ID: 532106
Sample Name: mal.dll
Cookbook: default.jbs
Time: 18:21:41
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report mal.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Emotet 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 6
Jbx Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 10
Simulations 10
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 17
Sections 18
Imports 18
Exports 18
Network Behavior 18
Code Manipulations 18
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: loaddll32.exe PID: 6880 Parent PID: 5432 18
General 18
File Activities 19
Analysis Process: cmd.exe PID: 6896 Parent PID: 6880 19
General 19
File Activities 19
Analysis Process: rundll32.exe PID: 6920 Parent PID: 6880 19
General 19
File Activities 20
File Deleted 20
Analysis Process: rundll32.exe PID: 6932 Parent PID: 6896 20
General 20

Analysis Process: rundll32.exe PID: 7016 Parent PID: 6880 20
General 20
Analysis Process: rundll32.exe PID: 7032 Parent PID: 6880 20
General 20
Analysis Process: rundll32.exe PID: 2600 Parent PID: 6932 21
General 21
File Activities 21
Analysis Process: rundll32.exe PID: 6464 Parent PID: 6920 21
General 21
Analysis Process: rundll32.exe PID: 4972 Parent PID: 7016 22
General 22
File Activities 22
Analysis Process: rundll32.exe PID: 5532 Parent PID: 7032 22
General 22
File Activities 22
Analysis Process: svchost.exe PID: 5672 Parent PID: 568 22
General 22
File Activities 22
Registry Activities 22
Analysis Process: WerFault.exe PID: 5648 Parent PID: 5672 23
General 23
Analysis Process: WerFault.exe PID: 5528 Parent PID: 6880 23
General 23
File Activities 23
File Created 23
File Deleted 23
File Written 23
Registry Activities 23
Key Created 23
Key Value Created 23
Analysis Process: WerFault.exe PID: 4588 Parent PID: 5672 23
General 23
Analysis Process: WerFault.exe PID: 1744 Parent PID: 6880 24
General 24
File Activities 24
File Created 24
File Deleted 24
File Written 24
Registry Activities 24
Key Created 24
Key Value Modified 24
Analysis Process: svchost.exe PID: 5400 Parent PID: 568 24
General 24
File Activities 24
Analysis Process: rundll32.exe PID: 5960 Parent PID: 6464 24
General 24
Analysis Process: svchost.exe PID: 7116 Parent PID: 568 25
General 25
File Activities 25
Disassembly 25
Code Analysis 25

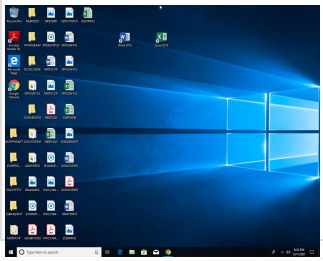
Windows Analysis Report mal.dll

Overview

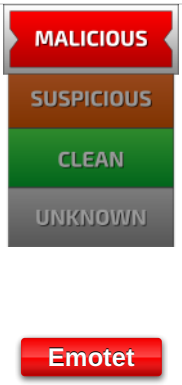
General Information

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

Most interesting Screenshot:



Detection

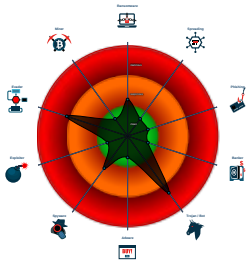


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Sigma detected: Emotet RunDLL32 …
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- One or more processes crash
- Contains functionality to check if a d…
- Deletes files inside the Windows fold…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6880 cmdline: loaddll32.exe "C:\Users\user\Desktop\mal.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6896 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\mal.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6932 cmdline: rundll32.exe "C:\Users\user\Desktop\mal.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 2600 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6920 cmdline: rundll32.exe C:\Users\user\Desktop\mal.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6464 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lxelxho\ggoife.qjv",clLaoeKXf MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5960 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Lxelxho\ggoife.qjv",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7016 cmdline: rundll32.exe C:\Users\user\Desktop\mal.dll,axamexdrqyrgb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4972 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7032 cmdline: rundll32.exe C:\Users\user\Desktop\mal.dll,bhramccfbdd MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5532 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\mal.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 5528 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6880 -s 304 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1744 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6880 -s 324 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5672 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5648 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6880 -ip 6880 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4588 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 564 -p 6880 -ip 6880 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5400 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7116 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **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": [
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2",
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.1037130438.0000000000CF0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.1168490551.0000000002D7A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.1063275616.0000000000E8C000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.1035699542.0000000000CF0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.1028366032.0000000000800000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.loaddll32.exe.cf0000.6.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.4af0000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.3070000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.2cc0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.cf0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 33 entries				

Sigma Overview

System Summary:

Sigma detected: Emotet RunDLL32 Process Creation

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:

Hooking and other Techniques for Hiding and Protection:

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

Stealing of Sensitive Information:

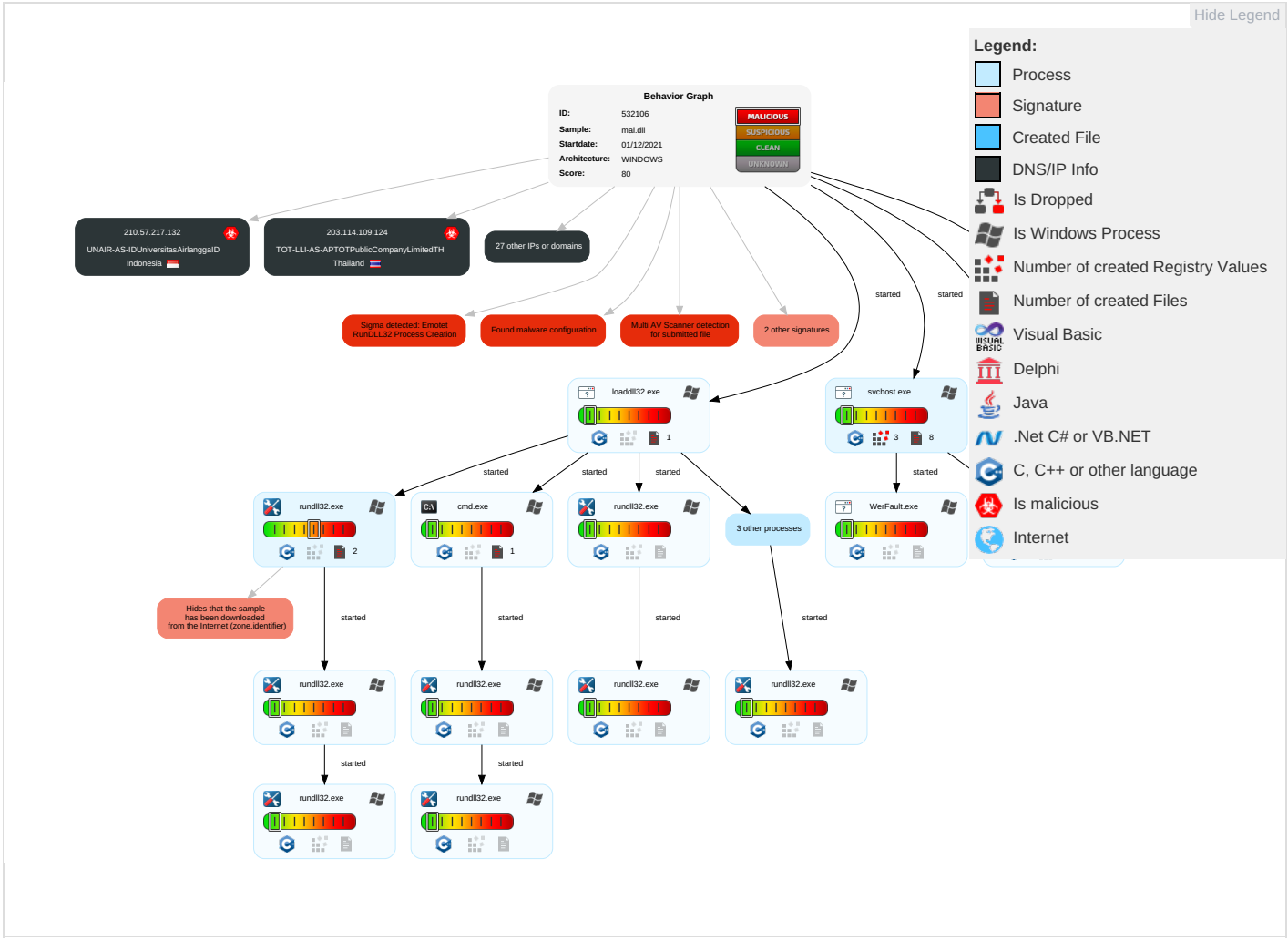
Yara detected Emotet

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	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 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 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	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	Security Software Discovery 4 1	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	Virtualization/Sandbox Evasion 1	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	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	File and Directory Discovery 2	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	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

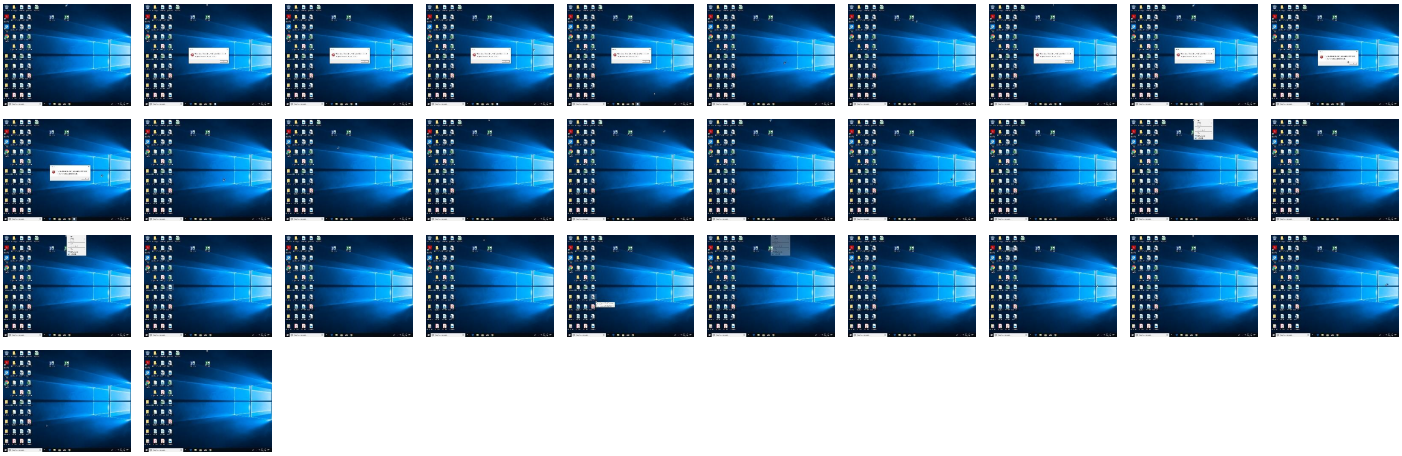
Behavior Graph



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.cf0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.3070000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.cf0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.cf0000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.2cc0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.800000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.a90000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.cf0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.4af0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.cf0000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

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-IDPTCitraJelajahInformatikalD	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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532106
Start date:	01.12.2021
Start time:	18:21:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 24s
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
Number of analysed new started processes analysed:	21
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@34/14@0/29
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 18.7% (good quality ratio 17.9%) • Quality average: 71.6% • Quality standard deviation: 24.8%
HCA Information:	• Successful, ratio: 80% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:25:59	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.154.133.20	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	
	ma9Kq24IDH.dll	Get hash	malicious	Browse	
212.237.17.99	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	
	ma9Kq24IDH.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ARUBA-ASNIT	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
	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
	b6GJG5t0kg	Get hash	malicious	Browse	• 31.14.139.51
OnlineSASFR	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
	jSxIzXfwc7.dll	Get hash	malicious	Browse	• 195.154.146.35

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_88e9c9cb640b4f665f2020b110738337d7578_d70d8aa6_142e078f\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):	0.6740916034847534
Encrypted:	false
SSDEEP:	96:BiarZqyfy9hkoyt7Jf0pXIQcQ5c6A2cE2cw33+a+z+HbHgOVG4rmMOyWZAXGng5p:1BAHnM28jjSq/u7sKS274ItW
MD5:	8B6CC0A8CD57C51E59BCC26286FE9080
SHA1:	C24D429F56E4F385E3069AC93DF2D778E2CE7DDF
SHA-256:	577C96830F420FD747CA70FDB590467989DDF046C194AF2E3C601061DF8DA0C5
SHA-512:	C84F43C71F18D660DA7903E3DF40A8A421A22156D658BF480B4D3CA54D1CEA6FED216E8737018F98236B5D760C805DDF1118555607EC9073CC28DBFAD6EAD84

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_88e9c9cb640b4f665f2020b110738337d7578_d70d8aa6_142e078f\Report.wer	
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.=.1.3.2.8.2.8.5.3.1.3.8.0.2.7.7.6.0.8.....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.=.0.8.e.3.9.8.9.7.-.4.3.8.0.-.4.b.3.9.-.9.7.b.c.-.f.a.8.0.f.7.6.7.e.d.e.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.0.6.9.5.f.7.c.-.e.b.d.0.-.4.d.a.6.-.b.3.5.7.-.6.4.6.2.3.8.d.5.8.e.f.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.a.e.0.-.0.0.0.1.-.0.0.1.b.-.a.3.4.7.-.7.a.0.9.d.8.e.6.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_0766c198\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):	0.6775010169886009
Encrypted:	false
SSDEEP:	96:5jF3RarZqycy9hk1Dg3fWpXIQcQic6fcEKcw3KW+a+z+HbHgOVG4rmMOyWZAXGn5:d1MB0H8bQ5jSq/u7slS274ItW
MD5:	7AFCD1BD51040404605337C60BD472E9
SHA1:	03CA0F35512AF716A95BFB16660A2C6B4AB89D6C
SHA-256:	990AF6D85CF4CBCB31B1D8D5627CFBED274DF42808493348062AC58DFBF4C9EE
SHA-512:	CAD0A0A3F537F7D1D9D1162C95081D7161344B43355DD3A7B2B312899C860D04A1D2660F1B4F9D820D2FDFCCC3E63A5E85A2A4C9BABCD795C19C636432B3077
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.=.1.3.2.8.2.8.5.3.1.4.6.5.0.9.4.1.8.4.....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.=.1.3.2.8.2.8.5.3.1.5.7.7.5.9.3.6.8.8.....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.=.4.c.5.2.d.4.b.a.-.8.4.2.5.-.4.3.4.d.-.b.9.5.9.-.0.e.7.8.5.8.2.f.7.8.8.4.....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.=.2.7.4.f.0.7.6.c.-.6.a.a.7.-.4.a.8.5.-.b.4.5.d.-.4.0.8.a.0.b.3.b.1.8.8.9.....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.a.e.0.-.0.0.0.1.-.0.0.1.b.-.a.3.4.7.-.7.a.0.9.d.8.e.6.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.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1952.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed Dec 1 17:25:47 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1058996
Entropy (8bit):	1.3712773239769518
Encrypted:	false
SSDEEP:	1536:bxYD5OU5ERxUg6yTR+RDOYIawA30cvhDhjUlzxAINxmsRKNBnMGCaOsU:rRx7/R+MdawA30cvhDiNxm3vnfCaZU
MD5:	7A4E56B2558285ADD418A7A78AE6013F
SHA1:	BEA34760885B4B6F6E72E5DF7203C47F4B79425C
SHA-256:	58034C4613B0834F9A3C455D338201F3878DF04327E67AC512A325461A431A92
SHA-512:	4DFEEE02F3DC33302089C8BB232C598C51AAB90B800B11054EE168FCE673EEEA01D1415D39CBD32BFB8B76DB4CFA99DFD4E8FFF4EB7EE5D75A9401DE0A33BD73
Malicious:	false
Preview:	MDMP..... .....a.....4.....H.....$.....`.....8.....T.....@...t.....U.....B.....p.... ...GenuineIntelW.....T.....]..a;.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2151.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):	3.6954095323269565
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi8X6OI6Yr3SUXy6gmfL8GSq+pD0/x89bULsfDcm:RrlsNiM656YLSUXy6gmfLrSxUQf9
MD5:	E3A11A63623CFEBFB66EB6BE4286B4AD
SHA1:	F7F64CC325FD71646673B03D6ED7D060CF455B6B
SHA-256:	32C311DBE17A4F7FD7E964151DA66BBBD707A42310650C91C3A653E147FFAFCF
SHA-512:	01A461E419779C1384874EDF910B36050564CB793712A86C597F255F57AA27D80D26C3FFEC957F6CEAF357A21277E2B7C7775F03ECB0298994926820FDDB35D5
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2151.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2338.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	49514
Entropy (8bit):	3.046922393170869
Encrypted:	false
SSDEEP:	1536:FUHA8ZHr/z7dqVKCK0awYNP2molncPX4BssI:FUHA8ZHr/z7dqVKCK0awYNP2molncP4q
MD5:	760C0C341E6D4AB6E90B4CF99ECB6B72
SHA1:	5F4BD5FA694532B332EEDA311AD7E4C28DE57C4A
SHA-256:	0A3139412B1E043F7423A4F2D75C5745EABBA5E9D74F8F7AD738E41E9EDD4694
SHA-512:	DB1C3A2FA38AA6B825D7AEBBFB2544BBBE285EA32D695AC5D3871D77BD7D8885987F146A4A919F32EB8D31535B5E67DBC2C83D0B0ABDB765923620530126A8B3
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\WER2440.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):	4.430482411772029
Encrypted:	false
SSDEEP:	48:cvIwSD8zsTJgtWl9Zj1WSC8B98fm8M4J2yGtFe+q84tjDKcQIcQwQhdd:uITftyESNEJEWxDKkwQhdd
MD5:	C44D5FCFA4C7968F2231DFF934C914C4
SHA1:	93FD6221DEC7251F05DF251E592E69996D3718E1
SHA-256:	B34488C435110C11B59626E8EC4017CFBD4B51FDE8CFA83024F6812AD76E4EF4
SHA-512:	C11EC26808E1AA6E10DEA8CAB9963700C09EE51D25974E1268993CAC34A9F9FFAFCBA0E31FF48351B476030ED6FBDA067BC4F3629A913636858FFE3362B7338
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="1278876" />.. <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\WER277F.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.694366916894771
Encrypted:	false
SSDEEP:	96:9GiZYWeU1eH4Y8EYHW4IH1YEZsvtk0iKEqI+NwqdNMpaGMSjizIdO3:9jZDe4SmrvAaGMSji8dO3
MD5:	D34028D15FCFB3E93CDDCDDEF534FE9C
SHA1:	ACFB14695F6CD566CE203DB0D8B551E50AB27D70
SHA-256:	68410881C59F5C019913F972562D5D03D0C0FCDC4AE9E8122AAB68368FBE3500
SHA-512:	CA156539250FC8DB276B2F3FF64FE97F59DD2DF03A7307C06B581884714BA480A6A6FF70E6FB6FF0DFD999BF3CA785FC06469C192DA2A8B8A861216DD32F716
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\WER2E.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):	4.477100128494388
Encrypted:	false
SSDEEP:	48:cvIwSD8zsTJgtWI9Zj1WSC8BT8fm8M4J2yvZFL7+q84Wz/KcQIcQwQhdd:uITftyESN2JBTw/KkwQhdd
MD5:	BCA921FB2139CC9CBF9FA843E8E04CCE
SHA1:	09B6E777D80619083576F0073B5C141044DA816F
SHA-256:	5643B318FAAC21EEF41F479F2907F8CBBB2BA2B6394E1ABA182BF109CB73967D
SHA-512:	633BCB6560AFE7BA2194E29D8E8529E51BA6D3B60FC4E978A5708421BC15395EC359D69978201E2CBDBB6CD9E9C4D8EF9C5E13070BD61ADDBD7544AD22C87 07
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="1278876" />.. <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\WER475C.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	49504
Entropy (8bit):	3.046214480484183
Encrypted:	false
SSDEEP:	1536:fNHk8hA9rD9d3dqxACKLw2C9mo1nZahK8qs:fNHk8hA9rD9d3dqxACKLw2C9mo1nZaKu
MD5:	3A6B79A861C2498DC74B41C4C47AD1C2
SHA1:	C917A29F1AFCF3CD4484558A50540AEE9492712B
SHA-256:	E9EFA2B3CD17C1A8D96C4BAF257E272AB8612D6139CA638C6158DC93745F968F
SHA-512:	1638262533B220652B62B7ACEDE2360B5DB4C25A2B696F86E47D4C6625B33FEDF418EC0DAFD6BC79B95C292AC04ED303A40507A32B3292740D9756865B679E5
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\WER4AA9.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.693853769718937
Encrypted:	false
SSDEEP:	96:9GiZYW7u9M4zb1Y1YKWA6yUHXYEZZatFiKyq7+Sw7aNXa0a4wZR6Izj3:9jZDy9ZizhQlma0a4kRtzj3
MD5:	815160F2FA14825C852FE6F40CB8334B
SHA1:	EA39BEB4C2958129BB3BA9797D4FE7814A600D5F
SHA-256:	77B2156C6621EE98C47304B22ED3B1985698E82C8C937061691D17731EF87297
SHA-512:	742A7C4E4237FFA10EC46D8529F262F387218B87EDA662584CCF901E722DA3A916A036400423E012F1028377550FD9BA38AE29409804AAED8C0CBD3C71EE8F4C
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\WERF82D.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed Dec 1 17:25:38 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	25940
Entropy (8bit):	2.552323813346806
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF82D.tmp.dmp	
SSDEEP:	192:WrlaMO5hgMhy/5kgJmgi0ilF6ZWUcHEjzU:15uh/5kgJmgvilF6ZWVj
MD5:	4DEE3193ADBBB8E856D847FA57D241A7
SHA1:	262B42363EBEC83706CDA0CB5FA0ED306B0139DD
SHA-256:	E13B0D3DBD6B6544ABA508382E0BF48A723E5D4601C590E71CE9552B12B1F936
SHA-512:	FE3D3E7EA25B407A6DAC1AE28C4EEE34887E645DE9D9780C19153A4DFF719320DD8047121C940C60BE9E1D45AD78BC29F0A08720F3D1929E0B36DD9B309333E
Malicious:	false
Preview:	MDMP..... .....a.....4.....H.....$.....`.....8.....T.....h....X.....U.....B.....p.... ...GenuineIntelW.....T.....]..a;.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC74.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):	3.7034129553024777
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi8Y6WBXs6YrwSUByogmfOSzn+pB889bKLsf6Om:RrlsNiz6z6Y8SUByogmfOSzoKQfK
MD5:	D16931DDE458EACE169C4C614F5F04F3
SHA1:	2E01D79C131812A24342C537874F4E14BA1262FD
SHA-256:	9D1B2688A25E89A630F0E9D013611E6D86190697852CB3D07C9350A68B91245A
SHA-512:	25590A733DB4AC407C59A00A5AC2B1AFA2EF0AD8E874F8ABEA39C46B4431FE67C6C678EBBFDE0FD1F2BF59AEC2DCD5862A9F8BBAA3B5570E21029EE44FAD7E83
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.>.6.8.8.0.</.P.i.d.>.....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.23561428467192
Encrypted:	false
SSDEEP:	12288:j3rLo+MuY6hOQgWN8F9ZK5eeXAQEnHNi064cmgrUV9J99BzM:7rLo+MuY6hxgWNywX
MD5:	ACC34EDE4E06ED83933625F4CC7356DF
SHA1:	966066CEFF7348D96671527DE7402DA839AC3F1F
SHA-256:	399C9EF22BBEA528A7B8C6AAC0192A0A233490D8E2AF34935EA7240BFD400135
SHA-512:	E63F078C8C9DAC0BE90B4B0ED05E50D9A35B7640CEB51A42A122C7172C3C2FC875E2603CCF15D63AC8DCF2FA83380D190BBC1F2D1A18B7CFADDF142892CD5A0
Malicious:	false
Preview:	regfl...l...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.H.t..... ....]*).....

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):	3.7163846064597656
Encrypted:	false
SSDEEP:	384:CM45K5hocv4KgnVVeeDzewo1NKZtjooT8GRFwonU:leKVg/eeDzejNYtjOGRFwo
MD5:	98B36B1143289161730CE1E931F90DD9
SHA1:	B00EB50471991DE35EE39B0CC23902448BD555D4
SHA-256:	31B386D7BFDF10A381CC92B9A24C011E34BC8224CD60A582B7D0A981C8A796DD
SHA-512:	93C2E48BD5C9C1A5C81F71380FFA0A23B05E7E9D643E0F8BF7D652B11A06569C4791765B57F8090D095F5F3A7705C708E008C4E5015A2675D80ECE4468A00ED3
Malicious:	false

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Preview:	regfH...H...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.H.t..... ....(}*)HvLE.>.....H.....].gC..B...v.....hbin.....p.\.,.....nk,...0t..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...0t..... ....Z.....Root.....lf.....Root....nk ...0t..... .....*.....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..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: 6880 Parent PID: 5432

General

Start time:	18:22:37
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:	0x13c0000
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: 00000000.00000000.1037130438.0000000000CF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.1063275616.0000000000E8C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.1035699542.0000000000CF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.1063104639.0000000000CF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.1035947080.0000000000E8C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.1100911301.0000000000E8C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.1064906650.0000000000CF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.1037359091.0000000000E8C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.1100727595.0000000000CF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.1065208047.0000000000E8C000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6896 Parent PID: 6880

General

Start time:	18:22:38
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:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6920 Parent PID: 6880

General

Start time:	18:22:38
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:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.1028366032.0000000000800000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000003.971608734.0000000002CD9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6932 Parent PID: 6896

General

Start time:	18:22:38
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:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.1031543020.0000000002E63000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.1023539885.0000000002CC0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7016 Parent PID: 6880

General

Start time:	18:22:42
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:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1033480524.000000000310A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1033332210.0000000003070000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7032 Parent PID: 6880

General

Start time:	18:22:52
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:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.1035861580.0000000004AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.1035732972.0000000003193000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 2600 Parent PID: 6932

General

Start time:	18:25:02
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:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6464 Parent PID: 6920

General

Start time:	18:25:05
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lxelxho\ggoife.qjv",clLaoe KXf
Imagebase:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1168490551.0000000002D7A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1167572272.0000000000A90000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4972 Parent PID: 7016

General

Start time:	18:25:24
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:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5532 Parent PID: 7032

General

Start time:	18:25:29
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:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

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

General

Start time:	18:25:29
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 5648 Parent PID: 5672

General

Start time:	18:25:30
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 6880 -ip 6880
Imagebase:	0xea0000
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: 5528 Parent PID: 6880

General

Start time:	18:25:35
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6880 -s 304
Imagebase:	0xea0000
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: 4588 Parent PID: 5672

General

Start time:	18:25:42
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 564 -p 6880 -ip 6880
Imagebase:	0xea0000
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: 1744 Parent PID: 6880

General

Start time:	18:25:45
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6880 -s 324
Imagebase:	0xea0000
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

Analysis Process: svchost.exe PID: 5400 Parent PID: 568

General

Start time:	18:26:06
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5960 Parent PID: 6464

General

Start time:	18:26:28
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Lxelxho\ggoife.qjv",Control_RunDLL
Imagebase:	0xb00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7116 Parent PID: 568

General

Start time:	18:26:37
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Disassembly

Code Analysis