ID: 532106
Sample Name: mal.dll
Cookbook: default.jbs
Time: 18:36:43
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

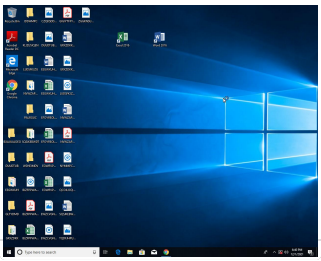
Windows Analysis Report mal.dll

Overview

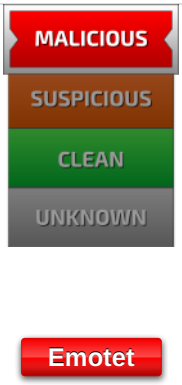
General Information

Sample Name:	mal.dll
Analysis ID:	532106
MD5:	9efbd03d5576686.
SHA1:	0b821e78137018..
SHA256:	972f9350219dcc2..
Infos:	

Most interesting Screenshot:



Detection

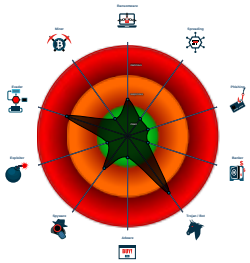


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Found detection on Joe Sandbox Clo…
- 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: 6524 cmdline: loaddll32.exe "C:\Users\user\Desktop\mal.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6552 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\mal.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1432 cmdline: rundll32.exe "C:\Users\user\Desktop\mal.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5784 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1324 cmdline: rundll32.exe C:\Users\user\Desktop\mal.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6444 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jxqjexglbxuwcsnd\ncmurmkelbjyq.yqk",ewrKlpBownvGxgM MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2132 cmdline: rundll32.exe C:\Users\user\Desktop\mal.dll,axamexdrqyrgb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5304 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5300 cmdline: rundll32.exe C:\Users\user\Desktop\mal.dll,bhramccfbdd MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5644 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 5316 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6524 -s 308 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 2804 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6524 -s 344 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4932 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6964 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6224 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6524 -ip 6524 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3732 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 572 -p 6524 -ip 6524 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
00000000.00000000.650731221.0000000000C3C000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.649143533.00000000007B0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.676710015.0000000000C3C000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.649539674.0000000000C3C000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.620619819.00000000029C0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.loaddll32.exe.c42f68.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.29c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.c42f68.7.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.c42f68.10.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.7b0000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 25 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

System Summary:

Found detection on Joe Sandbox Cloud Basic with higher score

Hooking and other Techniques for Hiding and Protection:

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

Stealing of Sensitive Information:

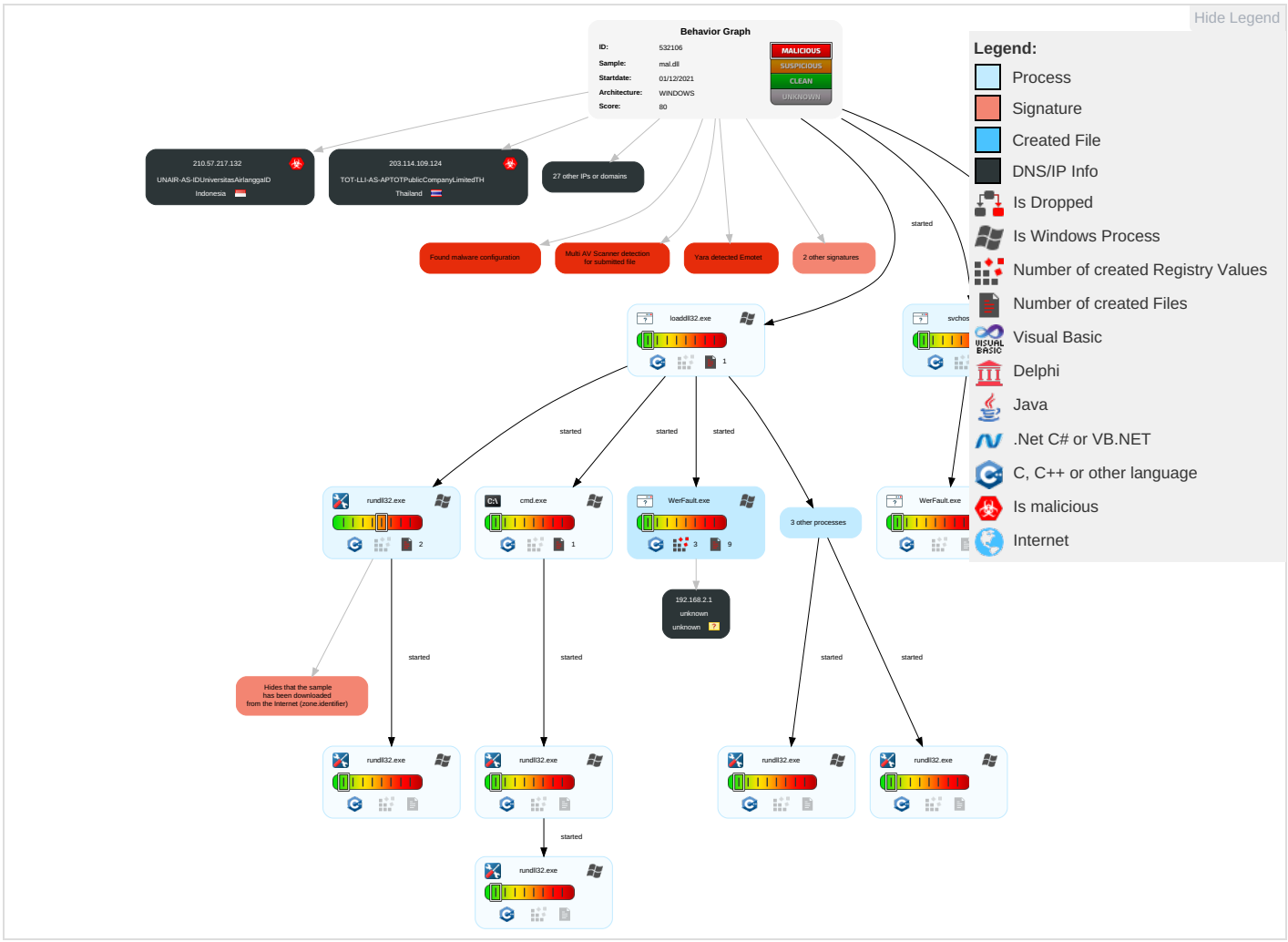
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	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	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Security Software Discovery 5 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	System Information Discovery 3 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

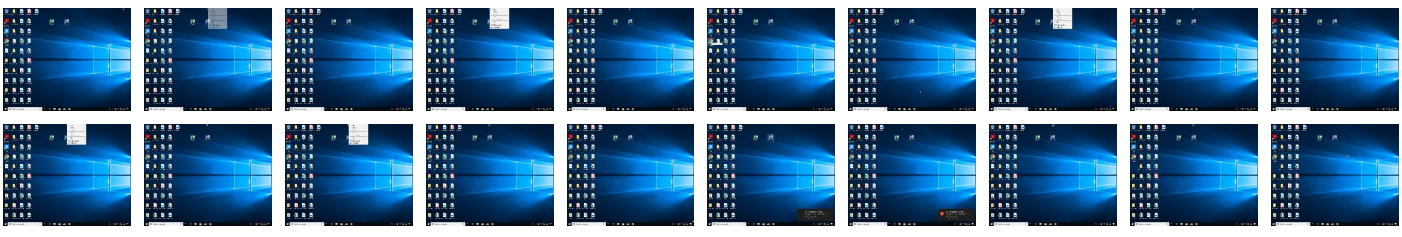
Behavior Graph

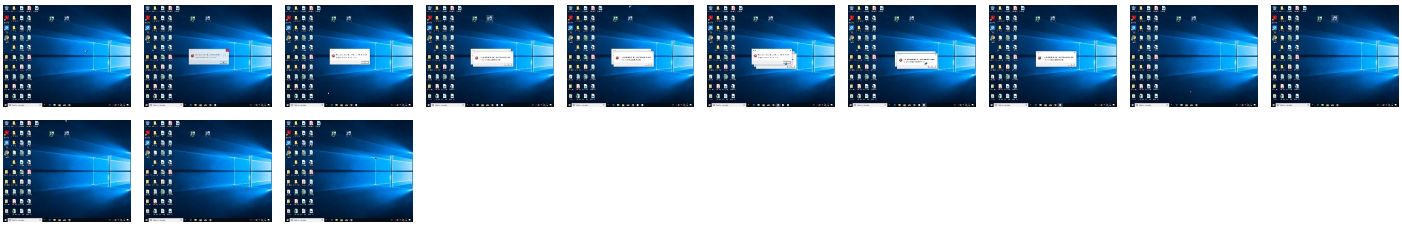


Screenshots

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
mal.dll	24%	ReversingLabs	Win32.Trojan.Midie	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.loaddll32.exe.7b0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.7b0000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.2c10000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.2780000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.7b0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.2d60000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.7b0000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.29c0000.0.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	

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
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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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:	532106
Start date:	01.12.2021
Start time:	18:36:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mal.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:	22
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:	mal80.troj.evad.winDLL@31/18@0/31
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 17.9% (good quality ratio 17.1%) • Quality average: 71.9% • Quality standard deviation: 24.5%
HCA Information:	• Successful, ratio: 76% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:39:28	API Interceptor	1x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.154.133.20	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	
212.237.17.99	mal2.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ARUBA-ASNIT	mal2.dll	Get hash	malicious	Browse	• 212.237.56.116
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mal2.dll	Get hash	malicious	Browse	• 212.237.56.116
	GYRxsMXKtwSwhoreniggagay.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
OnlineSASFR	mal2.dll	Get hash	malicious	Browse	• 195.154.133.20
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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):	0.248598563745147
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4m:BJiRdwfu2SRU4m
MD5:	CEAE2DB47CE8C24ED5DADE99415E85A6
SHA1:	FE6069BE3FC50906B6D16E1B0467B3E76BACD4EE
SHA-256:	11C84C83DB6D353DC2D36623672967040E4AD44FD08A9223095A8BF47B156A5E
SHA-512:	73E2367BDF324F372E6FB12A15F195BF41368E8DF23BE450D948F839C87F95B05F25A6F2E9C5E83F6C916CDD19BFB19F4F668BD3C30049FF488923163049FBB3
Malicious:	false

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
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 0x450f8f8a, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25066881879413755
Encrypted:	false
SSDEEP:	384:M+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:TSB2nSB2RSjlK/+mLesOj1J2
MD5:	2B910197B18D4E99EC3FCF8398C7C321
SHA1:	713A0D479C03AC930151338D2C52EC4B0A2111D8
SHA-256:	48A4FD15A60DCE4D772390B1DCCC1FB10B064A93F08DE88A2D9EA6A8C1993266
SHA-512:	7BAB0E1273301135A63288533AD0DD7BA25CC3C446E9CDE4071DB243B1395192985BB82BD15B5EF2BBDF970236904CF2DF82C19FEAB8910966C2B3231BFC457
Malicious:	false
Preview:	E..... .....e.f.3...w.....&.....w...'...yS.h.(.....3...w.....B.....@..... ....3...w..... .....J..'...y.....#...'...yS..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07713236509382654
Encrypted:	false
SSDEEP:	3:Q/l1Ev4Cpcw8l/bJdAtiaU4CnEll3VkttlmlnI:Q/lQ4Cpd8t45U4uM3
MD5:	D83879C90B026F0111D4AB358C4B1BC7
SHA1:	8D403DAE39A0CF734E8C68C9B026AD5023CCC895
SHA-256:	B7D691FD806FFEBEB5FE84ADAC09B4EA23019E551071A75AB644DB8E3C9D9C78
SHA-512:	7ADBBD19717DFAD92118C5B21985B1CD74E22ACD31B15250C60802D12D9CE536BD01ED730BE1D9F6EEA61DB360D6C53173140C25DE21E2358251B3FC05D88E
Malicious:	false
Preview:	.{d!.....3...w...'...yS.....w.....w.....w...:O.....w.....#...'...yS..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_8c5962cbbdb13a8671f1f3c3793157e73bd5d897_d70d8aa6_154f1fea\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):	0.6738757938696471
Encrypted:	false
SSDEEP:	96:cueJk3ARKgZqyiy9hkoyt7JfapXIQcQ5c6A2cE2cw33+a+z+HbHgOVG4rmMOyWZQ:c4LiB7HnM28jjSq/u7sYS274ItW
MD5:	3979C938293636DFE1825F076E48B744
SHA1:	2A0BDCA11089394BFBF79AD5085AEF011B333099
SHA-256:	A0C8A7850F565271357535E70DE6FBDF5F924CC5232D411CBB6BE67B80C614DF
SHA-512:	36A38DA82660A3F73A7AD611A75A80419E22568BE073062507E08190C1CAF085EB9459A28B1A9218935FA13C3E007662BD32E4D0727D8A5851118234AE94E4EB
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.=.1.3.2.8.2.8.8.6.4.3.2.4.0.3.3.9.8.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.4.9.7.1.f.e.3.-.1.d.2.a.-.4.f.6.b.-.9.b.3.d.-.d.3.2.c.6.8.e.2.f.c.b.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.0.2.1.4.8.6.6.-.e.a.e.b.-.4.9.5.1.-.8.b.c.d.-.9.e.d.b.6.f.c.f.6.2.e.e.....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.=.I.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.=.0.0.0.0.1.9.7.c.-.0.0.0.1.-.0.0.1.c.-.6.9.2.b.-.f.3.9.6.2.5.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.!.I.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.!.I.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_0b7f51a9\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_0b7f51a9\Report.wer

File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6780496869404035
Encrypted:	false
SSDEEP:	96:/YFNUbYfMKgZqyFy9hk1Dg3fWpXIQcQic6fcEKcw3KW+a+z+HbHgOVG4rmMOyWZQ:QPUUfDiBFH8bQ5jSq/u7sYS274ItW
MD5:	253E67524E665CED7FCB680D0B15A679
SHA1:	24639CE4E89EBE95A718F39E052B66EE1DB8571E
SHA-256:	D735AF532B084C095252034F04EA6E719F558707D29D910C1AAC03E4434D78B6
SHA-512:	6C524B0409FF6FEC5A18672AE22713F10264605A27EF509BACAD28FB8858B02B1229CEBE148A46BFCFA83D8F5DD5DDFFFDDC49879E9CF9247F79FBC36B69EC29
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.=.1.3.2.8.2.8.8.6.4.4.5.2.5.3.6.5.5.7.....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.=.1.3.2.8.2.8.8.6.4.5.0.3.0.0.5.1.0.2.....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.=.8.c.6.5.1.a.a.b.-.c.b.9.c.-.4.e.a.e.-.b.0.8.d.-.7.3.b.d.1.b.2.a.e.7.9.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.d.f.2.b.9.a.3.-.8.2.8.8.-.4.1.6.5.-.8.9.7.b.-.b.3.4.2.2.7.6.c.2.b.c.4.....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.=.0.0.0.0.1.9.7.c.-.0.0.0.1.-.0.0.1.c.-.6.9.2.b.-.f.3.9.6.2.5.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\WER130B.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):	4.474808152945533
Encrypted:	false
SSDEEP:	48:cvIwSD8zsPJgtWI9OzkaiWSC8Blb8fm8M4J2yzZFlT+q84WvuKcQIcQwQkd:uITfxFIajSN8JJNguKkwQkd
MD5:	D74B9CA42FCB4FF47670DBB70126665D
SHA1:	C713CE9910F32D106BDA790CB5B81050AFB6EA4E
SHA-256:	351496A5886658C4E4EAC55F0BA237EEC44C116671BD7983947295C19FD3B259
SHA-512:	4794B84A709693530AD15FC706F662029230CF25AE8A83F08896FA1826DBF0B359E053F56265706028B07CC7FEC1C1B5B9851AEB59FA64188688A38AC6A8B1CE
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="1279431" />.. <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\WER3AA6.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 02:40:46 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1059516
Entropy (8bit):	1.352706935657892
Encrypted:	false
SSDEEP:	1536:Gt1e8iM+a4YlSOTeBvftH4l48olYfvW0eYkp4GmC4XzcYpM6IcgPO:S17iM+hYlSbvftYHoieIZllPO
MD5:	609F488A07CAB33EE4C369EC64AB8E68
SHA1:	13F1F816D89247048761B91950FB0A6342295791
SHA-256:	ECDBC0A49FDF15A6886ED1056B4CA76D37D08D4C8A41036A4B6E2FC932FA4F24
SHA-512:	11F2B75FFA6E5B0DE6AF9B8B4F20512D3ED40C59A5076452DC1BB2837817D62ECDB44622224F785A54532E18F9C679B74CA451CF65C6739392DC9BCE223B9C9
Malicious:	false
Preview:	MDMP..... .....2.a.....4.....H.....$.....`.....8.....T.....@...|.....U.....B.....p.... ...GenuineIntelW.....T.....|...z1.a4.....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\WER449A.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):	8302
Entropy (8bit):	3.6915284993016986
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER449A.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNi/al6q56YFNSUtugmfL8GSqCpDe89boZsfUUGYm:RrlsNi+686YvSUtugmfLrSNoyfNw
MD5:	1F87088A2C4B50685F9DF738D891EE0D
SHA1:	C3AFE2940FCAE79DBF0F28CC6BB96B51671A5A8F
SHA-256:	93619AAB36DF73654B94426D43A83B7A0111F98AED5F22995DB9CEDD9FC70661
SHA-512:	56B3EE353C0D6920650BE842CB90BBDF78AC03BE89E73E3D88FC58FE934B344D3377B9DCCE622C5E4B5A56EF5C43F750E7F6FC470A80DF7419D019C9D1F3AC 00
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.>.6.5.2.4.</./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4789.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):	4.433540504001836
Encrypted:	false
SSDEEP:	48:cvIwSD8zsPJgtWI9OzkaiWSC8B58fm8M4J2yGtFw+q84tjCKcQIcQwQkd:uITfxFIajSNoJEoxCKkwQkd
MD5:	917A30CB8F45138C5B6CE4832BD64950
SHA1:	462BCE590F4F8B964B444066E2A558AEA1A41822
SHA-256:	F37BFB12A9C8E0181148949B5B642904E89663392CC7658E5D6A02D1F36BDB41
SHA-512:	8B95835D70E20375A89A272CDB69D67DCE858835C5911EBE14EE8A8EF3757AA1E6E0308DD1167C307523373AF4F4F6EE9DCA4E44ECB69D9DA722B50AAE3627 B
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="1279431" />.. <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\WER4E7D.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51764
Entropy (8bit):	3.066226886579781
Encrypted:	false
SSDEEP:	1536:znHBfC2qopFhm5NMFBqCAEzfnEbLt1Zy/yaD2kwxNog:znHBfC2qopFhm5NMFBqCAEzfnEbLtzyG
MD5:	0C82D3D4C22C53918FA237399AE6871C
SHA1:	4898B947854FDB7D7AF136F1B54CB6BCFA097933
SHA-256:	23B4A7A2F4E5E85842A640A1CCC54ABA392E7A4E96DBDC871C413447DDA646EC
SHA-512:	5486DA1D4E56902CF9824653FD0D1294E7A8AD91935B79DFE1E0A558E3BCD2D5D3325DEEA1F17540CF364977A8117617758E4B3C44F6B350F9BD8F1A6065C2D
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\WER538F.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.695643602908232
Encrypted:	false
SSDEEP:	96:9GiZYW8QuNj0Y5YLWIFiHIUYEZUwtFiIOkprwj/72a9fKLGZhIDo3:9jZDnehxT2a9fWGZeDo3
MD5:	4F565AA7FF00770992EA2D46A65C181C
SHA1:	E71996407985D1EFC7802A26A616CD6BCAFAD017
SHA-256:	7D9388E1E756539E15D21F3233476519475F0546E654BA1DBEB23EB284091E4B
SHA-512:	65C13B833696C293743496B47B275318A99FC4C57879E211AB3D0DEE73BF7D7940C697976A7AAB7FF616007B474CF66E4A980776D2D2C0AB29D7F47582B6A3F8

C:\ProgramData\Microsoft\Windows\WER\Temp\WER538F.tmp.txt	
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\WER830C.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51386
Entropy (8bit):	3.0669804346601217
Encrypted:	false
SSDEEP:	1536:YpH7qfTmlXLIta6T/yshq/wIGzI9o3Sv79yqlzRl:YpH7qfTmlXLIta6T/yshq/wIGzI9o3SL
MD5:	7AEB64E6732D8507B55CDB97065F5551
SHA1:	E336635236D2CA4885F0AF446932A888356E86EF
SHA-256:	7B2551D74FF3C3335954AB31B2B3591B17DB35B97C998AFBA5E675E85C52643A
SHA-512:	572BE12F411E2B7809F380A7E8EADF43D942BBCEB7A875E99EE242F60FE4A26966382E046DB7385BA727CC0A750CC1268EE7A2A7F962498187EA733DEEE93D8 5
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\WER8792.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6960488456297536
Encrypted:	false
SSDEEP:	96:9GiZYWF5XUOYUY1WmiHGUYEZHGUtFikO8pWwPisaZefyl7Z+IGn3:9jZDLTlGuPaZefg7ZJGn3
MD5:	DE94B8774A8048437382D1A660F29AA9
SHA1:	1A8665F56338D79BE34B9232DD84C5B565065CAE
SHA-256:	6E07764DD487971E78C9FF24B371410E8498F8143EEB163B9D167A15DC006283
SHA-512:	B201C8D8F965F33DB6F6EC16201323A4AA192CDC5FA4D6745FBBF1590284E66EBA634BF9E5512EEFED2C55CEE593B7E94671FFF678626D8D23A0A13A39C537[9
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\WER87A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 02:40:33 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	26500
Entropy (8bit):	2.499854907523872
Encrypted:	false
SSDEEP:	192:QxA1R8L2Oyej8VlR/395FyQorZxJjb5XcRJX+xS+u2xh9c9u:78Vbj1LJj1Xcv+xS+u2xX
MD5:	590591470D673CCE95BF4573423BCF62
SHA1:	4AAB40C626AF3781AD5D0A67C0D8A571887859E5
SHA-256:	A51E1E0FD6D7C38020106070BE7FA729FD0E8DC15E191C4C27D83E1CD636EDDA
SHA-512:	2DFF7DAAB01486716915E7395DE249F5E8261E20EA957002D202606C2716AEE535FE4BAEC8BE44A1BD0DE82A1103A7642292C78D277F341240C4EB3481D3ECD
Malicious:	false
Preview:	MDMP..... .....!2.a.....4.....H.....$.....`.....8.....T.....h....[.....U.....B.....p.... ...GenuineIntelW.....T.....|...z1.a4.....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\WERF90.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):	8342
Entropy (8bit):	3.6998766295075085
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/w6yBA6YFrSUIogmfsSznCpBN89bjZsfnhm:RrlsNio6r6YpSUIogmfsSzXjyfc
MD5:	6FF22358E066039C4E5F9D652B81942B
SHA1:	0CC99443BF6C6A1C36A9DE208E077B759FAAA2CA
SHA-256:	97AA98F872A9592C2687DBAE180859D4D54891CACF80F4494D8FFAAD5FC2F4C6
SHA-512:	B94048F34EC84C49044F17F4C17EB4CFA0E79400B99E9E85EF18268B53C8188B962E1EB3F3CB91E8CF7CEF44F47D1E855448EF8D7460AAC6EA08135EAC18B20 8
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.>.6.5.2.4.<./.P.i. d.>.....

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
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):	4.272985782131946
Encrypted:	false
SSDEEP:	12288:a3OEDNLIT7EuGX8LKyVySY9jugewol3v1TmymCBrDca+XrpsQRiu0:GOEDNLIT7EuGX8Gv
MD5:	54185C71541C66EA07E6DDE84B4C437A
SHA1:	61BBAC5E98BDC0CB940804F0D6A8CB468B9ABD78
SHA-256:	07303B5CD2B6D05BC20136A5846EBE6CFD2E6850ED441124179D1C4ECD241419
SHA-512:	48085F353E3430961FF9CC8A9E57AFDA948B3631E6C6ECA8F5DDD6EC49DF8FBEFA579B7C6EDF19CC2EA3C3948241285524050B4DD07CD6E37666404943758E E
Malicious:	false
Preview:	regfZ...Z...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.]7.%..... ....k.3..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.3978501417394353
Encrypted:	false
SSDEEP:	192:IZXfi1dkpA0sfYK5FSEsWftx12xgoJ4XBaJNSdkyFn6yvRrsf9WfYjdsiDoXzCH:+ve5Rftx12PJ4XB7FFn7eZd1DoXzCH
MD5:	43A63F75192D7286A2D714CB22AA13E3
SHA1:	2E59B86D1E7967E0B713CAE9B65EBD9897CC506F

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
SHA-256:	2EE75911842651EE3E0492EA94DB6A7391AC8F7DA2DAC9AF8E5E8E89F2FF6EAF
SHA-512:	CBB8698D79385AE8609DB7FE6EFDF845E652075A34C95AFABE69E111B5400404817A8BED9BCC4CA6BF1D5FB2D707E99AAA75355D3D79589CFC6E5521D668A187
Malicious:	false
Preview:	regfY...Y...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.]7.%..... ....m.3.HvLE.>.....Y.....a1I?c.>.....3.....0.....hbin.....p.\..,.....nk,.K.9.%.....0..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .K.9.%..... ....Z.....Root.....lf.....Root....nk .K.9.%.....}..... .....*.....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:	mal.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
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: 6524 Parent PID: 956

General

Start time:	18:37:46
Start date:	01/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\mal.dll"
Imagebase:	0x10c0000
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: 00000000.00000000.650731221.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.649143533.00000000007B0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.676710015.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.649539674.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.675954463.00000000007B0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.678039015.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.677709015.00000000007B0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.650535103.00000000007B0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6552 Parent PID: 6524

General

Start time:	18:37:46
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\mal.dll",#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 1324 Parent PID: 6524

General

Start time:	18:37:47
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\mal.dll,Control_RunDLL
Imagebase:	0x2f0000
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: 00000003.00000002.620619819.00000000029C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000003.607531187.0000000002F59000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 1432 Parent PID: 6552

General

Start time:	18:37:47
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\mal.dll",#1
Imagebase:	0x2f0000
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: 00000004.00000002.646384056.000000000291A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.646347873.0000000002780000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 2132 Parent PID: 6524

General

Start time:	18:37:51
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\mal.dll,axamexdrqyrgb
Imagebase:	0x2f0000
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: 00000006.00000002.639924880.0000000002DAA000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.639880819.0000000002C10000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5300 Parent PID: 6524

General

Start time:	18:37:59
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\mal.dll,bhramccfbdd
Imagebase:	0x2f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.648863734.0000000002D60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.648896656.0000000002EEA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 4932 Parent PID: 572

General

Start time:	18:39:26
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5784 Parent PID: 1432

General

Start time:	18:40:08
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\mal.dll",Control_RunDLL
Imagebase:	0x2f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 6444 Parent PID: 1324

General

Start time:	18:40:11
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jxqjexglbxuwcsnd\ncmurmkelbjyq.yqk",ewrKlpBownvGxgM
Imagebase:	0x2f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 5304 Parent PID: 2132

General

Start time:	18:40:15
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\mal.dll",Control_RunDLL
Imagebase:	0x2f0000
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: 5644 Parent PID: 5300

General

Start time:	18:40:27
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\mal.dll",Control_RunDLL
Imagebase:	0x2f0000
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: 6964 Parent PID: 572

General

Start time:	18:40:27
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: WerFault.exe PID: 6224 Parent PID: 6964

General

Start time:	18:40:28
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6524 -ip 6524
Imagebase:	0xbc0000
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: 5316 Parent PID: 6524

General

Start time:	18:40:30
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6524 -s 308
Imagebase:	0xbc0000
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: 3732 Parent PID: 6964

General

Start time:	18:40:40
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 572 -p 6524 -ip 6524
Imagebase:	0xbc0000
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: 2804 Parent PID: 6524

General

Start time:	18:40:42
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6524 -s 344
Imagebase:	0xbc0000
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