



ID: 553377
Sample Name: ALNgwfVtrB
Cookbook: default.jbs
Time: 19:31:37
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report ALNgwfVtrB 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Emotet 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 12
Static File Info 16
General 16
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Rich Headers 17
Data Directories 17
Sections 17
Resources 17
Imports 17
Exports 17
Possible Origin 17
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 18
TCP Packets 18
Code Manipulations 18
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: loaddll32.exe PID: 6764 Parent PID: 1864 18
General 18
File Activities 19
Analysis Process: cmd.exe PID: 4616 Parent PID: 6764 19

Copyright Joe Security LLC 2022

General 19
File Activities 19
Analysis Process: svchost.exe PID: 5264 Parent PID: 560 19
General 19
File Activities 19
Analysis Process: regsvr32.exe PID: 3408 Parent PID: 6764 20
General 20
Analysis Process: rundll32.exe PID: 6048 Parent PID: 4616 20
General 20
Analysis Process: rundll32.exe PID: 6800 Parent PID: 6764 20
General 20
File Activities 21
Analysis Process: rundll32.exe PID: 6980 Parent PID: 6048 21
General 21
File Activities 22
File Deleted 22
Analysis Process: svchost.exe PID: 4588 Parent PID: 560 22
General 22
File Activities 22
Analysis Process: WerFault.exe PID: 4680 Parent PID: 4588 22
General 22
Analysis Process: WerFault.exe PID: 6496 Parent PID: 6764 23
General 23
File Activities 23
File Created 23
File Deleted 23
File Written 23
Registry Activities 23
Key Created 23
Key Value Created 23
Analysis Process: rundll32.exe PID: 4668 Parent PID: 6980 23
General 23
Analysis Process: rundll32.exe PID: 4584 Parent PID: 4668 24
General 24
File Activities 24
Analysis Process: svchost.exe PID: 5688 Parent PID: 560 24
General 24
File Activities 24
Analysis Process: rundll32.exe PID: 400 Parent PID: 3408 24
General 24
Analysis Process: svchost.exe PID: 5796 Parent PID: 560 25
General 25
File Activities 25
Analysis Process: svchost.exe PID: 4532 Parent PID: 560 25
General 25
File Activities 25
Analysis Process: svchost.exe PID: 2932 Parent PID: 560 25
General 25
File Activities 25
Registry Activities 25
Disassembly 26
Code Analysis 26

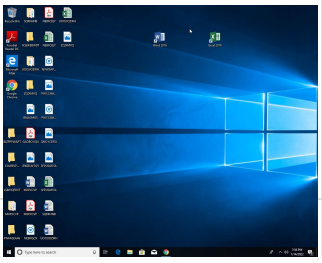
Windows Analysis Report ALNgwfVtrB

Overview

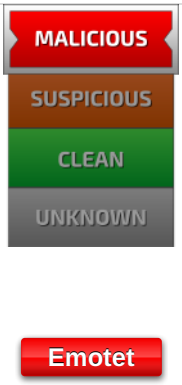
General Information

Sample Name:	ALNgwfVtrB (renamed file extension from none to dll)
Analysis ID:	553377
MD5:	61308ba77d051e..
SHA1:	95d2cd6c7be346..
SHA256:	bd2c1b86de45c3..
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

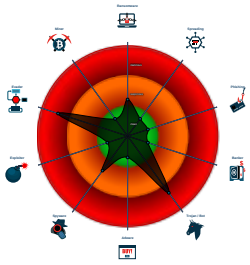


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 6764 cmdline: loaddll32.exe "C:\Users\user\Desktop\ALNgwfVtrB.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 4616 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\ALNgwfVtrB.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6048 cmdline: rundll32.exe "C:\Users\user\Desktop\ALNgwfVtrB.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6980 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\ALNgwfVtrB.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 4668 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Mhgwckn\ikgetkts.aey",QTEnBIyMIuE MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
          - rundll32.exe (PID: 4584 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Mhgwckn\ikgetkts.aey",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 3408 cmdline: regsvr32.exe /s C:\Users\user\Desktop\ALNgwfVtrB.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 400 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\ALNgwfVtrB.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6800 cmdline: rundll32.exe C:\Users\user\Desktop\ALNgwfVtrB.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 6496 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6764 -s 528 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5264 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4588 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 4680 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 164 -p 6764 -ip 6764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5688 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5796 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4532 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2932 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.388319825.0000000005640000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.388061342.00000000053B1000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.388938400.0000000005A60000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.425302680.00000000054F1000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.388421865.00000000056A0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.5200000.2.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.5a90000.13.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.54c0000.4.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.46a0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.53b0000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 49 entries				

Sigma Overview

System Summary:



Copyright Joe Security LLC 2022

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:



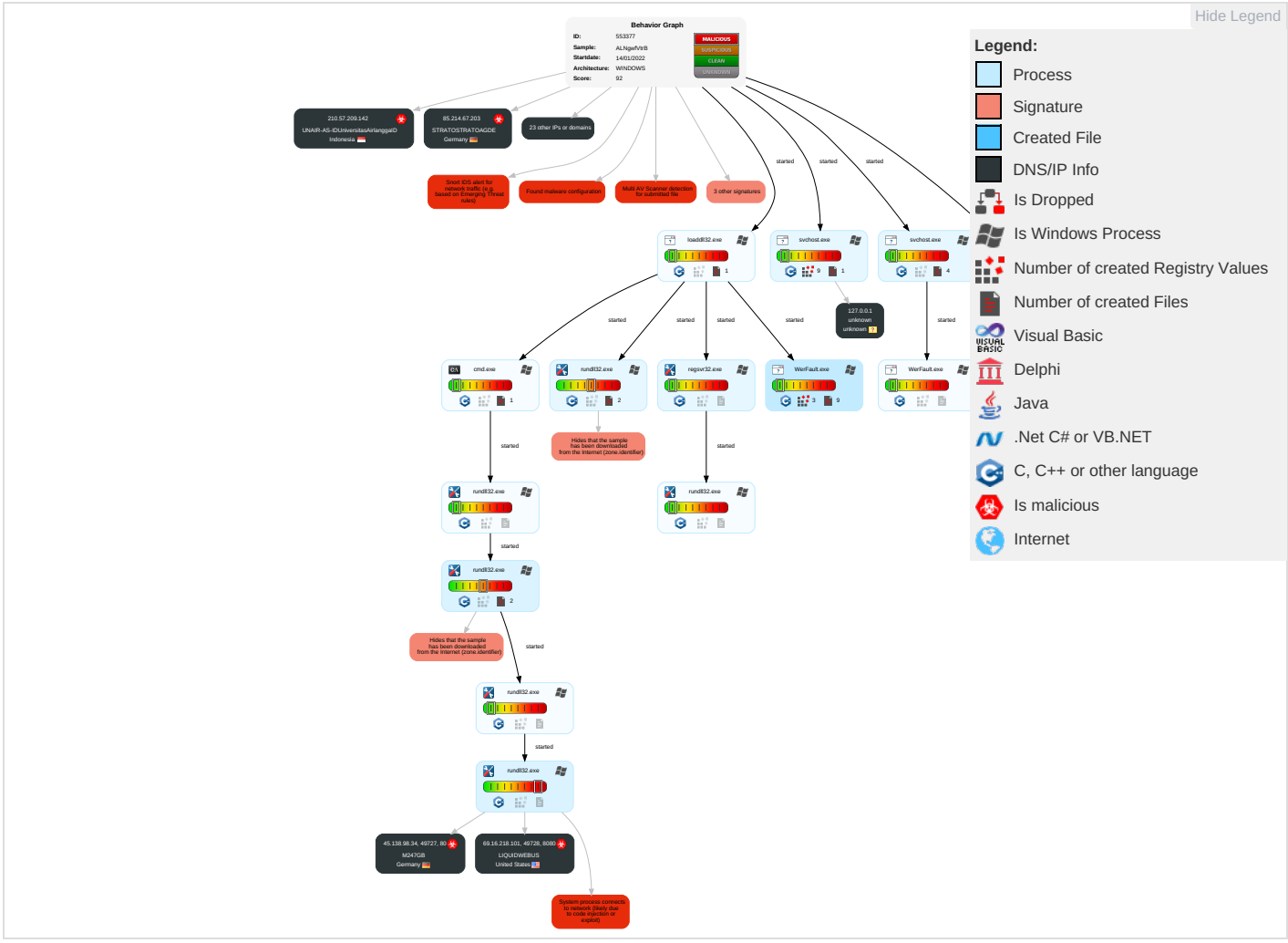
Yara detected Emotet

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Security Software Discovery 5 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Regsvr32 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

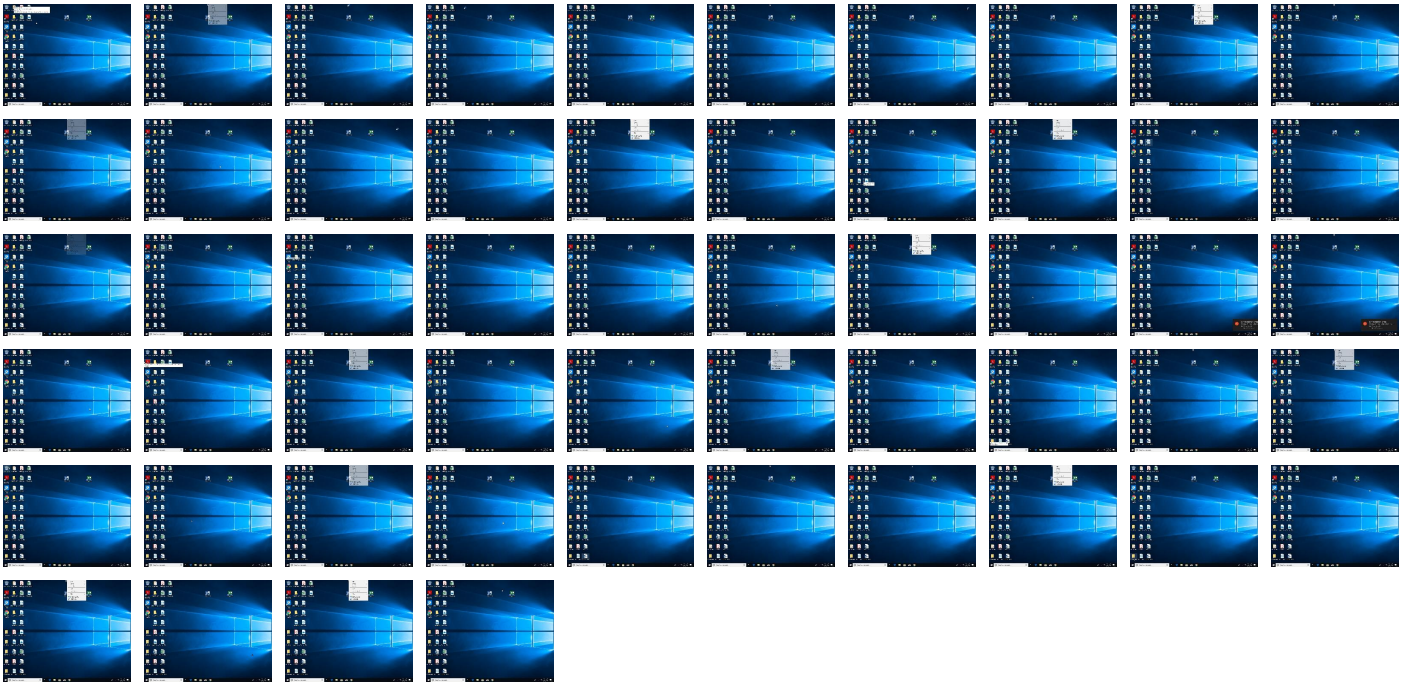
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ALNgwfVtrB.dll	15%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.rundll32.exe.5640000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.b50000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.d30000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.53c0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.56d0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5490000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5460000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.b50000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.53b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.5200000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.5a90000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.46a0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.54c0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.55d0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.46d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5930000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.5630000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.55a0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.56a0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.0.loaddll32.exe.d30000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5380000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.5600000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.4e60000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.33b0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.5670000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.4020000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.3080000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.33d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.54f0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.3660000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.4a10000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.5900000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.5a60000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
3.2.regsvr32.exe.4050000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.b50000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.2.loaddll32.exe.d30000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://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	

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.81.119	unknown	United States		20473	AS-CHOOPAUS	true
104.131.62.48	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternet SABR	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNET AR	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
185.148.168.15	unknown	Germany		44780	EVERSCALE-ASDE	true
51.210.242.234	unknown	France		16276	OVHFR	true
217.182.143.207	unknown	France		16276	OVHFR	true
69.16.218.101	unknown	United States		32244	LIQUIDWEBUS	true
159.69.237.188	unknown	Germany		24940	HETZNER-ASDE	true
45.138.98.34	unknown	Germany		9009	M247GB	true
116.124.128.206	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
37.59.209.141	unknown	France		16276	OVHFR	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
185.148.168.220	unknown	Germany		44780	EVERSCALE-ASDE	true
54.37.228.122	unknown	France		16276	OVHFR	true
190.90.233.66	unknown	Colombia		18678	INTERNEXASAESPCO	true
142.4.219.173	unknown	Canada		16276	OVHFR	true
54.38.242.185	unknown	France		16276	OVHFR	true
195.154.146.35	unknown	France		12876	OnlineSASFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
128.199.192.135	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553377
Start date:	14.01.2022
Start time:	19:31:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 25s
Hypervisor based Inspection enabled:	false

Copyright Joe Security LLC 2022

Report type:	light
Sample file name:	ALNgwfVtrB (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@28/15@0/28
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 45.1% (good quality ratio 41.9%) • Quality average: 73.2% • Quality standard deviation: 28%
HCA Information:	• Successful, ratio: 65% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:33:51	API Interceptor	10x 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

Copyright Joe Security LLC 2022

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):	0.2494552734353501
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU45:BJiRdwfu2SRU45
MD5:	ACEC30FA0B2887F7209FFA7C485EF3E6
SHA1:	729B9EBF8483F0E62F50146AB125A7E594EE5397
SHA-256:	012529C218728BF9B3632898D3B6DAD496391C68D17E00E5B3B7D519D3B63238
SHA-512:	CB8A710D87BE4A10A5690DFE99CD1F3ED52E252068BECDFCA3CB72F8B717680FCBA77B4DD4C7346911D8961B9CBB9FB629117C66E30132E6B5FAC13A7F1D0 FC
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 user DataBase, version 0x620, checksum 0x1ff79e9b, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25063246514845516
Encrypted:	false
SSDEEP:	384:+zH+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:+zsSB2nSB2RSjlK/+mLesOj1J2
MD5:	6A5F82169C1E928B7B2813D982DF0CC4
SHA1:	5E00E7DC875F2290DEB199B7CDFD88EB7F00FA2B
SHA-256:	9499ABBD834BC69C141A5659C76E2C1A226C0579893B10375BB19AA659A9BCD5
SHA-512:	E2B1AD0F38F387DA0207B6BBCBD8927AF5178C84C2EB291623E40AE892D58551DE356EB2BEAE42155B8267455B411B512942545112C0578B08DB11EDE4DC831
Malicious:	false
Reputation:	unknown
Preview:	....e.f.3...w.....)....%...z..:!...zS.h.(.....%...z....).....3...w.....B.....@..... ....%...z.....%...z..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07692722651967188
Encrypted:	false
SSDEEP:	3:wW9mllr7vfPUWff8+E2kfoulXDAopll3VkttlmlnI:wWElZrEWUfoRa3
MD5:	72D779F2D6EEF5FD6670D0AA17207A6A
SHA1:	C9D5EC2D9E22E21027BE655F633AE052EA6991ED
SHA-256:	1FB083D386ED7399D0F5BF9006A1A2283F66D8DCD0CC6106B14D3E439F0CD0EA
SHA-512:	5DA3FB2B95F46E3D950A27070C25D6A2CD06F6FA79E0038F7AA5B60F071729343718C7FB41C154B1EC3B8A7C632431136C2EB13B947D0E5A875F1EFFF1721506
Malicious:	false
Reputation:	unknown
Preview:	..s.....3...w..:!..z...%...z.....%...z...%...z.....%...z.....%...z.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_669a8c10d0efd6a57917dbe0788b74fa72a925de_7cac0383_1987fea0\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):	0.7987378948423511
Encrypted:	false
SSDEEP:	96:K6qnYy4y9haol7JfHpXIQcQSc6mcEUcw3/s+a+z+HbHgNVG4rmMoVazWbSmEBFdo:gnhHsieryj9q/u7sgS274ltW
MD5:	A403F656EF604A2E49F9E4ACC2129A24
SHA1:	AF381E16D8639F6C2A553E58499FC088D151624C
SHA-256:	198C574233F816519CA62027DD72FF837F64C00F391442DB3BE612A4F6C9BCD7
SHA-512:	717CAC97CE4145DD90A3B600D32BFF8B749DD64CA7B38E9AD853FEA5D72697EE8BF2DF181AC9350F93AF342880FD1A7A554820551FC0E62C20D07941945FFBB
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.=.1.3.2.8.6.6.9.1.1.7.7.9.5.2.6.3.3.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.=.e.n.t.i.f.i.e.r.=.f.d.3.f.9.0.f.b.-.a.4.6.6.-.4.5.c.a.-.b.c.8.c.-.3.7.e.1.f.d.c.9.c.e.c.9.....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.=.3.5.a.0.5.5.1.8.-.f.2.c.9.-.4.6.e.e.-.a.e.b.1.-.8.c.a.a.4.a.2.a.0.5.8.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.6.c.-.0.0.0.1.-.0.0.1.7.-.b.e.b.8.-.a.9.8.f.c.0.0.9.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\WER178B.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51940
Entropy (8bit):	3.0778019180962497
Encrypted:	false
SSDEEP:	768:g+HIinEqdSll0Lme/AFvprFwgzyLFOUP2IcOenKI:g+HIiTj0Lme/AFdFWL6IcxnKI
MD5:	F15E9557C7C73AC82EE1B580B68A2CED
SHA1:	3BE551D3FA3D2713F9A1E990F026642749A95291
SHA-256:	0884B007D12886A2952F62389F88D2AE4DB62DBB9932C30C436D19C3E17E5255
SHA-512:	82CB9E72779B86BBA19253D767B7C2269A5385546846EAAF39274F5868FA00BF23220DF70282CB0203AF2B440C9532C5933BC716517F4DBD3DE0643B02365628
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\WER20B4.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.695073459938915

C:\ProgramData\Microsoft\Windows\WER\Temp\WER20B4.tmp.txt	
Encrypted:	false
SSDEEP:	96:9GiZYWqRgM+egtYk6YoiWApH+YEZJXtFiPFPDxwUCoBaqS9SMUM8wIDA3:9jZDqRC760AalaqS9SMfuDA3
MD5:	D49BF9037244600A0CD2D79B93509810
SHA1:	2833D9A483D595D915E9DEB58BC9926FED4F759E
SHA-256:	BF470317ADFF9552AA6D0DCF8D8670396BCAC888218FB8315367F8092BB7DE87
SHA-512:	A449EC0761501982A2A5F6C92433BB50E99FCED6961A46BC52811472A329C87D69D7FEF1D081D76B7F9095DF623C071606991324312467486 2DF8BE0C5B145C8
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:\ProgramData\Microsoft\Windows\WER\Temp\WERE79D.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Jan 15 03:32:59 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	45124
Entropy (8bit):	2.098341530597131
Encrypted:	false
SSDEEP:	192:iy8ESGlOJZN9hk6j8JxA7og3Nw//23doYpZDgHLPtelqSi:lSXJD9h7j8JM3Nw//QKYpZDPc3
MD5:	DAB40B8A2FE746E26BD59BF1F619D0B3
SHA1:	997A811F47D255D8D0122ABBA88DCF5C55B2AF63
SHA-256:	F92B6C9AE0E483FBCB33AC6439A2EF5037B44FF2CC6D551DDC85579E5186E2C2
SHA-512:	001F72EDDDB7281F7171FE0440AA788B119142E9BFE95BD1C45AA4D717744C4C264FD85BD5DB220859B26C7ED11066EB5AEDC378BD659BB631903B40E94BE9 0
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....k@.a.....$...T.....%.....`.....8.....T.....D.....x.....d.....U.....B..... ...GenuineIntelW.....T.....l...]@.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\WEREDA9.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8348
Entropy (8bit):	3.697343737092656
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi5Z62N6x6YJlSUnhfcgmfMSwGgUgCpBP89bjisfJhm:RrlsNin62N6x6Y7SUhfcgmfMSw/jhfe
MD5:	D514B316FFDBD11B597FD5F66CA24489
SHA1:	6D718BA8A62C1BB7319632453784636A802D7250
SHA-256:	2B1E5FC24CE57AAAFD0293E548E6B8E3593AD7F7C314DBC9A48AD30B29759D23
SHA-512:	4600C40C9A76804BFEB66637ACA1C705836E79CD0A2E172A1FEFC59E9AB08D02F1D50E5AA9FA8393A1A1526D2068B2CA512AAD6A90A4024FD70E6DFF0733C1 9
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.>.6.7.6.4.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2EA.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):	4.467767420732888
Encrypted:	false
SSDEEP:	48:cvIwSD8zsFJgtWI9TxVWSC8Br8fm8M4J2+dZFDA+q84pUVDKcQIcQw0jd:uITffUiSNeJHgmVDKkw0jd
MD5:	3A20FBA7560974648D5C6FD0FBE27049

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2EA.tmp.xml	
SHA1:	1B2936A30334473F327037AD839B933AB7B62DAB
SHA-256:	A4BB07E9135F384984942E1A3465ECE84D992E9D258186FED1A1F8E97542996C
SHA-512:	333835F634DBA55CA56D86FE9FF0F4C2549DB4DF02E65D32E1922EDF8D5BE670CB5F8B5FB8F54A2DA2040846BC901D4832F28C699D2E4B32702D1DB6EA1FA4D
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="1342843" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090
Malicious:	false
Reputation:	unknown
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U...."<ke.....I.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.".g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....==#..M.I..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-..< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.........N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F._..z...._...gY..!Z..?l....vp.l.:.d.Z..W.....~...N.._k...&.....$.....i.F.d.....D!e.....Y..,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1244568012511515
Encrypted:	false
SSDEEP:	6:kK/ik8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:3i9kPlE99SNxAhUeYlUSA/t
MD5:	07CC39D29F4CA82C03F8504E0C7EA130
SHA1:	70415CF2F85A8F938BD8F2B8C6EBF715C456DDFB
SHA-256:	0355462F022A6428FFBA5E817D4F32023BF3DEC73C4B4225DBE147E91525B423
SHA-512:	0BCA6521AD134F78BE1A91967464865A47D7591E941859ED86AFC636DD0565205B273FB6C3603945712F59EA047785ADCB48DF50A8C2A0617D743766A83459F8
Malicious:	false
Reputation:	unknown
Preview:	p..... .....y.....(..... .....q.\}.....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Reputation:	unknown

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.215110798990463
Encrypted:	false
SSDEEP:	12288:c4o+1HZRlIDertUbZuiJLXbIof4B6be/ZVg/bUcY9NZ0GEx2gqVWOA:Lo+1HZRlIDetUbxDhUz5
MD5:	868DF6447DD2874362A5BE2ADAF2146A
SHA1:	2526129D9344E32246BCC0FEC54AB4D11F103242
SHA-256:	3E47D1DB4AC1E014C1CCAC89CD1269991F017F8DB9E735BE47D7DEC809BE0C2F
SHA-512:	688BB08B5B2D3E37B2561124468491797 00A4FE63BA747EEBF4CB74414FE49CCE34E7DD3ED8DD9F453F2CBCAB7D71A7D5D4BD04F31477AFF1502DE9C67DC3E40
Malicious:	false
Reputation:	unknown
Preview:	regfV...V...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.rmtmB,..... ....

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):	2.894669053877629
Encrypted:	false
SSDEEP:	192:nB1yi16rlb5saYd5FSETJq/bDIpn8h8i1ZV6nGoS6:nBge5lAIpn88iTVgGt6
MD5:	8E5C9B7424BDF99BA1911FB3FC1025DF
SHA1:	40EC7528423D63ED6763EE2C849B0EBED3E1BB30
SHA-256:	D7C473E994FCF24BA803756C84131603042C482D06787A0274B23AC0E749A38D
SHA-512:	D916D59AFD76CF95D68E3BB47D128E5E356DBD80DD0ADD819ADA538FA1F9208710B4BB7DA6A9D72C65DE3C62E7890CB68C83A5201290B6FE512533D2574886B
Malicious:	false
Reputation:	unknown
Preview:	regfU...U...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.rmtmB,..... ....HvLE.>.....U.....%S.[..`.I..EhW.....p.....hbin.....p.\..,.....nk,..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ....Z.....Root.....lf.....Root....nk .....}..... .....*.....DeviceCensus..... vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.767598862658865
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:	ALNgwfVtrB.dll
File size:	588288
MD5:	61308ba77d051e4e76e532f9709635e0
SHA1:	95d2cd6c7be346d29735ed970d3f373d37b7e13f
SHA256:	bd2c1b86de45c3e9d0d7c85322228c3512ce2c041765d95bb613cdf12647bea9

General

SHA512:	2baf01ad017b6e5f2940398b8866aed84daa66a069e29e7ecad4dadf4854b206e14e1e8175f59c26f7d6d5a17ea1b2f4e258595d8a33fd4e8675898c576c618
SSDEEP:	6144:cNU5LwA22222GgngDrDRVyYli/ci2tEGW78ODQiE4tvOSk5DKXOW14IkFxVFgY4E:x5w7YM/cYVV7E5OpOJyvnHtytFyQ
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	5.22204269745	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x51000	0x3735c	0x33800	False	0.741035535498	data	6.11335979295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0x3410	0x3600	False	0.306640625	data	4.34913645958	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8d000	0x8c34	0x8e00	False	0.346308318662	data	4.00973830682	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-19:33:26.871063	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49727	80	192.168.2.6	45.138.98.34
01/14/22-19:33:28.093726	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49728	8080	192.168.2.6	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: 6764 Parent PID: 1864

General

Start time:	19:32:45
Start date:	14/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\ALNgwfVtrB.dll"
Imagebase:	0xb80000
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: 00000000.00000002.403379597.0000000000D31000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.378920575.0000000000B50000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.380234706.0000000000B50000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.380280063.0000000000D31000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.403315549.0000000000B50000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.379032722.0000000000D31000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 4616 Parent PID: 6764

General

Start time:	19:32:46
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\ALNgwfVtrB.dll",#1
Imagebase:	0x2a0000
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: svchost.exe PID: 5264 Parent PID: 560

General

Start time:	19:32:46
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:	0x7ff6b7590000
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: regsvr32.exe PID: 3408 Parent PID: 6764

General

Start time:	19:32:46
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\ALNgwfVtrB.dll
Imagebase:	0xf0000
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: 00000003.00000002.421593787.0000000004051000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.421559907.0000000004020000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6048 Parent PID: 4616

General

Start time:	19:32:46
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\ALNgwfVtrB.dll",#1
Imagebase:	0x8b0000
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: 00000004.00000002.377076576.00000000046D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.376980438.00000000046A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6800 Parent PID: 6764

General

Start time:	19:32:46
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\ALNgwfVtrB.dll,DllRegisterServer
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.425302680.00000000054F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.424744123.00000000033B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.425412117.0000000005600000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.425380885.00000000055D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.425231298.00000000053C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.425055302.0000000005200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.425273355.00000000054C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.425444879.0000000005631000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.424828975.0000000003661000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.425344500.00000000055A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6980 Parent PID: 6048

General

Start time:	19:32:48
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\ALNgwfVtrB.dll",DllRegisterServer
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.388319825.0000000005640000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.388061342.00000000053B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.388938400.0000000005A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.388421865.00000000056A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.388494502.00000000056D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.388374896.0000000005671000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.388137915.0000000005460000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.388743358.0000000005900000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.387667842.0000000004E61000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.387995858.0000000005380000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.389038479.0000000005A91000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.388835673.0000000005931000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.387132452.00000000033D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.388209292.0000000005491000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: svchost.exe PID: 4588 Parent PID: 560

General

Start time:	19:32:52
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6b7590000
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: 4680 Parent PID: 4588

General

Start time:	19:32:52
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 164 -p 6764 -ip 6764
Imagebase:	0x1150000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 6496 Parent PID: 6764

General

Start time:	19:32:54
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6764 -s 528
Imagebase:	0x1150000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 4668 Parent PID: 6980

General

Start time:	19:32:55
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Mhgwckn\ikgetkts.aey",QTEnBIyMIuE
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.390300102.0000000004A11000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.389941280.0000000003080000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 4584 Parent PID: 4668

General

Start time:	19:32:57
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Mhgwckn\ikgetkts.aey",DllRegisterServer
Imagebase:	0x8b0000
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: 5688 Parent PID: 560

General

Start time:	19:33:07
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
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: rundll32.exe PID: 400 Parent PID: 3408

General

Start time:	19:33:12
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\ALNgwfVtrB.dll",DllRegisterServer
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2022

Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5796 Parent PID: 560

General

Start time:	19:33:29
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:	0x7ff6b7590000
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: 4532 Parent PID: 560

General

Start time:	19:33:49
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:	0x7ff6b7590000
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: 2932 Parent PID: 560

General

Start time:	19:33:57
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:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Copyright Joe Security LLC 2022

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2022