ID: 532221
Sample Name: 6zAcNlJXo7.dll
Cookbook: default.jbs
Time: 20:58:28
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

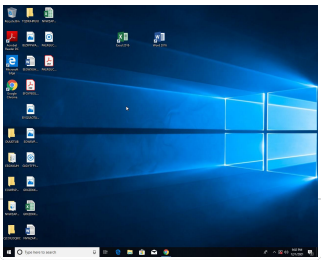
Windows Analysis Report 6zAcNlJXo7.dll

Overview

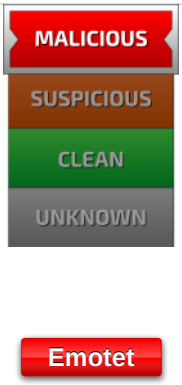
General Information

Sample Name:	6zAcNlJXo7.dll
Analysis ID:	532221
MD5:	c7e23f2764d6ed9.
SHA1:	67f31b13485f91b..
SHA256:	d048f196a39fc7d..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

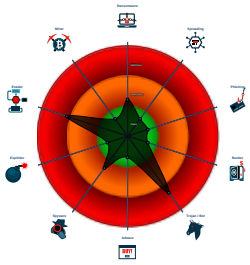


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- 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 …
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4668 cmdline: loaddll32.exe "C:\Users\user\Desktop\6zAcNlJXo7.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6172 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\6zAcNlJXo7.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6176 cmdline: rundll32.exe "C:\Users\user\Desktop\6zAcNlJXo7.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6324 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\6zAcNlJXo7.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6404 cmdline: rundll32.exe C:\Users\user\Desktop\6zAcNlJXo7.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6312 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Zsdkqzebleakbz\gnpornwqabjsi.vaq",YawfQDI MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6996 cmdline: rundll32.exe C:\Users\user\Desktop\6zAcNlJXo7.dll,axamexdrqyrgb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6300 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\6zAcNlJXo7.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4248 cmdline: rundll32.exe C:\Users\user\Desktop\6zAcNlJXo7.dll,bhramccfbdd MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5344 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\6zAcNlJXo7.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 5544 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4668 -s 272 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3860 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4668 -s 324 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4884 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5644 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 2824 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 4668 -ip 4668 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3160 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 572 -p 4668 -ip 4668 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4820 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": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.598946349.000000000072A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.596768757.0000000000A60000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.615675303.0000000000B8C000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000003.557368858.0000000002D65000.00000004.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.595689976.000000000060A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.loaddll32.exe.a60000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.a60000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.b93b30.7.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.622160.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.2ce22d0.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection:

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

Stealing of Sensitive Information:

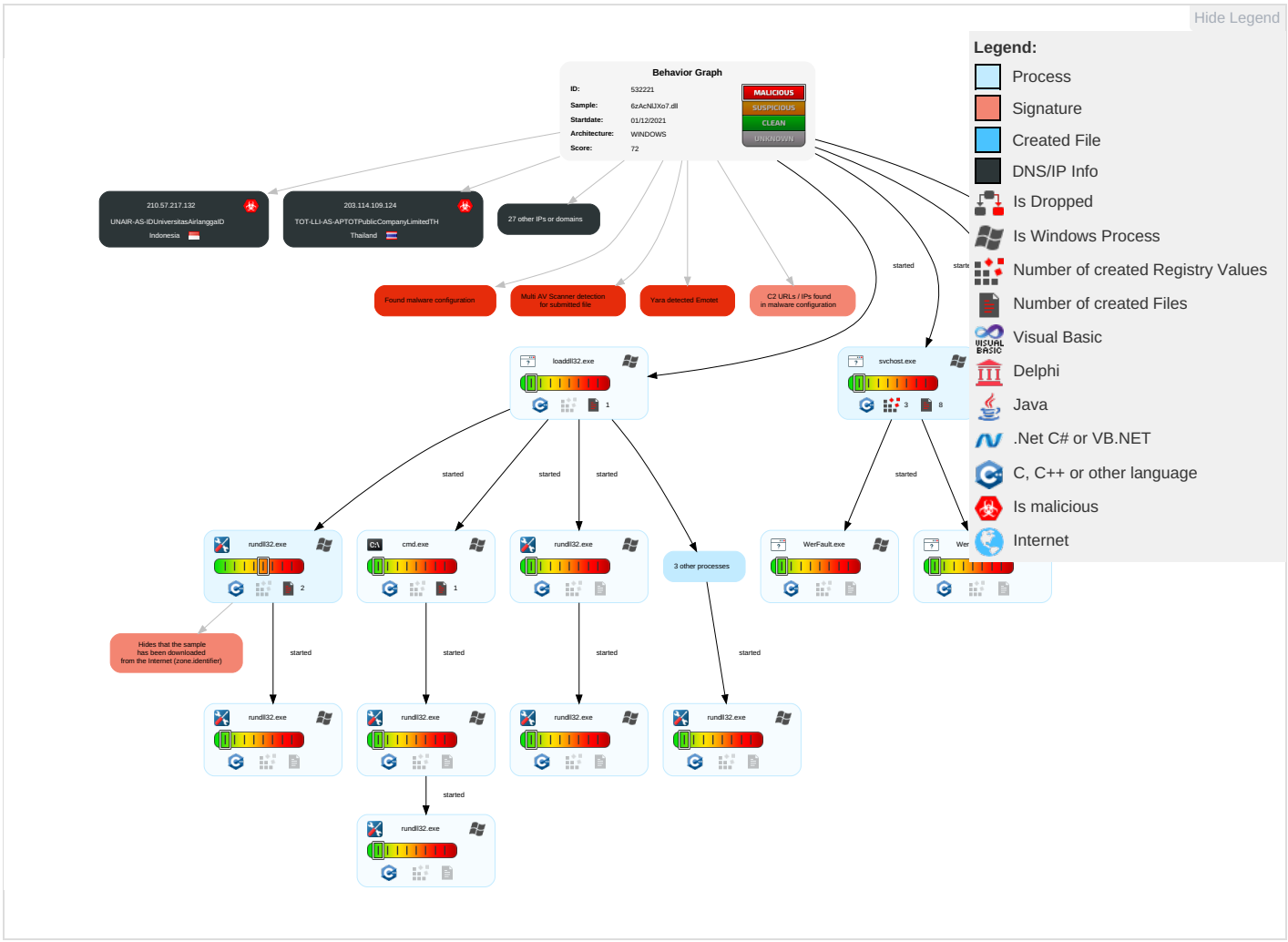
Yara detected Emotet

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
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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
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

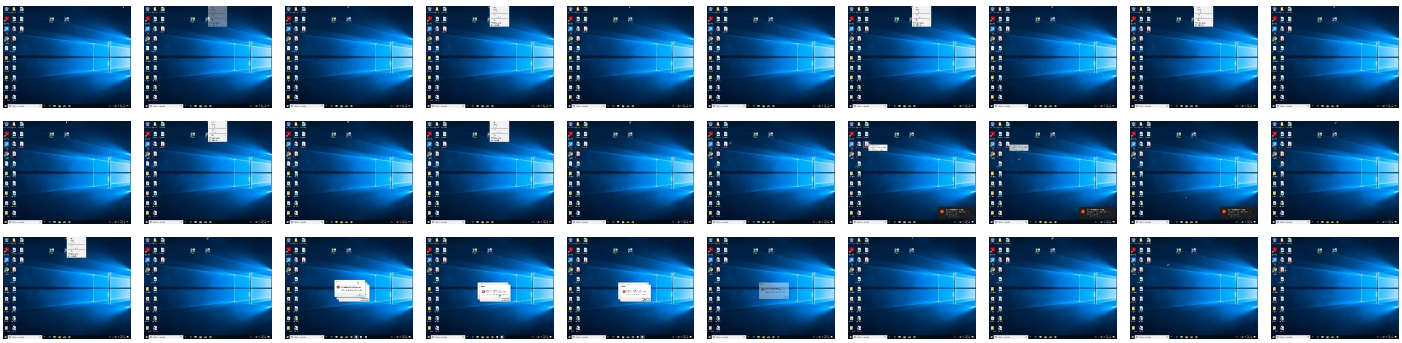
Behavior Graph



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
6zAcNlJXo7.dll	23%	Virustotal		Browse
6zAcNlJXo7.dll	24%	ReversingLabs	Win32.Trojan.Injuke	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.970000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.a60000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.510000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.a60000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.a60000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.3c0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.8e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.a60000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.a60000.6.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-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
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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532221
Start date:	01.12.2021
Start time:	20:58:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6zAcNlJXo7.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:	23
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:	mal72.troj.evad.winDLL@32/18@0/30
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.9% (good quality ratio 17.3%) • Quality average: 73.3% • Quality standard deviation: 24.2%
HCA Information:	• Successful, ratio: 79% • 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
21:01:14	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	
	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	
212.237.17.99	6zAcNlJXo7.dll	Get hash	malicious	Browse	
	mal.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ARUBA-ASNIT	6zAcNlJXo7.dll	Get hash	malicious	Browse	• 212.237.56.116
	DHL DOCUMENT FOR #504.exe	Get hash	malicious	Browse	• 62.149.128.40
	RqgAGRvHNwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	RqgAGRvHNwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	dFUOuTxFQrXAwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	RbrKCqqjDPUwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	dFUOuTxFQrXAwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88
	RbrKCqqjDPUwhoreniggagay.dll	Get hash	malicious	Browse	• 94.177.217.88

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mal.dll	Get hash	malicious	Browse	• 212.237.56.116
	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
	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
OnlineSASFR	6zAcNlJXo7.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
	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

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):	0.2485944511597269
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4G:BJiRdwfu2SRU4G
MD5:	5AA9010F86AAA454CA8AEE0BC5432844
SHA1:	6386A8DADB09CD4AAB9D91049CD1D1963B92A931
SHA-256:	47DA8C9FC8223551A0BD062C9DECFC1D0D6F9AFD5FDD71D3708F4A019B47ED4A
SHA-512:	E23E7173DD345E611CBA31DFB30C896E2D4CB00B50E099CAE0C69415BA53A607FF19BF102672CB5524E0A04E3D3AA80047A71D2E58DFBF69281E7ECF7A801
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....d#.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xce62c60e, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25065042679573807
Encrypted:	false
SSDEEP:	384:M+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:TSB2nSB2RSjlK/+mLesOj1J2
MD5:	6AB5EC32ABEAAD3B2D169DAD0DB571C1
SHA1:	678C6CFA14486816AEE71C4414F21ADAD5FD6188
SHA-256:	7246BA67A66D83694DECB8DA5F406339E7D4DD0BC106A0434FA3A18DE8DB9267
SHA-512:	3DF86A60CA8C704905450B1BE34110BE196CBC3452ED240A4FAACC87944A4EE03839DEEF9A810991AE7AEB75763EC110F15C0CE02EB3B02F6F0535BF4BD9B7C6
Malicious:	false
Preview:	.b..... .....e.f.3...w.....&.....w.....ya.h.(.....3...w.....B.....@..... ....3...w..... .....Oo.....y'q.....s.).....ya..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07670392576224366
Encrypted:	false
SSDEEP:	3:eEXll9EvrppcwAl/bJdAti5fgnp0ll3VkttlmlnI:eE1lYVpvAt46fgK3
MD5:	D931A9ECA494794C06C28E09F3FEED68
SHA1:	A58E08E3E371B8B5FA3BBC3F794D8AFA3FE80466
SHA-256:	84BE51EED8346F223265ADF7BD72801632C85C5B6E7459BC7446E62095ADF39D
SHA-512:	5B731CAB9B7E1E7F87A3E21012ED4296C8A33ABAA165F8C2F9E27C9CF2AD05BC15133BC949487B15D6793ACB1B8D35023C57251845FF37258CAFAC2D5E555DC
Malicious:	false
Preview:	U.....3...w.....ya.....w.....w.....w....:O.....w.....s.).....ya..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_8c5962cbbdb13a8671f1f3c3793157e73bd5d897_d70d8aa6_1403bece\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):	0.6757075644118485
Encrypted:	false
SSDEEP:	96:EHCVwZqyQy9hkoyt7JfapXIQcQ5c6A2cE2cw33+a+z+HbHgbEVG4rmMOyWZAXGno:cbBZHnM28jjKfq/u7s6S274ItW
MD5:	E551AE87CD4BFFDB52D2729EB71CA116
SHA1:	25E9433B73898DDF598B3C6AA832943A20204A38
SHA-256:	2139D02A6621817D10D5087037509E8EAD4748A15BF6DED6D219712F321A15CA
SHA-512:	BCE9AA5E5E1977BF76074B9B85BFB6C48B76DD79DF3C8E509C21F2C32C6FA16EE62DAAF932C6FC1C6A783D797A74D1E3AAE7A8C49139137675F584B5911222D
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.=.1.3.2.8.2.8.9.4.9.1.2.6.9.9.5.2.7.4.....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.=.b.e.4.a.f.b.3.8.-.8.6.6.5.-.4.a.5.7.-.8.3.2.0.-.7.7.8.0.c.d.0.c.0.4.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.=.1.9.b.7.c.4.a.e.-.c.4.b.7.-.4.3.8.8.-.b.4.3.c.-.c.e.6.3.3.e.8.f.3.4.2.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.3.c.-.0.0.0.1.-.0.0.1.c.-.a.0.c.6.-.2.9.6.3.3.9.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.8.:.1.1.:.5.3.:.0.5.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_0ebff56f\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):	0.6788179917265483

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_0ebff56f\Report.wer	
Encrypted:	false
SSDEEP:	96:cgFdfwZqyhy9hk1Dg3fWpXIQcQmc6W6hcEPcw3f+a+z+HbHgbEVG4rmMOyWZAXGo:JqBBH45FLjKfq/u7s6S274ItW
MD5:	9315D9FBF557FA80186C275A58BD321A
SHA1:	757D0034D1502A4A2BE1598CFAE67783FBA4ED66
SHA-256:	277F69162DD92575BF47BF9D18909659F3AE992F9FE8C2500CD7635FA0BECF8D
SHA-512:	D55717982C3B94AD577F05ACC3AB2E81DB9ECAE056EBBA2C05B57589AC3BA2965F940ED973E9EDF53057203ECDDA762CA64D8767DAF95CC800042563CC293DF
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.=.1.3.2.8.2.8.9.4.9.2.0.8.8.5.1.4.7.4.....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.=.1.3.2.8.2.8.9.4.9.2.8.2.9.1.3.6.7.4.....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.=.f.7.b.9.3.e.b.4.-.b.4.3.d.-.4.4.9.c.-.a.a.2.1.-.a.a.d.7.8.7.5.d.b.d.e.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.0.a.9.4.c.d.a.-.2.3.f.d.-.4.e.c.a.-.b.a.8.b.-.c.0.d.1.e.6.3.6.a.c.5.1.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.3.c.-.0.0.0.1.-.0.0.1.c.-.a.0.c.6.-.2.9.6.3.3.9.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\WER2C87.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54786
Entropy (8bit):	3.076333984011047
Encrypted:	false
SSDEEP:	1536:+HHb2TSLk7+W7AMbl6jEk8b+E10Wm1v5I:+HHb2TSLk7+W7AMbl6jEk8b+U0Wm1v5I
MD5:	C02DA58C9163875DDE4A126EB462E9A1
SHA1:	0A2F8FDCF105F9B01A97FE544632CADBEB57CB01
SHA-256:	E7F165C48F9A84354B60EE280D62E72E364E282ACCE1F73D91CE24E2D2A557DD
SHA-512:	1B2DAD82728DB75D3874CEB380F2E4A12F274C3771A4EAFC08F2B3CFFDACEDD213B31247516C2471555D40E69463CF8B4F9225E45B2D2D78C8580A0D3D44F7
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\WER3041.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.694710494201981
Encrypted:	false
SSDEEP:	96:9GiZYWSuxx/OYwYmWWuHYfUYEZLetFi4OD6nhwiWbOzaUmv1TFoKIxZ3:9jZDC3h3+otzaUmv1TFo9xZ3
MD5:	30F32608D2A56E14CAC4A2EEB0A4F51D
SHA1:	2C38E92DCC306540B28DC098EA8A26B89B58FD12
SHA-256:	EBEB6A9A01BB1141B1C90052011DBDA150B6F053AF34EEA02417F94EC5ADCAA6
SHA-512:	01171CD40D37AD87E8A53E3A9339262C6CB51616377B95A621D843437DAC022790261B59B6B5AA1AD5A71099416CAC0A70EE0519059418D47D456F559D034D1F
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\WER507C.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	53092
Entropy (8bit):	3.0784294516944835
Encrypted:	false
SSDEEP:	1536:ZvHF0cAHIGL5l+G7AMUVEgmpMc+c20W55rO8q:ZvHF0cAHIGL5l+G7AMUVEgmpMc+v0W5y
MD5:	B3690B79E2319DD5C7A0A447090B9B47
SHA1:	09C24AB18C0AB36AE28D3BA286F3C0CBDE03BF18
SHA-256:	FCA6A165CDA7189936ECE2410340E6BD9EDD19122DF254C33A70CF9F2D548CD0

C:\ProgramData\Microsoft\Windows\WER\Temp\WER507C.tmp.csv	
SHA-512:	DD24C70BB04178A4B65E586A9374CF7188D5D3E876A4CEBCCE92A31C4A613D37C6478FBAC69E20D6053609B79AD4F679CE3DF15614ACA5F238F45431C6009DF
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\WER5EC5.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.694643598554126
Encrypted:	false
SSDEEP:	96:9GiZYWghOD3LYFYF5W2u2HeUYEZ3y2btFi0O5z9wgcCrEaKmYPAro0IqZ3:9jZDD7SgXLLcsaKmYPArojqZ3
MD5:	79B97CAE7376674F218C321A353AA8CB
SHA1:	2F137749749239960FB3DD68BFE1D6DA62ABC6DA
SHA-256:	7720CF386642AB215CBE095291534BED4EF24B40D1E414D078CC8A5C4EB5D062
SHA-512:	AC171DE93F9F991C22F869D5AEB63C2D3737B65BBE0055A9A07B423415E7E5EFC0E9E2AA0E2302BA7B6D7FFCD9CD7424856A9928537248C47E73C935F0A8358
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\WERB1ED.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 05:01:53 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	26388
Entropy (8bit):	2.5129117145884763
Encrypted:	false
SSDEEP:	192:POFyf+dOlrx+qZhZyqjaBDdHnHvRBwak6J0dOe+UZr:2sflrxlnZtKTwak6lOi
MD5:	E414D434C126C5E3A34B58BF2C2691E2
SHA1:	E3E1241B44D69FF7425AD84838DF348E2BCDB613
SHA-256:	9D2635AB0D5B57C214B5983F7A7E0D5D24EE84C6FFA50FEC14F8F9BE448339E8
SHA-512:	C6580681F6BEAA7035D894DC4763FD3BFAFB16D4C3E4C02FDB0BAB43A4C641E431F468B68E802EDBDE3593537EA983C1516C8D561146E9198D6CC78B822E8A0
Malicious:	false
Preview:	MDMP..... .....AS.a.....4.....H.....$.....`.....8.....T.....h....Z.....U.....B.....p.... ...GenuineIntelW.....T.....<....R.a/.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB5D6.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):	3.702216729606524
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimF6gBXF6YFZSUJ5GgmfsSzKCpBH89bQ3sfpQm:RrlsNik686YbSUXGgmfsSzIQ8f7
MD5:	7439244D3ACB486F21A0681908A0773A
SHA1:	081E8D4257C5DB8CEF0A9EE9B011D2EE05D3E7C7
SHA-256:	FEA0D259E46748096FFA28A6B6B09EDF7B54A26F651D1E10B49BED15B7A376D6
SHA-512:	E297109798879B6AF9A731AF62FA35298576154FBA34F06F6572DB31EF84F44625E132E78D9012CEF1449E0813B7C1A29909494F0C9035375434CA25E8BE7E69
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB5D6.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.>.4.6.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB858.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):	4.476568550462276
Encrypted:	false
SSDEEP:	48:cvIwSD8zstJgtWI9Z1WSC8Bsr8fm8M4J2yzZFO+q84Wvq6KcQIcQwQXd:uITfHmESNbJJKgrKkwQXd
MD5:	A78FEB1C65A67FC0A5A5CECF5CFFDC92
SHA1:	0244D7CCB68AEA72550587A4A08CBCA6FA3C9530
SHA-256:	884FCFEEB48463B3A3B83B85E683B4527E7ADAFA4ECCF36A63BB85AD3F27ACB9
SHA-512:	AE660DE25F2E61EE330EF9128566DBD74257EE4DBD86B87043DBABF1B9C7E543FDE5D09F3842F62F7242A6C6087CC240C74811B86F8F76760A59F510A437A84
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="1279572" />.. <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\WERD1D9.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 05:02:01 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1059424
Entropy (8bit):	1.3568715112423828
Encrypted:	false
SSDEEP:	3072:YS3icXpg4oWGI3vHoh5PHsQyv94WPBj8AOUXg+0AZoIa:YS3icZg3OwLnAZoIa
MD5:	621936AFF9F5A401CBDBA7ED16571403
SHA1:	29F29ACC36431B4D59B2C5BF4BE163DAB5F0DEBB
SHA-256:	10EC4FA7950277BECF177024730901D9DAAE25BF03FD394C364AAFE29D33CA7E
SHA-512:	0DF28A112CED2EB54E3B1CBAC018B16991240A064640B737797675325C4791A3485853DB363523CABBF494B05B748EBF4673B355C117EB95855FEF309737D463
Malicious:	false
Preview:	MDMP..... .....IS.a.....4.....H.....$.....`.....8.....T.....@... .....U.....B.....p.... ...GenuineIntelW.....T.....<....R.a/.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9D9.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):	3.693826829409955
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNim86dUB6YFTSUYLgmfL8GS+CpD/89b23sfzSm:RrlsNiN6I6YRSUYLgmfLrS+28f3
MD5:	F60B15870675CDB4422B00D653EFF506
SHA1:	F580DE8D043587932F0272A555FAD4C617E6F798
SHA-256:	04BFA5603A7A900A5848F91F5A0CFFD16A41EC35324C6118871D4A7105652801
SHA-512:	54CB1E94429AFA584ABF7EB51554F4E9D9DE5C6CF8E98A5DD211F29015D16091AD028BDB3D86C3838A9EADEDBCEDE444FF28858C7C3E683F20FB743348ED1 4A
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.>.4.6.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC99.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):	4.430210411043158
Encrypted:	false
SSDEEP:	48:cvIwSD8zstJgtWI9Z1WSC8BsD8fm8M4J2yGtFNO+q84tj26KcQIcQwQXd:uITfHmESNHJE1OxHKkwQXd
MD5:	E61215813E5A9C6F105D95D2D3B85DA6
SHA1:	3D13151819D197C4856EB99B5C9A881CAF0A3021
SHA-256:	16995677FCAE98C3F5AB6860B39580B89D7BD207BBC7AC5EEEA5D60E789E2663
SHA-512:	1B4B4FF5200579514DAFE7DE6AC9413F9F604CA319FF9D410ED65E9094D7707B5029B107AD7D39E59FF90A3C52D7B6453DFD0CA0F5363980DBF17878C869AF2
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="1279572" />.. <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:\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):	4.27231027976809
Encrypted:	false
SSDEEP:	12288:T2EgPRnkPnlSbC9T9+Zo/19pTMxgYg+yM2CDfmM6/BzjmagZ0VjrY:KEgPRnkPnlSbC9j7
MD5:	0952282E9A8B733598FC12A6EAB089AD
SHA1:	CDCECB08EBD1E2DC3D1F958850315EA86B0991C1
SHA-256:	D532EBDC2C479220E74B6C594EC73B30FF2FCE90DEAC7AA86A0A92DE83B7D3C3
SHA-512:	0585D70D59C83374AB85F837A35BFA708E46319427C5489F2EE9F6934A68B90ED1DBE16B3124F82405938316F55A212BFEF5B0D47EA4F7026D906F83D59E054B
Malicious:	false
Preview:	regf[...[...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.rmtmFI.9..... ....?..... .....

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):	3.3974347454025566
Encrypted:	false
SSDEEP:	192:dxsY2l1RrQAGxRCA8YP5FSEsWftx1bxgoJ4XsaJNSdkyFn6yvRrsf8TWfYjdsiDm:jDz5Rftx1bPJ4Xs7FFn7LTZd1DoXzCS
MD5:	1F2A51FB996D298AAD0AD576423CA175
SHA1:	E1E1446F0AB98723F7302916CE450E6FF6EAD747
SHA-256:	14CDC5B0A0F19BA0B829584F4A3977064BA40D1813776CCFF050F2CD2D0103C3

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
SHA-512:	24C660244FBDA76CB5D3A0B844D93B2D3FBA8A9B18148F65F8AB5D7B286D47E791CEA0A078EEE359776B8AC8785A7303DF2D28A5116E07C53A7825733D19DF0 9
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.rmtmFl.9..... ....9...HvLE.>.....Z.....f\..w..,..3ZNZ.V.....0.....hbin.....p.\..,.....nk,....9..... .....&...{ad79c032-a2ea-f756-e377-72 fb9332c3ae}.....nk ....9..... ....Z.....Root.....lf.....Root....nk ....9.....}..... .....*.....DeviceCensus..... vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	6.970978880732997
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:	6zAcNlJXo7.dll
File size:	387072
MD5:	c7e23f2764d6ed9b59b0fed69a4488b0
SHA1:	67f31b13485f91be7952b3df5628f14ef1c86a38
SHA256:	d048f196a39fc7dae500b057fa000ebbb81ae2e6c18b4dd ff445e8d7163f20ab
SHA512:	1184f739b241155c46fda5c005af5010de100dd50f40696 5ae39701029a8304810359cc85e589eefc3afa494c3204f b467691b3f0b23c74eb32be26f3a4ca927
SSDEEP:	6144:zBYrPMTsY8GR3j4fubnY6Zs/Bv6yGM6aSTsfA2q L6jpXNcc6CEteuQJPlgtlpZ5L:yhmT4GbnYks/BJGNWo 2LjpScDEteuOIi
File Content Preview:	MZ.....@.....!..L.!Th is 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	0.817810362251	data	7.40645886779	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: 4668 Parent PID: 3744

General

Start time:	20:59:29
Start date:	01/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\6zAcNlJXo7.dll"
Imagebase:	0xc80000
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: 00000000.00000000.596768757.0000000000A60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.615675303.0000000000B8C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.642951852.0000000000A60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.643045864.0000000000B8C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.597549993.0000000000B8C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.613993965.0000000000A60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.615392489.0000000000A60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.597443170.0000000000A60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.596835233.0000000000B8C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.614123815.0000000000B8C000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6172 Parent PID: 4668

General

Start time:	20:59:29
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\6zAcNlJXo7.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: 6404 Parent PID: 4668

General

Start time:	20:59:30
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\6zAcNlJXo7.dll,Control_RunDLL
Imagebase:	0x9c0000
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: 00000002.00000003.557368858.0000000002D65000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.576404694.0000000000970000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 6176 Parent PID: 6172

General

Start time:	20:59:30
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\6zAcNlJXo7.dll",#1
Imagebase:	0x9c0000
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: 00000003.00000002.595689976.000000000060A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.595650059.0000000000510000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6996 Parent PID: 4668

General

Start time:	20:59:34
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\6zAcNlJXo7.dll,axamexdrqyrgb
Imagebase:	0x9c0000
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: 00000004.00000002.597386823.00000000008E0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.599282857.0000000002D2A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4248 Parent PID: 4668

General

Start time:	20:59:38
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\6zAcNlJXo7.dll,bhramccfbdd
Imagebase:	0x9c0000
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: 00000005.00000002.598946349.000000000072A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.598782764.00000000003C0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 4884 Parent PID: 572

General

Start time:	21:01:12
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: 6324 Parent PID: 6176

General

Start time:	21:01:30
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\6zAcNlJXo7.dll",Control_RunDLL
Imagebase:	0x9c0000
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: 6312 Parent PID: 6404

General

Start time:	21:01:32
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Zsdkqzebleakbz\gnpornwqabjsi.vaq",YawfQDI
Imagebase:	0x9c0000
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: 0000000B.00000002.699398284.0000000002CCA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6300 Parent PID: 6996

General

Start time:	21:01:38
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\6zAcNlJXo7.dll",Control_RunDLL
Imagebase:	0x9c0000
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: 5644 Parent PID: 572

General

Start time:	21:01:47
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

Registry Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 5344 Parent PID: 4248

General

Start time:	21:01:48
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\6zAcNlJXo7.dll",Control_RunDLL
Imagebase:	0x9c0000
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: WerFault.exe PID: 2824 Parent PID: 5644

General

Start time:	21:01:48
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 4668 -ip 4668
Imagebase:	0xfa0000
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: 5544 Parent PID: 4668

General

Start time:	21:01:50
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4668 -s 272
Imagebase:	0xfa0000
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: svchost.exe PID: 4820 Parent PID: 572

General

Start time:	21:01:54
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:	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: 3160 Parent PID: 5644

General

Start time:	21:01:56
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 4668 -ip 4668
Imagebase:	0xfa0000
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: 3860 Parent PID: 4668

General

Start time:	21:01:58
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4668 -s 324
Imagebase:	0xfa0000

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