ID: 532100
Sample Name: mal2.dll
Cookbook: default.jbs
Time: 18:26:06
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

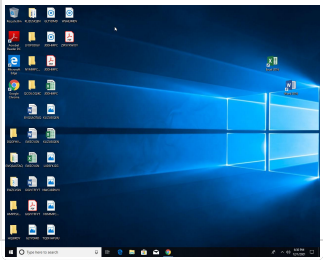
Windows Analysis Report mal2.dll

Overview

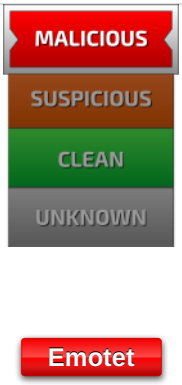
General Information

Sample Name:	mal2.dll
Analysis ID:	532100
MD5:	9efbd03d5576686.
SHA1:	0b821e78137018..
SHA256:	972f9350219dcc2..
Infos:	

Most interesting Screenshot:



Detection



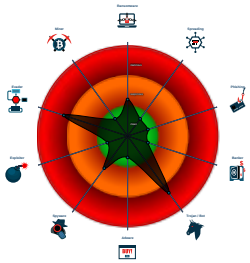
Emotet

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Changes security center settings (no…
- 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…
- Deletes files inside the Windows fold…
- May sleep (evasive loops) to hinder …

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 1456 cmdline: loaddll32.exe "C:\Users\user\Desktop\mal2.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 4892 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\mal2.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4652 cmdline: rundll32.exe "C:\Users\user\Desktop\mal2.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6928 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal2.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3868 cmdline: rundll32.exe C:\Users\user\Desktop\mal2.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6956 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Xjvbeeymcqp\hqokwlnubzbb.uql",vvWvMRmVQ MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6176 cmdline: rundll32.exe C:\Users\user\Desktop\mal2.dll,axamexdrqyrgb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 7028 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal2.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6220 cmdline: rundll32.exe C:\Users\user\Desktop\mal2.dll,bhramccfbdd MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 7124 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal2.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 5064 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1456 -s 304 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4320 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1456 -s 312 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5888 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6240 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6364 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6464 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6704 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6752 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 7116 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 7132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 7140 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5544 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 1456 -ip 1456 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4568 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 168 -p 1456 -ip 1456 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "46.55.222.11:443",
    "104.245.52.73:8080",
    "41.76.108.46:8080",
    "103.8.26.103:8080",
    "185.184.25.237:8080",
    "103.8.26.102:8080",
    "203.114.109.124:443",
    "45.118.115.99:8080",
    "178.79.147.66:8080",
    "58.227.42.236:80",
    "45.118.135.203:7080",
    "103.75.201.2:443",
    "195.154.133.20:443",
    "45.142.114.231:8080",
    "212.237.5.209:443",
    "207.38.84.195:8080",
    "104.251.214.46:8080",
    "212.237.17.99:8080",
    "212.237.56.116:7080",
    "216.158.226.206:443",
    "110.232.117.186:8080",
    "158.69.222.101:443",
    "107.182.225.142:8080",
    "176.104.106.96:8080",
    "81.0.236.90:443",
    "50.116.54.215:443",
    "138.185.72.26:8080",
    "51.68.175.8:8080",
    "210.57.217.132:8080"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.566657802.00000000007A0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000002.642601650.00000000007A0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.567231949.0000000000D2C000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.597839039.00000000007A0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.596491370.00000000007A0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.loaddll32.exe.d33b80.10.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.ba0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.7a0000.9.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.7a0000.9.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.d33b80.7.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 29 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

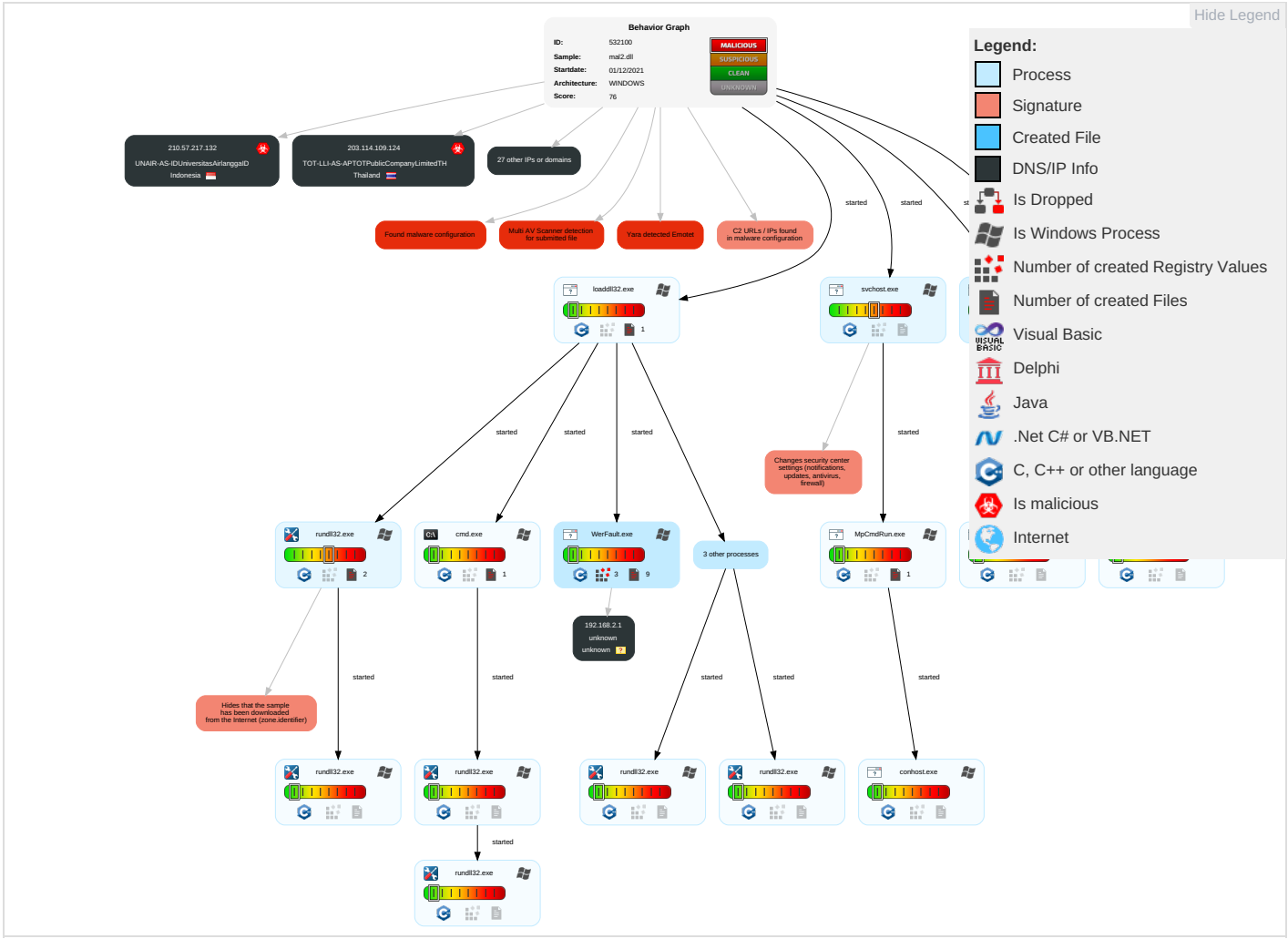
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 1 2	Masquerading 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Security Software Discovery 6 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganogra
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonati
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	File and Directory 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	Rundll32 1	Proc Filesystem	System Information Discovery 3 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfe Protocols

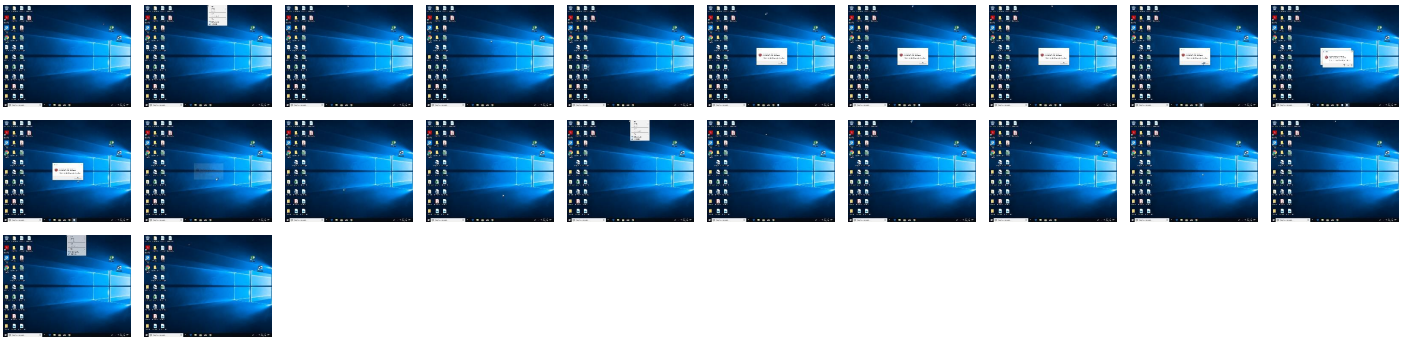
Behavior Graph



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
mal2.dll	6%	Virustotal		Browse
mal2.dll	24%	ReversingLabs	Win32.Trojan.Midie	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.loaddll32.exe.7a0000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.650000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.7a0000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.1060000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.da0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.7a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.7a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.7a0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.ba0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://%s.xboxlive.com/	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.154.133.20	unknown	France		12876	OnlineSASFR	true
212.237.17.99	unknown	Italy		31034	ARUBA-ASNIT	true
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
104.245.52.73	unknown	United States		63251	METRO-WIRELESSUS	true
138.185.72.26	unknown	Brazil		264343	EmpasoftLtdaMeBR	true
81.0.236.90	unknown	Czech Republic		15685	CASABLANCA-ASInternetCollocationProviderCZ	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikaID	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
216.158.226.206	unknown	United States		19318	IS-AS-1US	true
107.182.225.142	unknown	United States		32780	HOSTINGSERVICES-INCUS	true
45.118.135.203	unknown	Japan		63949	LINODE-APLinodeLLCUS	true
50.116.54.215	unknown	United States		63949	LINODE-APLinodeLLCUS	true
51.68.175.8	unknown	France		16276	OVHFR	true
103.8.26.102	unknown	Malaysia		132241	SKSATECH1-MYSKSATECHNOLOGYSDNBHDMY	true
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true
41.76.108.46	unknown	South Africa		327979	DIAMATRIXZA	true
103.8.26.103	unknown	Malaysia		132241	SKSATECH1-MYSKSATECHNOLOGYSDNBHDMY	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.79.147.66	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
212.237.5.209	unknown	Italy		31034	ARUBA-ASNIT	true
176.104.106.96	unknown	Serbia		198371	NINETRS	true
207.38.84.195	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
212.237.56.116	unknown	Italy		31034	ARUBA-ASNIT	true
45.142.114.231	unknown	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	true
203.114.109.124	unknown	Thailand		131293	TOT-LLI-AS-APTOTPublicCompanyLimitedTH	true
210.57.217.132	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
58.227.42.236	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
185.184.25.237	unknown	Turkey		209711	MUVHOSTTR	true
158.69.222.101	unknown	Canada		16276	OVHFR	true
104.251.214.46	unknown	United States		54540	INCERO-HVVCUS	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532100
Start date:	01.12.2021
Start time:	18:26:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mal2.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.evad.winDLL@39/21@0/31
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 10.3% (good quality ratio 9.8%) • Quality average: 72.3% • Quality standard deviation: 24.7%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:27:12	API Interceptor	1x Sleep call for process: svchost.exe modified
18:29:34	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.154.133.20	mal2.dll	Get hash	malicious	Browse	
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	
	9sQccNfqAR.dll	Get hash	malicious	Browse	
	FILE_464863409880121918.xlsm	Get hash	malicious	Browse	
	9sQccNfqAR.dll	Get hash	malicious	Browse	
	t3XtgyQEoe.dll	Get hash	malicious	Browse	
	t3XtgyQEoe.dll	Get hash	malicious	Browse	
	SCAN_35292280954166786.xlsm	Get hash	malicious	Browse	
	U4pi8WRxNJ.dll	Get hash	malicious	Browse	
	oERkAQeB4d.dll	Get hash	malicious	Browse	
	FC9fpZrma1.dll	Get hash	malicious	Browse	
	Z4HpRSQD6I.dll	Get hash	malicious	Browse	
	uLCt7sc5se.dll	Get hash	malicious	Browse	
	rGF1Xgw9Il.dll	Get hash	malicious	Browse	
	nBtjFS1D08.dll	Get hash	malicious	Browse	
	q8HPR8Yypk.dll	Get hash	malicious	Browse	
	mZuFa05xCp.dll	Get hash	malicious	Browse	
	TEm3oBxeXS.dll	Get hash	malicious	Browse	
212.237.17.99	mal.dll	Get hash	malicious	Browse	
	mal2.dll	Get hash	malicious	Browse	
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	
	9sQccNfqAR.dll	Get hash	malicious	Browse	
	FILE_464863409880121918.xlsm	Get hash	malicious	Browse	
	9sQccNfqAR.dll	Get hash	malicious	Browse	
	t3XtgyQEoe.dll	Get hash	malicious	Browse	
	t3XtgyQEoe.dll	Get hash	malicious	Browse	
	SCAN_35292280954166786.xlsm	Get hash	malicious	Browse	
	U4pi8WRxNJ.dll	Get hash	malicious	Browse	
	oERkAQeB4d.dll	Get hash	malicious	Browse	
	FC9fpZrma1.dll	Get hash	malicious	Browse	
	Z4HpRSQD6I.dll	Get hash	malicious	Browse	
	uLCt7sc5se.dll	Get hash	malicious	Browse	
	rGF1Xgw9Il.dll	Get hash	malicious	Browse	
	nBtjFS1D08.dll	Get hash	malicious	Browse	
	q8HPR8Yypk.dll	Get hash	malicious	Browse	
	mZuFa05xCp.dll	Get hash	malicious	Browse	
	TEm3oBxeXS.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ARUBA-ASNIT	mal.dll	Get hash	malicious	Browse	• 212.237.56.116
	GYRxsMXKtvwSwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	KsXtuXmxoZvgudVwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	xTpcaEZvwmHqwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	mal2.dll	Get hash	malicious	Browse	• 212.237.56.116
	GYRxsMXKtvwSwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	KsXtuXmxoZvgudVwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	xTpcaEZvwmHqwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	invoice template 33142738819.docx	Get hash	malicious	Browse	• 94.177.217.88
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 212.237.56.116
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 212.237.56.116
	9sQccNfqAR.dll	Get hash	malicious	Browse	• 212.237.56.116
	FILE_464863409880121918.xlsm	Get hash	malicious	Browse	• 212.237.56.116
	9sQccNfqAR.dll	Get hash	malicious	Browse	• 212.237.56.116
	t3XtgyQEoe.dll	Get hash	malicious	Browse	• 212.237.56.116
	t3XtgyQEoe.dll	Get hash	malicious	Browse	• 212.237.56.116
	QUOTATION FORM.exe	Get hash	malicious	Browse	• 62.149.128.45
	MA4UA3e5xe	Get hash	malicious	Browse	• 46.37.10.252
	SCAN_35292280954166786.xlsm	Get hash	malicious	Browse	• 212.237.56.116
	seL794VuEm	Get hash	malicious	Browse	• 31.14.139.79
OnlineSASFR	mal.dll	Get hash	malicious	Browse	• 195.154.133.20
	mal2.dll	Get hash	malicious	Browse	• 195.154.133.20
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 195.154.133.20
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 195.154.133.20
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 195.154.146.35
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 195.154.146.35
	AtlanticareINV25-67431254.htm	Get hash	malicious	Browse	• 51.15.17.195
	9sQccNfqAR.dll	Get hash	malicious	Browse	• 195.154.133.20
	FILE_464863409880121918.xlsm	Get hash	malicious	Browse	• 195.154.133.20
	9sQccNfqAR.dll	Get hash	malicious	Browse	• 195.154.133.20
	t3XtgyQEoe.dll	Get hash	malicious	Browse	• 195.154.133.20
	t3XtgyQEoe.dll	Get hash	malicious	Browse	• 195.154.133.20
	67MPsax8fd.exe	Get hash	malicious	Browse	• 163.172.208.8
	Linux_x86	Get hash	malicious	Browse	• 212.83.174.79
	184285013-044310-Factura pendiente (2).exe	Get hash	malicious	Browse	• 212.83.130.20
	MTjXit7lJn	Get hash	malicious	Browse	• 51.158.219.54
	SCAN_35292280954166786.xlsm	Get hash	malicious	Browse	• 195.154.133.20
	gvtdsqavfej.dll	Get hash	malicious	Browse	• 195.154.146.35
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 195.154.146.35
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 195.154.146.35

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

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false
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):	0.24942706526168892
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4x:BJiRdwfu2SRU4x
MD5:	46882A6830E76E84809FF61D41FC1A60
SHA1:	62C986CAD7FC75056669C8366B6299D7EC088CA9
SHA-256:	763C6AFC1CDB01A68D4CA86AB03C92DF28C1E60C840AECC73FA960C48D26CD32
SHA-512:	37F2DC3EA70AA2A9926010784A619B78AB5BA70F4CEA1C466C68699E59F9E360473A906AF50895BFCDB42980BDDBC1CB321E9D8FF432F1628A9F65A99FC08B2 9
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xecb7d22b, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2506006063210868
Encrypted:	false
SSDEEP:	384:xrK+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:xrlSB2nSB2RSjlK/+mLesOj1J2
MD5:	A47C47EF3D00475460F84F8516370E92
SHA1:	7F689445BF7967C5252B85CA244EE87D5B5C30C9
SHA-256:	4F0043163E1434024C3DE253F0DAF6FE34477506B00A169EF90DEEEDC8B172BE
SHA-512:	6B1E60A8946E8B00D01C081063CCDF145032767B76CDF694A59EA509638174C19BDD9729C46399A14547497884C5D94C0EF0CAAA77D91B7C62C612F482849951
Malicious:	false
Preview:	..+... .....e.f.3...w.....).....y.....y#.h.(.....y....).....3...w.....B.....@..... ....N>8`.....y.....A.....y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07605342734948045
Encrypted:	false
SSDEEP:	3:rVT7vpPA4np/l/Ky67cyORShtl4AyOl/ill3VkttlmlnI:RTrJAY/l/P67cyORifyOl/G3
MD5:	400EA9108E962862766500814F7D3466
SHA1:	87F9A5FC0B7C862F8C32D5847BCEF1C9450FE8A3
SHA-256:	FD04432EDFD989575D48B36ECC56286B108A9917AB6A23E340A5168DB780C7BF
SHA-512:	BABB9019C2631B2095B88F19BBEE29A3892C4F098ECFB31435FC669300F08C29AF03AD8315290324CFEFABD9BFBAB0EC8C3270767ABB8540E7057955297334E
Malicious:	false

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Preview:	8.....3...w.....y.....y.....y.....y..x.....y.....A.....y.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_747b3d3843a661accc8c92924ccfd5a2e2d128_d70d8aa6_12d2c47d\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):	0.6740553107090325
Encrypted:	false
SSDEEP:	96:vh2Zqy4ky9hkoyt7JfqpXIQcQ5c6A2cE2cw33+a+z+HbHg4VG4rmMOyWZAXGng5+:OBwHnM28jj0q/u7sQS274ItW
MD5:	BE82113082E2819C42982B02E0A9BD2E
SHA1:	0063CD51A4884D06C037EDAED974D114F1AE3B69
SHA-256:	71EA212CDCB5DA9D3FB46094F4F25860CC7938FFBC922EAE53A7DE6F02E5149F
SHA-512:	1D8AA30CA1532B3DE428D0974918460BE02EFD9398FB2C1CDB40A1D53B2C62F1164F4CBD86D1CA9591DB41EE2C8F0F476957712E2598B23B9354398E5BB4BE1F
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.8.8.5.7.8.2.7.4.8.5.7.8.7.....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.=.e.2.6.4.7.0.1.f.-.4.b.f.f.-.4.a.a.5.-.9.7.c.a.-.9.6.d.8.6.6.f.f.1.5.f.d.....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.=.5.6.6.6.1.7.1.1.-.e.1.3.8.-.4.9.4.1.-.b.f.b.5.-.b.5.f.7.a.9.4.9.9.7.d.1.....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.=.0.0.0.0.0.5.b.0.-.0.0.0.1.-.0.0.1.6.-.a.b.1.c.-.c.4.1.b.2.4.e.7.d.7.0.1.....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././.0.9././.2.8.:.1.1.:.5.3.:.0.5.!.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\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_11fb1c03\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):	0.6753216957227272
Encrypted:	false
SSDEEP:	96:0RFB82ZqyFky9hk1Dg3fWpXIQcQec6XFcE1cw3f+a+z+HbHg4VG4rmMOyWZAXGn5:ALvBmHgx/Lj0q/u7sQS274ItWA
MD5:	5B1C5CCFBA925A0022F40E0CEE00FEDB
SHA1:	CA6DA28C640B5982213ACEF6FEC1B111C089EE22
SHA-256:	57535D7DA24E9548E19ECAE80CEA01F7D68326C3EEC78D647305F3F7B3399D1F
SHA-512:	9E180B8A14A0384BB34784E16FEFD92EEFE4E8A22CA103E3B247174517DD7C14744873A5FDBA32867C6EC161CBEA45DB3C043E6A26CBE62D1B0F7C9A52D400E6
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.8.8.5.7.9.2.9.1.7.2.0.6.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.2.8.8.5.8.0.7.3.7.0.3.0.2.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.c.1.d.6.8.5.4.-.3.6.a.8.-.4.2.5.3.-.b.2.c.5.-.e.b.7.c.4.7.a.4.8.c.a.6.....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.=.d.3.5.0.b.8.0.5.-.a.b.8.f.-.4.3.e.f.-.8.e.e.5.-.a.3.6.3.8.d.8.7.f.1.e.5.....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.=.0.0.0.0.0.5.b.0.-.0.0.0.1.-.0.0.1.6.-.a.b.1.c.-.c.4.1.b.2.4.e.7.d.7.0.1.....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.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB46F.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 02:29:43 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	26296
Entropy (8bit):	2.5210712860247995
Encrypted:	false
SSDEEP:	192:BLSTpuda2OX0cYPKfXHWRlhvnQsPPud0MnY:MpBX0DPKf3WTh4sPPuK
MD5:	AAB65F6BFD0CCCB966FA7D8B3C42EED1
SHA1:	C5208BC22BF1768A49E1FAC1868CE5786BC7496B
SHA-256:	DB94B5E3D75A56D250D4A656C127B918D42A8B88635C72D0D4C3811F2C23DE9E
SHA-512:	80C7C663745DFD436D820EC3A4CB847A873044C959406F86D06FEFCE4C7B287FE7F59AF624DC3FA71D49D216C1808DC199FB2DCBC01E3B0EF65D3FF91843DE5
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB46F.tmp.dmp	
Preview:	MDMP..... ...../.a.....4.....H.....$.....`.....8.....T.....h...PZ.....U.....B.....p.... ...GenuineIntelW.....T.....a0.....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\WERB8C6.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):	8340
Entropy (8bit):	3.702469143283619
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNisX6TBi6YIFSUEsgmfcSzpCpBx89bL5sfG5m:RrlsNi86Q6Y6SUEsgmfcSzdLSfJ
MD5:	E1387B79527B0F7C5B2F7AF6E4A19E54
SHA1:	44B0651BB01C15A2813E87D0D623A0F02354EA1B
SHA-256:	420AE0927113DAF8FD0BC36D83AB80D62239FB7E9B7AE97DDF382FD72CDEFAA0
SHA-512:	90FF0BC1B0684C978CA4F9F9E01155AE4E8916BC0D8F67C212B0CF8604990839FB228A0A88D222375F7EC8A0D38D31ACB5B5CC1EB8F8CE7F112C8E22437C2D 1
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.4.5.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBC41.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):	4.478117007255109
Encrypted:	false
SSDEEP:	48:cvIwSD8zs7uiJgtWl9HoSWSC8Bv8fm8M4J2ynZF8+q84WDhKcQIcQwQVTd:ulTf7uwsozSNOJ1YYhKkwQVTd
MD5:	2D3F62C4A24855DABE5433BF864A0808
SHA1:	425FDF2F32B9B96E06F14A0737032C6D05F1D61F
SHA-256:	BFA43B078D32ADB3D8A78A94108E56A392A80539D2F451E338647F61858FFF58
SHA-512:	E5EFF8935C708AC7EC8E4369A8298403270A2122C8322906F03BD239AE207F9F4C7102A3CE9BC57E7B77DB8AC566D6CCF6828A774E487AA1863B3D4C0F47AEE
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1279420" />.. <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\WERD250.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	48280
Entropy (8bit):	3.0668805174003246
Encrypted:	false
SSDEEP:	768:4oHIWaUE2sVcr22+ktXYVnZiCnN/17yikONct9d3FA/vEyaw/R:4oHjaGsVcr22jtXYVnZiUN/17yikONc6
MD5:	9D6EA18F0C9A3E42895DCE6A7D053153
SHA1:	292776A1784841FB8747847B331AF63CC0BE3B5F
SHA-256:	3AA4FBF2E7004BFF21138200358B14F8163767731CD42A4A998E08E996458596
SHA-512:	913AC1F2E21B5404A28B0356EC0057597A93DFBDDCC637789FE779810B498D183C0FF51835096716F6A9B64881245FA91117A43B53256F2283DC87ADC311440E
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD704.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.69398988774531
Encrypted:	false
SSDEEP:	96:9GiZYWfo9Ye2gYJpYVWqpOH+UYEZ2LtFivZWoAwOO3AO2adEYcRolhS3:9jZDYgqkoadEYcRPhS3
MD5:	8BCF9317469B01F7DA25DEBEB94A1BC3
SHA1:	0C8E3189A1989713BC69F55BCECC9A7259C59EDC
SHA-256:	81A00250D03925CE08193E09D29FCA1034984D12ED7268F7DA2FEEC1F3505B99
SHA-512:	F95E1979E53BBAD689D698DDDAACEBFC7EBD6028951D7C282A6506D9F445162CBBE227DBB0BE3F8611278FD796AF85D75093BCCE69E13EE2066322B3FE4D1(E9
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC2B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 02:29:53 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1059292
Entropy (8bit):	1.3394211426156184
Encrypted:	false
SSDEEP:	1536:Q63A0FeV+OijAJl3zesnL+c+Nxn0zdC8JytfBLfVt5YotOWr8/OQK:X3A0FeEjssnL+c+Nxn0zdCxfBLfCjK
MD5:	B6F12D89DCD06074C15E346D0C902E31
SHA1:	13044E542E7BDE9206E9825793CF5F392E16F43D
SHA-256:	1D1EA0E145FECBFAE10B1267DF2ED6619DB413D1A0AB930E4065875FF9939DA1
SHA-512:	F2B7A31FE3A5BA908E540A5CC7F97752D386C3330A40DA992ED29C668251EFCC33D6A5A39F7A77C9D2D53E195E9ABFB3599C62B836B2AFB9F9F4BC53B3930A B2
Malicious:	false
Preview:	MDMP..... ...../.a.....4.....H.....$.....`.....8.....T.....@.....U.....B.....p.... ...GenuineIntelW.....T.....a1.....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\WERE6BB.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):	8298
Entropy (8bit):	3.695238338561699
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNisA6oi6Yl0SU/gmfL8GS5JCpDx89bj5sfNBm:RrlsNir6F6YLSU/gmfLrSJjSfi
MD5:	E93183C3F58E98E6C1E7DA3D5B4F4ACE
SHA1:	A380DC8E1EC24DE82245EAFAA86E036038CCB650
SHA-256:	9825CFD4238956F06D375D3065938D03A0CEEED6C4E657DE6CD2A3D1FA28FAF3
SHA-512:	6A8FEF1588000E848EE4D5DAF9B3F4BF5E7674173D660D76C679AE8E87A6650D2FF860739D8F93C284A1EFA17BD3CBD0BAAE2A87DFD21D6B607ED26E8440A5 AA
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.4.5.6.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREAD3.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4558
Entropy (8bit):	4.432755522380974
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREAD3.tmp.xml	
SSDEEP:	48:cvIwSD8zs7uiJgtWl9HoSWSC8Bl8fm8M4J2yGtFmIp+q84tjNKcQIcQwQVTd:uITf7uwsozSNwJExpxNKkwQVTd
MD5:	0CCD3E2FE0BCD82AFC1EF99DC0F4B7FE
SHA1:	540B7C5A57950860C3DAB0B07F22C461C6B52EB1
SHA-256:	8AF913F7FD1C2FA96865DCC8F62FB4F94C9A32F673AB8AB2C91864911CD94E65
SHA-512:	17F8597FDC2A882CDF0D114DE481520B9D0B836DE350B743319050FA2D782ED674037CF05E655591D8ACADCC3483BBE26994C3ACA0C290E0E9E080D0553B17A
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1279420" />.. <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\WERF3D.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6939928290108095
Encrypted:	false
SSDEEP:	96:9GiZYWcZVqGYIYyWqHbRHsUYEZojtriIZZonwrXVa1PUKxjzIQj3:9jZDyPK/la1PUKF8Qj3
MD5:	56AE4194C1BB65AD9AF492B9491A5C71
SHA1:	15B5F6602BEE253ED6D9CE5F8010BD8FFAC71029
SHA-256:	7212649472ABFBE93D55BB3A2E96A261A09CCAB292AFBB723DDD54E1C2CCAD8D
SHA-512:	1E12ADF8EABC2AEF70D8D7074ABA57BA47A0F9AFEEF3BB9105CA4ACCACA404C328625FA037093DC0555CD2C7CA051CE23560CA582F71AE01CA271C8A0BDAFFEA
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFDB.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	47834
Entropy (8bit):	3.066530967527075
Encrypted:	false
SSDEEP:	768:CaHU6UEZjoSW22BktVgDVnZnKINpg7y8kMRg8tHZ1/RiYr:CaHU6pUSW22itVgDVnZnDNpg7y8kMRgy
MD5:	CCAEEAC32B5802D28F61DC7EB35C34B6
SHA1:	22B309FDB15FE6C3A19670D7F3C60B029CD95906
SHA-256:	DB8FF87D34A276D88FD5E154A2EFEE86C440FAEDB82344B95A7D7FE6DC6A5F53
SHA-512:	0646030B04F91F7B5BFE28C6579E645FD3B70DB7215403B6559DF66CCF82B57756BE2928B58D996F6CC2160ABD21AF378466A81D19E4896F765D475F6B130F42
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\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
Malicious:	false

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
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):	3.166050568584806
Encrypted:	false
SSDEEP:	96:cEj+AbCEH+AbuEAc+AbhGEA+AbNEe+Ab/Ee+AbPE6w9+Ab1wTEl+AbB:cY+38+DJc+iGr+MZ+65+6tg+ECa+I
MD5:	95A18A0B546B551A9112E9FEBA266B36
SHA1:	BA13E20597440DEEA08F7EA9DE5005359510D0FF
SHA-256:	BC6DE2D0EDE221EB64960702F74D1F894897F276389FC07DC69E9033E5671555
SHA-512:	5C5B0A1E2C37559134482364E07549587E2B95FD07671E45F23AC5C45F975B89F9A1EBD40D51B5CC108E9588C82420F1F5131B5BC4766757EE6ED08A30FCD56A
Malicious:	false
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.20211202_022741_833.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.8177630021785336
Encrypted:	false
SSDEEP:	96:g7CTaIPo+U/5lD9S/YqVCDCI2lOfk0c4v+T2XjFz5NMCvdJRwj5DNTNMCYj5YUMd:VZg46N2gAVCLRCVCEC9CKCl
MD5:	E0D1E78802BDE82B83FD99A15EF7BABA
SHA1:	B3DC38EBD2659EFBA4CE05162C54A32E76DCE98A
SHA-256:	DF16AD69D70D465FAC34CB8F4053CA88A4438A02C8BF5535B4F7BBCF7195E661
SHA-512:	6846993E4645CD270596CA5029BBDABCDCC92E870D60F713D2FB9951DB55C4C04A03E19601FCA11AA80FA8926067E4A0C338A5B40E9C180873A3CB3D5DCD87 6
Malicious:	false
Preview:	....!....................................C......................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..... .....m...$...........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...2.0.2.1.1.2.0.2._.0.2.2.7.4.1._.8.3.3...e.t.l.........P.P..........C.. ....

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):	4.264641005685364
Encrypted:	false
SSDEEP:	12288:USVCOdRHvb/XjPUXtSa8TRl6R5Umg2VnPr4kgjEDbCOKnf4QK3DjTvZl:tVCOdRHvb/XjPUXeN0fl
MD5:	045F66989BC9205C456E041FFFC8F4ED
SHA1:	658910D42949706991D1B2456FA0A15ED51EFEE2
SHA-256:	494836BB7203B77BD212C641C1FFC4C82CA86FE0A8716604C8982D62B53FBE3A
SHA-512:	ED4A3D464C136F03D4269F9EE9EFF039C0A6EEC10936E701C940BA314A7B60ED3AE838F0C0D7F82A804F89D406D34EEB5F5EE48656C556848690DF487CEDBE E
Malicious:	false
Preview:	regfR...R...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.W.s$.. ....

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

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Entropy (8bit):	3.0508349292287393
Encrypted:	false
SSDEEP:	192:xXiqAM1ayVRDlfYb5FSE9lMqXyQVWnxuYW2oCKqe8mxwpLuN5Z:pi5z5TXQnxuf2oCPmxwpLuN5Z
MD5:	F1B58F5B7D299D4061CA93F06CEB6B6E
SHA1:	ED84123DB60948661D8BAE7F50B35057673F4ADC
SHA-256:	E3BD54AA97BE3E68FBF0C4A185A622D67132835F785F516BCF5EA231B3E23E29
SHA-512:	FC0223155CA4449DEE6E02153E8EA25A9AE0BD287A74BEFB23209FB3DAB580BFEB96F0CA02E371994E2C67A435155AD035215F0CA3FFBFBFF88BCD2C85E1A9A6
Malicious:	false
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.W.s$..... ....HvLE.>.....Q.....j{L...0.....hbin.....p.\.,.....nk,....s$.....@..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ....s$..... .....P..... .....Z.....Root.....lf.....Root....nk ....s$.....}..... .....*.....DeviceCensus..... ...vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.970959661903669
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • 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:	mal2.dll
File size:	387072
MD5:	9efbd03d5576686dd9f0678c09abe9fc
SHA1:	0b821e78137018bbf3f9c67d3b049e33d5b36ae5
SHA256:	972f9350219dcc2df463f923ec5b559f4ab69f083da9ccbd0976c51bc19f3f5b
SHA512:	fa2def2a793d79b63cf2c808c62e031544282bc3e01f97efa47b3114c702b004d767b818764f47c120007c680274ad9327587ac235186ee6e6d7bb168a19acc9
SSDEEP:	6144:zBYrPMTsY8GR3j4fubnY6Zs/Bv6yM6aSTsfA2qL6jpXNcc6CEteuQJPIgtlpZ5L:yhmT4GbnYks/BJNWo2LjpScDEteuOIoZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0...Q...Q...Q..E#...Q..E#...Q..E#...Q../$...Q...$...Q...$...Q...$...Q..E#...Q...Q...Q...Q...Q../$...Q../$...Q..Rich.Q.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1001cac1
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A73B52 [Wed Dec 1 09:07:30 2021 UTC]
TLS Callbacks:	0x1000c340
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0

General

File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	609402ef170a35cc0e660d7d95ac10ce

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x28bb4	0x28c00	False	0.53924822661	data	6.1540438823	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2a000	0x32362	0x32400	False	0.817800645211	data	7.40644078277	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5d000	0x1ba4	0x1200	False	0.287109375	data	2.60484752417	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x5f000	0x4c4	0x600	False	0.360677083333	AmigaOS bitmap font	2.17228109861	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x60000	0x1bc0	0x1c00	False	0.7880859375	data	6.62631718459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 1456 Parent PID: 6140

General

Start time:	18:27:10

Start date:	01/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\mal2.dll"
Imagebase:	0x1170000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
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: 00000000.00000000.566657802.00000000007A0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.642601650.00000000007A0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.567231949.0000000000D2C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.597839039.00000000007A0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.596491370.00000000007A0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.568652514.00000000007A0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.643009162.0000000000D2C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.596841009.0000000000D2C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.598456484.0000000000D2C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.568840979.0000000000D2C000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 4892 Parent PID: 1456

General

Start time:	18:27:10
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\mal2.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: rundll32.exe PID: 3868 Parent PID: 1456

General

Start time:	18:27:10

Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\mal2.dll,Control_RunDLL
Imagebase:	0x10d0000
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: 00000002.00000002.545043648.0000000001060000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000003.526115475.0000000003368000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 4652 Parent PID: 4892

General

Start time:	18:27:11
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\mal2.dll",#1
Imagebase:	0x10d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.543502348.0000000000BA0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.543542843.0000000000CFA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 5888 Parent PID: 556

General

Start time:	18:27:11
Start date:	01/12/2021
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: rundll32.exe PID: 6176 Parent PID: 1456

General

Start time:	18:27:15
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\mal2.dll,axamexdrqyrgb
Imagebase:	0x10d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.564875818.000000000328A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.564446850.0000000000DA0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6220 Parent PID: 1456

General

Start time:	18:27:21
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\mal2.dll,bhramccfbdd
Imagebase:	0x10d0000
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: 00000006.00000002.564537877.000000000076A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.564451857.0000000000650000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6240 Parent PID: 556

General

Start time:	18:27:21
Start date:	01/12/2021
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
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6364 Parent PID: 556

General

Start time:	18:27:36
Start date:	01/12/2021
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
Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6464 Parent PID: 556

General

Start time:	18:27:43
Start date:	01/12/2021
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: SgrmBroker.exe PID: 6704 Parent PID: 556

General

Start time:	18:28:02
Start date:	01/12/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff711470000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6752 Parent PID: 556

General

Start time:	18:28:18
Start date:	01/12/2021
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

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6928 Parent PID: 4652

General

Start time:	18:29:18
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal2.dll",Control_RunDLL
Imagebase:	0x10d0000
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: rundll32.exe PID: 6956 Parent PID: 3868

General

Start time:	18:29:18
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Xjvbeeymcqp\hqok wlnubzbb.uql",vvWvMRmVQ
Imagebase:	0x10d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7028 Parent PID: 6176

General

Start time:	18:29:26
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal2.dll",Control_RunDLL
Imagebase:	0x10d0000
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: MpCmdRun.exe PID: 7116 Parent PID: 6752

General

Start time:	18:29:33
Start date:	01/12/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff737de0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Written

Analysis Process: rundll32.exe PID: 7124 Parent PID: 6220

General

Start time:	18:29:33
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal2.dll",Control_RunDLL
Imagebase:	0x10d0000
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: conhost.exe PID: 7132 Parent PID: 7116

General

Start time:	18:29:33
Start date:	01/12/2021
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: 7140 Parent PID: 556

General

Start time:	18:29:33
Start date:	01/12/2021
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

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 5544 Parent PID: 7140

General

Start time:	18:29:34
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 1456 -ip 1456
Imagebase:	0x1360000
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: 5064 Parent PID: 1456

General

Start time:	18:29:36

Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1456 -s 304
Imagebase:	0x1360000
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: WerFault.exe PID: 4568 Parent PID: 7140

General

Start time:	18:29:48
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 168 -p 1456 -ip 1456
Imagebase:	0x1360000
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: 4320 Parent PID: 1456

General

Start time:	18:29:50
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1456 -s 312
Imagebase:	0x1360000
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 Modified

Disassembly

Code Analysis