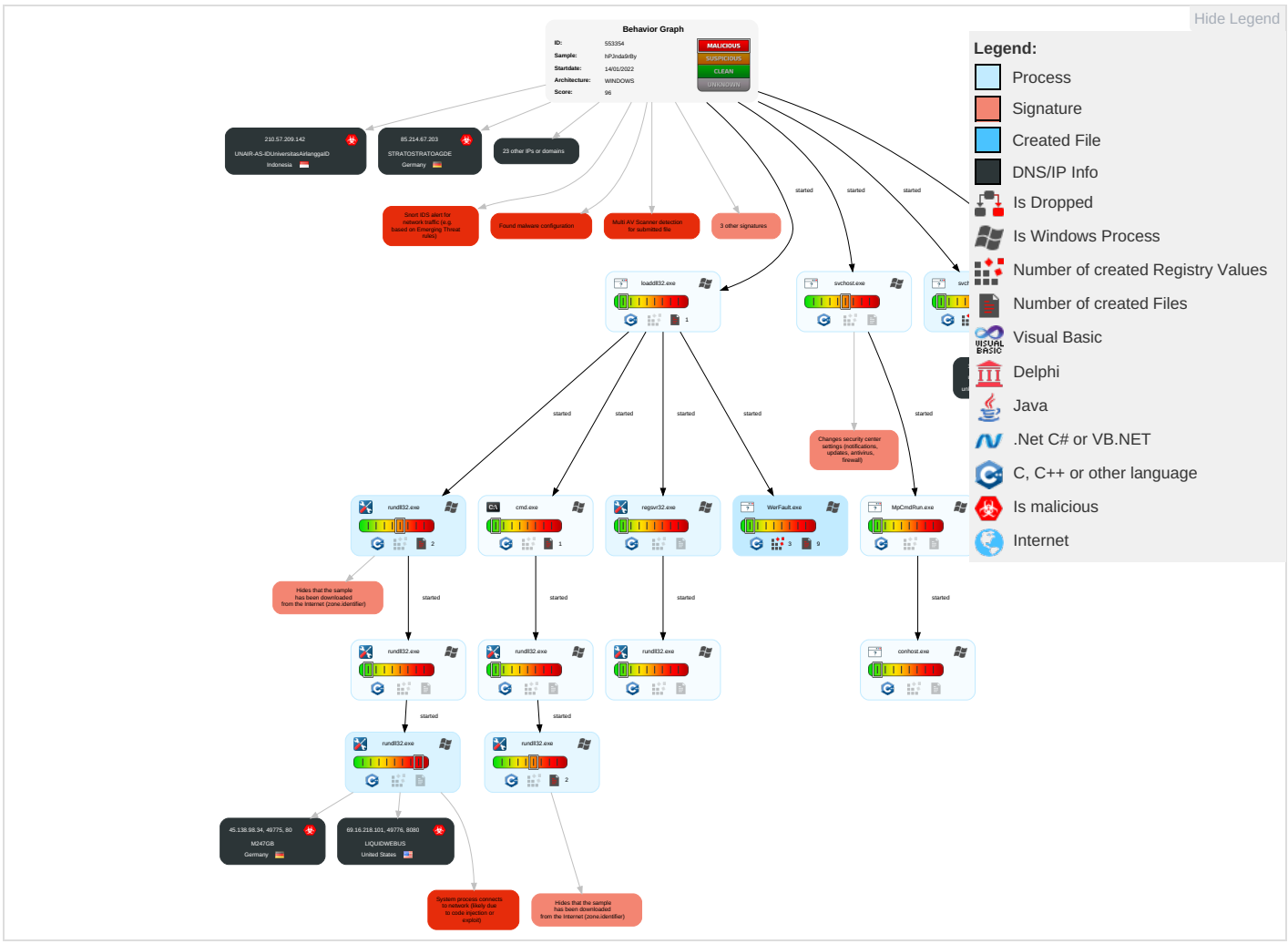
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 2	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypt Channe

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 3 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-St Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Security Software Discovery 6 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Regsvr32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

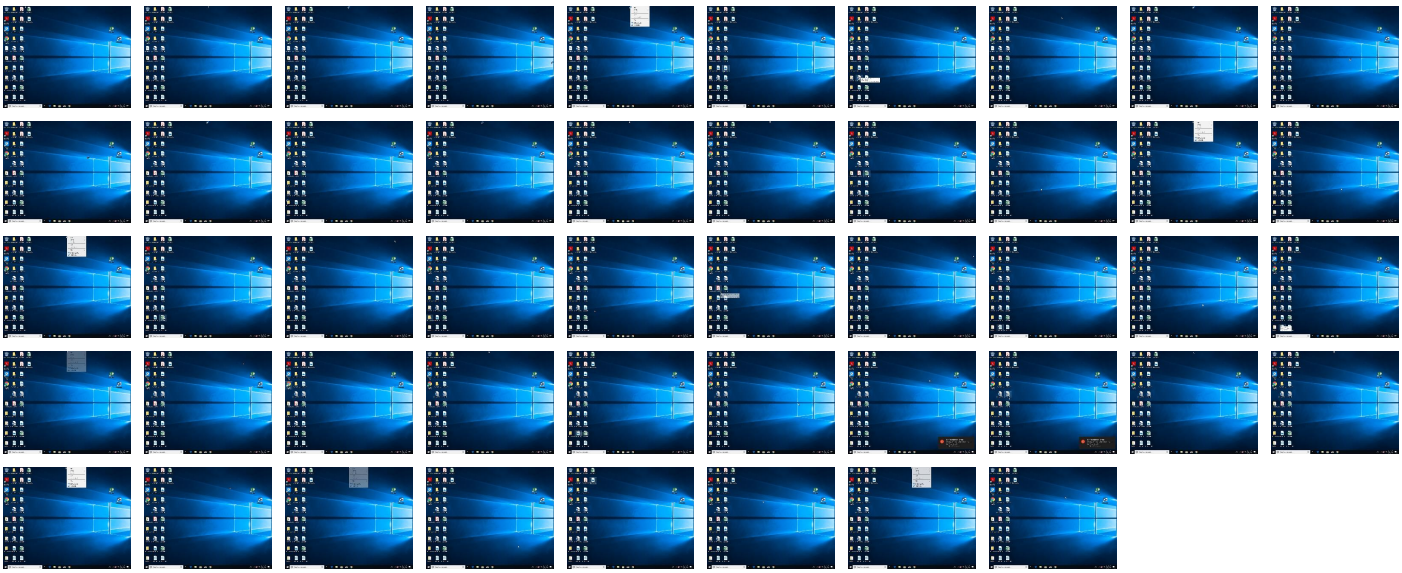
Behavior Graph



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
hPJnda9rBy.dll	18%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.loaddll32.exe.eb0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5390000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5230000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.rundll32.exe.2ab0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.4ec0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.4f20000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.5360000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.2.loaddll32.exe.d40000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4c70000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.d40000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4ca0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.48f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
15.2.rundll32.exe.4da0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.4ad0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.50f0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.d40000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.4ef0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.loaddll32.exe.eb0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.rundll32.exe.45e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.47b0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.4aa0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2f60000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.53c0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.4dd0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5150000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5200000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.4f50000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2f30000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.2.loaddll32.exe.eb0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdate.s.llnwi.net	95.140.236.0	true	false		high

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.16.218.101	unknown	United States		32244	LIQUIDWEBUS	true
159.69.237.188	unknown	Germany		24940	HETZNER-ASDE	true
45.138.98.34	unknown	Germany		9009	M247GB	true
116.124.128.206	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
37.59.209.141	unknown	France		16276	OVHFR	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
185.148.168.220	unknown	Germany		44780	EVERSCALE-ASDE	true
54.37.228.122	unknown	France		16276	OVHFR	true
190.90.233.66	unknown	Colombia		18678	INTERNEXASAESPCO	true
142.4.219.173	unknown	Canada		16276	OVHFR	true
54.38.242.185	unknown	France		16276	OVHFR	true
195.154.146.35	unknown	France		12876	OnlineSASFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
128.199.192.135	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553354
Start date:	14.01.2022
Start time:	18:49:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	hPJnda9rBy (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:	41
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:	mal96.troj.evad.winDLL@37/17@0/28
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.1% (good quality ratio 92.4%) • Quality average: 70.7% • Quality standard deviation: 27%
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
18:50:25	API Interceptor	10x Sleep call for process: svchost.exe modified
18:51:44	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false
Reputation:	unknown
Preview:	.....*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.2494437587788148
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4y:BJiRdwfu2SRU4y
MD5:	480F1D8F507E6F3F9FE0B7A4A018C8F7
SHA1:	AC93D87E2C4C645026D7D5A3853870BCB9139E41
SHA-256:	1A525D00790F8EB0418D255015F85E171DA4496889C17690C5D6F4E541D0157B
SHA-512:	87A72B0EEE13287A7CFA6D6305EDBA930BAF99EB2274C6DD385C2BC6DB8A60BFB0134EF51761A83F344367B5F7CC7A263591CC91FC9BFA352EF55DE6620DD7 27
Malicious:	false
Reputation:	unknown
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x57df8562, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25061660725172696
Encrypted:	false
SSDEEP:	384:Kfj+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:KfQSB2nSB2RSjlK/+mLesOj1J2
MD5:	B9976BD699FD40EC2597214BD70D42DB
SHA1:	85B44DDF230461CF51FDA956563B716D1A7C8058
SHA-256:	A541FA8B6CAEC46F6DC533C32077CFF305F7DA4AE567BA7439C657227182B072
SHA-512:	8CFF58CE8FD93C4D176E26E063F3EF17F29C1CCC9090A9E8D32FC5A001306CDBDD56E291F06169AB266E0B1914359EFB0D6EE390B8E8DB17F0CF58E656054A E
Malicious:	false
Reputation:	unknown
Preview:	W.b... .....e.f.3...w.....)....$5...z...2...z..h.(....$5...z...).....3...w.....B.....@..... ....+Z.$5...z.....z$5...z..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07540473094423805
Encrypted:	false
SSDEEP:	3:SZ7v/3t+HtNW+uq501qnM//Dmqkf+Htall3VkttlmlnI:SZrPt+XW+uO01qnsaqkf+o3
MD5:	BB6FF757E36C514FC9BFB6F5A097860E
SHA1:	721D7CB22C57D2532090EE19CC75F1F9465D6986
SHA-256:	C20C401E05EB6CD262D23FCFBB0F822315049C9014AEF90AD1CCA38098490ED9
SHA-512:	3009E2C8177659100AA640BCDF05E068F8E874FB819002D571B02227A8CF78B9B654FED6E5AA0316B34CFDCD4346BF519A13B5ABC9470E8E8DB67A984D3BD48 F
Malicious:	false
Reputation:	unknown
Preview:	..d.....3...w...2...z..$5...z.....$5...z..$5...z..0...$5...zE.....z$5...z..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d422a667165d65114742feca998c4f65a16c35b9_7cac0383_1be2745f \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

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d422a667165d65114742feca998c4f65a16c35b9_7cac0383_1be2745f\Report.wer	
Entropy (8bit):	0.7987727240843838
Encrypted:	false
SSDEEP:	96:q/VJZnYyXy9haol7JfqpXIQcQSc6mcEUcw3/s+a+z+HbHgrVG4rmMoVazWvMLsNd:wVnnTHsieryjLq/u7sCS274ItW
MD5:	70384C8F40FEF1CB13FB622793A064FB
SHA1:	C6015969E6BF416C80AC5660B550C2BE10FF1891
SHA-256:	263C1DA703EB7FF99381640F8D213430787C3020C9C279B5B1949989FA3D6601
SHA-512:	7BD0D4DB6214E90873FDA51EB46633C5BA6D622666AC25779A2E74BEC9834664C2125B2274FE15E7E55FC91326392CAE1BE7133232F6F39789E3CEA782375906
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.8.8.6.2.4.9.2.8.4.0.7.1.....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.=.c.8.4.c.3.b.e.1.-.b.2.6.4.-.4.a.f.b.-.9.f.9.b.-.5.0.4.b.3.4.0.8.8.c.5.7.....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.=.7.c.0.a.b.a.3.a.-.8.2.f.1.-.4.0.6.f.-.a.1.1.0.-.6.6.a.6.0.8.5.d.3.0.8.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.f.c.-.0.0.0.1.-.0.0.1.6.-.6.b.e.f.-.a.4.9.e.b.a.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\WER16A.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	53488
Entropy (8bit):	3.0615549522643883
Encrypted:	false
SSDEEP:	1536:pRHsfrEWFbe22KkrqcWL5ZTyD7frGWDKw6H7h/+D:pRHsfrEWFbe22KkrqcWL5ZTyD7fr5DKY
MD5:	972E6872AB588C93A987C3763E8FF60D
SHA1:	469DE7754D1563A0B903028C48196772537AE3D6
SHA-256:	6E6705CEC01CDE97A616E314CF92D1934FC18086BBC5EE05D80687041CA6F807
SHA-512:	C86C499380FF9E7A1082FD73735550B6BB87C99A48F3B10639DF85ABCC47ACB5D5C5801669AD4E276ECE5AA6C2A876C9F237149446E691F11161FEF4D8CADA
Malicious:	false
Reputation:	unknown
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\WER5B88.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Jan 15 02:50:26 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	45020
Entropy (8bit):	2.1152568398952414
Encrypted:	false
SSDEEP:	192:pSEesTOU2Ldw/oKCiIUr9ygv4b7kYROSz/2iCUSD5yD:EUodw/oDiIU3v4b7k8OSz/3
MD5:	D2FE87042ECA1FD35C67B74A136F7340
SHA1:	1B9E8F2AFA839EE6F7EB0C744C0AFD9B90A93B39
SHA-256:	4A5B8952BEFDDA27286F771870F572FEAD94EB322241D406095A0F26428D53F5
SHA-512:	A0387E13FDFF4F2A9974048031CA698131669DD5F0ACB92D13ADE3151E43D6B726834CDE1ABDA023AEE34A098FFBF47E357938A22850596177FEEC38D4859A0
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....r6.a.....$...T.....%.....`.....8.....T.....x.....d.....U.....B..... ..GenuineIntelW.....T.....e6.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\WER61D2.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):	8346
Entropy (8bit):	3.699938523491725
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiY46/Vjzx6YIZSUAUhYgmfjSwGqCpBF89bOvsfTV0am:RrlsNiv6/V/x6Y2SUAoYgmfjSwTOUfTO

C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D2.tmp.WERInternalMetadata.xml	
MD5:	3D73E97743B6D71D2CE7E360CE83B0E4
SHA1:	6DD1CA01E57659066B0FDFEF68A519CF384B1332
SHA-256:	AD05D6019F5A76DA135A8C73DF6D475452D1C1DD3C6B5D2864D3104CB459E909
SHA-512:	FC2B56DDF4F38653AA8BB199F2352AF5F84ECE58F63388CAF18BF6870E7091E088A6F8C7CFEF4537E666D00AEFC89399B6C687576ECA480ED7C8124300AC19C
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.3.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER66B5.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):	4.469439709213211
Encrypted:	false
SSDEEP:	48:cvIwSD8zsPJgtWI9PfWSC8B/8fm8M4J2++ZFG+q84pDr3QKcQIcQw07d:ulTfxQOSN6J4ylDQKkw07d
MD5:	35AFB0959F866102EFCEF8CFB03D7CF4
SHA1:	102464CB0E6D372AA1B96AF55051D6CF0863F25F
SHA-256:	7EE8969FE2312FBD972D2DBD7763819ED689B01319CE35DF07833E3A0824C281
SHA-512:	FDBEA2D81CDC9171FD4D562C56AA9490D0C92B9F6B7F0AAA24FA6EA24A9CAD2F495094B3F9988CE6960063779CE0DDEA5E463CBBEC3802A970982A95EA31D51
Malicious:	false
Reputation:	unknown
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="1342801" />.. <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\WER8FD.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.693556707675597
Encrypted:	false
SSDEEP:	96:9GiZYW0lHc1RkWY7YgWHvHwGYEZnOt8idZKJfwoI2dDarGw0x/Ibo3:9jZD0678uYoLDarGw0xQbo3
MD5:	CDF93CF01FE266D9413C5F468E72D0BF
SHA1:	81F0302DD34173F096751DD7E3E8C10154311CAB
SHA-256:	9E3B6B144B3D88BE0FCB92968B6168E559E3A2CA48275604F127620D4CD144E8
SHA-512:	B947972656CCB44B7ED790C6DBD259E7C1FFFDDD43CB97542E9CD2E1EFA36BBB455610BC417E5B3F5624815E82BB9864330BF8CA63465AECC094DE50849DBDF
Malicious:	false
Reputation:	unknown
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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

<table>
<tr><td>SHA-512:</td><td>FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>MSCF............,...................I.......;w........RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne......<.w......A..B........c...wi......D....c.0D,L........f y....Rg...=........i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.......~U...."<ke.....l.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.".g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....l..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...?.....l.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&.....</td></tr>
</table>

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1244568012511515
Encrypted:	false
SSDEEP:	6:kKONhk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:Kh9kPlE99SNxAhUeYlUSA/t
MD5:	C825C3B963A4EDD130C1ED69E8DB5165
SHA1:	939347D739FBCACF514F706123325C83A45C6EFC
SHA-256:	9065DAC879286F740D2C31A7807B7474A9C9A783133236919FCA9AA27B447811
SHA-512:	23525BA36A6448CC83B0AB0A8883589BB298369EC028FB75F4D188DCB5E8B8AF36E72E8A743791F8D42F5CD44E4ECE2267F7E0096EA4162D55AA12458F5E1FC
Malicious:	false
Reputation:	unknown
Preview:	p...... ....`......(... ....q.\].......&..............h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBAA
Malicious:	false
Reputation:	unknown
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	7250
Entropy (8bit):	3.167116140196023
Encrypted:	false
SSDEEP:	96:cEj+AbCEH+AbuEAc+AbhGEA+AbNEe+Ab/Ee+AbPE6w9+Ab1wTEx+AbY:cY+38+DJc+iGr+MZ+65+6tg+ECG+h
MD5:	9DAAEF8A5E401B4B4FB8E40C4209D947
SHA1:	C57BCC0397D823196CF033FB9EBF4DE4EFC98379
SHA-256:	E507D467ED93E99586D91585D7332A90E76ED9FEF80170D5856AD69776DA2586
SHA-512:	1F9B287917BA24AC22A52271743A6D2FFB27B63488EA36182BAAFCC3A5287FC84892C0633D0914BCD3AD755ADF60CB259D9CF9355E31E555DB7F1D262A23F94
Malicious:	false
Reputation:	unknown
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:. 4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7. 0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220115_025036_670.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.7840681033565295
Encrypted:	false
SSDEEP:	96:RCad72o+gT5Ov9z/YjRC0WI2lcTkeY4YaT2kjFzRNMC1dJR8q5j5FNMCZY5lUMC3:APDbvG2CuNCp4C8C6DCrCyCo
MD5:	E61B2F014940B7E98E976655C4904B64
SHA1:	E4807D63E9488F9E15ED5C0F14DBBD1A4FD691CF
SHA-256:	67889112EB75B5283A7437C528B12CD463875865559C2C6F169A0B2900E3A304
SHA-512:	2EE6F25C4E4E52BCFF98693F2F977EA6C3CA2282004C6DC3B4944B4E9D383EB3896A7333D2566DC0541DDA2ED62C057CF53E2242F88A09D59D4E6E99B799FB 8
Malicious:	false
Reputation:	unknown
Preview:	....!.....D.....B.....Zb.. ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1...../_8.... .....[.V.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.2.0.1.1.5._.0.2.5.0.3.6._.6.7.0...e.t.l.....P.P.....D..... .....

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):	4.261458161750714
Encrypted:	false
SSDEEP:	12288:gy3mVq0u4mqFICqp4A1NBB+WCAI9Smf0jyoqAYx/NMn+733oIIDkcad5:93mVq0u4mqFICqpPTRU5
MD5:	30895F1B808AF0A0F36C9AC8DC3C8DA3
SHA1:	96292AAA73F88F5D6D630B0C98F88CCB61FDB4BC
SHA-256:	2FF4438EB94E16380307213D04B64CA20A8A91816EBD3CEA50BCDF15E2DE866B
SHA-512:	DBCD5F758F6CF0B1BFFEB8698AF4269EA82F02DC692743E600EE7209A958E4743310374BEF7A43ECE49A4ACF5419960390B64B649C3E334169362B1D0B83915F
Malicious:	false
Reputation:	unknown
Preview:	regfQ...Q...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..I..... ....PsB..... .....

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):	3.047087575815636
Encrypted:	false
SSDEEP:	192:EeN/g18deDMGtY+5FSE9lMqXyQVWnxuYW2oIKqe8mxwpBuN5y:p9Y5TXQnxuf2oIPmxwpBuN5y
MD5:	B5438EDFDB8F0C941C2FDB4C839F2277
SHA1:	FB6C2BC358A72FC4EA19B0E932D2DA10BBA84A75
SHA-256:	FE1E867A5EC16F5C0202213154038F4862BB97EE81A7A23D12BDD57E7E36EE2C
SHA-512:	F200F2A7B939982F1E9632FD0EB9C5FD55FF183DF589E35C66DDC90EF33DC52BFBEC05AE90AC98829D3E183B9C1235FF5E54C6B362DE7E403626ABF1D71DB2 C
Malicious:	false
Reputation:	unknown
Preview:	regfP...P...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..I..... ....VsB.HvLE.>.....P.....h.....u..Lt...2.....hbin.....p.\.,.....nk,...I.....H..... .....&...{ad79c032-a2ea-f756-e377- 72fb9332c3ae}.....nk ...I..... .....P..... .....Z.....Root.....lf.....Root....nk ...I.....}..... .....*.....DeviceCensus..... ....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.76756574902532
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:	hPJnda9rBy.dll
File size:	588288
MD5:	56c2941eb73ea59306cc9d2a6b15974c
SHA1:	8d483f2069955ae7a3f7e70e6dafa2641cbf4a75
SHA256:	7caa923401ec9a16969f0b37225b77cd16c6923abff2eda76f1fa9a35bff2879
SHA512:	cdd0692c8a2bf51e1c27085869067f886680a4d0ee6d721d9ed337ba90e185d7af8c11db718850bd17fa49dd1bb903e412b6b4214cad8f22a766254bfd43b540
SSDEEP:	6144:cNU5LwA22222GgngDrDRVyYli/ci2tEGW78ODQiEjtvOSk5DKXOW14IkFxVFgY4E:x5w7YM/cYVV7E4OpOJyvnHtytFyQ
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	0.357372428797	data	5.22176472438	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
01/14/22-18:51:09.071744	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49775	80	192.168.2.5	45.138.98.34
01/14/22-18:51:10.239050	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49776	8080	192.168.2.5	69.16.218.101

Network Port Distribution

TCP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:51:00.364427090 CET	8.8.8.8	192.168.2.5	0x4cac	No error (0)	windowsupdate.s.llnwi.net		95.140.236.0	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6396 Parent PID: 4344

General

Start time:	18:50:13
Start date:	14/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\hPJnda9rBy.dll"
Imagebase:	0x1340000
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: 00000000.00000000.249579927.0000000000D40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.249666455.0000000000EB1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.273369713.0000000000EB1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.248107963.0000000000EB1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.273136577.0000000000D40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.247589289.0000000000D40000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6436 Parent PID: 6396

General

Start time:	18:50:14
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\hPJnda9rBy.dll",#1
Imagebase:	0x150000
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: 6448 Parent PID: 6396

General

Start time:	18:50:14
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\hPJnda9rBy.dll
Imagebase:	0x10d0000
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: 00000003.00000002.240583182.00000000047B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.240663709.00000000048F1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6472 Parent PID: 6436

General

Start time:	18:50:14
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\hPJnda9rBy.dll",#1
Imagebase:	0x2c0000
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: 00000004.00000002.283401737.0000000004C70000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.283457312.0000000004CA1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6524 Parent PID: 6396

General

Start time:	18:50:15
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\hPJnda9rBy.dll,DllRegisterServer
Imagebase:	0x2c0000
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: 00000006.00000002.292238203.00000000050F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.292440539.0000000005360000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.292503101.00000000053C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.292286268.0000000005151000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.291899393.0000000004AA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.292382538.0000000005231000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.291926283.0000000004AD1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.292348767.0000000005200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.292473375.0000000005391000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6552 Parent PID: 6448

General

Start time:	18:50:16
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\hPJnda9rBy.dll",DllRegisterServer
Imagebase:	0x2c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6620 Parent PID: 556

General

Start time:	18:50:19
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
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: 6656 Parent PID: 6620

General

Start time:	18:50:19
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6396 -ip 6396
Imagebase:	0x300000
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: WerFault.exe PID: 6752 Parent PID: 6396

General

Start time:	18:50:22
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6396 -s 524
Imagebase:	0x300000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 6868 Parent PID: 556

General

Start time:	18:50:25
Start date:	14/01/2022

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
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

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 7080 Parent PID: 556

General

Start time:	18:50:32
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:	0x7ff797770000
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: 7124 Parent PID: 556

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 localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7132 Parent PID: 6472

General

Start time:	18:50:35
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\hPJnda9rBy.dll",DllRegisterServer
Imagebase:	0x2c0000
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: 0000000F.00000002.292882371.0000000004DA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.292911557.0000000004DD1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.292454173.0000000002F30000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.293034859.0000000004F20000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.292508980.0000000002F61000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.293001920.0000000004EF1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.293065921.0000000004F51000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.292962848.0000000004EC0000.00000040.00000001.sdmp, Author: Joe Security

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 988 Parent PID: 556

General

Start time:	18:50:36
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6080 Parent PID: 556

General

Start time:	18:50:36
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 468 Parent PID: 6524

General

Start time:	18:50:39
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vrptpiaqednpvbdv\iiexcwhjv lokrgr.var",pFqaCuAaxr
Imagebase:	0x2c0000
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: 00000012.00000002.296105740.0000000002AB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000012.00000002.296341429.00000000045E1000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: SgrmBroker.exe PID: 3688 Parent PID: 556

General

Start time:	18:50:41
Start date:	14/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6cb2a0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6384 Parent PID: 468

General

Start time:	18:50:41
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Vrptpiaqednpvbdv\iiexcwhjv lokrgr.var",DllRegisterServer
Imagebase:	0x2c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities | Show Windows behavior

Analysis Process: svchost.exe PID: 6300 Parent PID: 556

General

Start time:	18:50:41
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 1056 Parent PID: 556

General

Start time:	18:50:45
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6724 Parent PID: 556

General

Start time:	18:51:03
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 1704 Parent PID: 6300

General

Start time:	18:51:42

Start date:	14/01/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff688a40000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6276 Parent PID: 1704

General

Start time:	18:51:43
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 2188 Parent PID: 556

General

Start time:	18:52:47
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6412 Parent PID: 556

General

Start time:	18:53:04
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis