ID: 532314
Sample Name: IGidwJjoUs.dll
Cookbook: default.jbs
Time: 01:04:32
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

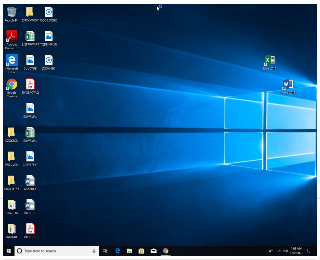
Windows Analysis Report IGidwJjoUs.dll

Overview

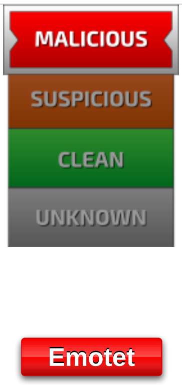
General Information

Sample Name:	IGidwJjoUs.dll
Analysis ID:	532314
MD5:	daf0060326338fd..
SHA1:	b11244a64678d1..
SHA256:	e9f7e82f30ad535..
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

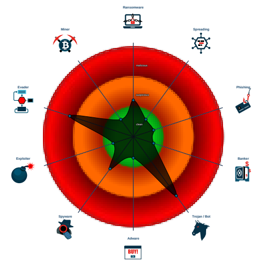


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Sigma detected: Emotet RunDLL32 …
- Changes security center settings (no…
- 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 …
- Checks if Antivirus/Antispyware/Fire…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 2888 cmdline: loaddll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 244 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1752 cmdline: rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 7124 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4408 cmdline: rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5300 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Zataohhmydsvookq\ujdgr.cef",FwwsJBocT MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5004 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Zataohhmydsvookq\ujdgr.cef",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5852 cmdline: rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,ajkaibu MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6260 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6224 cmdline: rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,akyncbgollmj MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6240 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 1240 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2888 -s 316 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4256 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2888 -s 324 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4876 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6388 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6620 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6804 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6908 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 7044 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6124 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 4568 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 4540 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 420 -p 2888 -ip 2888 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4464 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 500 -p 2888 -ip 2888 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4692 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2320 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.495947216.000000000343A000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.554615326.000000000116C000.00000004.00000020.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000000.554615326.000000000116C000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.536076698.00000000006E0000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000006.00000002.536076698.00000000006E0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.loaddll32.exe.1173618.10.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.1173618.10.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.1050000.3.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.1050000.3.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.1050000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 71 entries				

Sigma Overview

System Summary:

Sigma detected: Emotet RunDLL32 Process Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

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)

Lowering of HIPS / PFW / Operating System Security Settings:

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

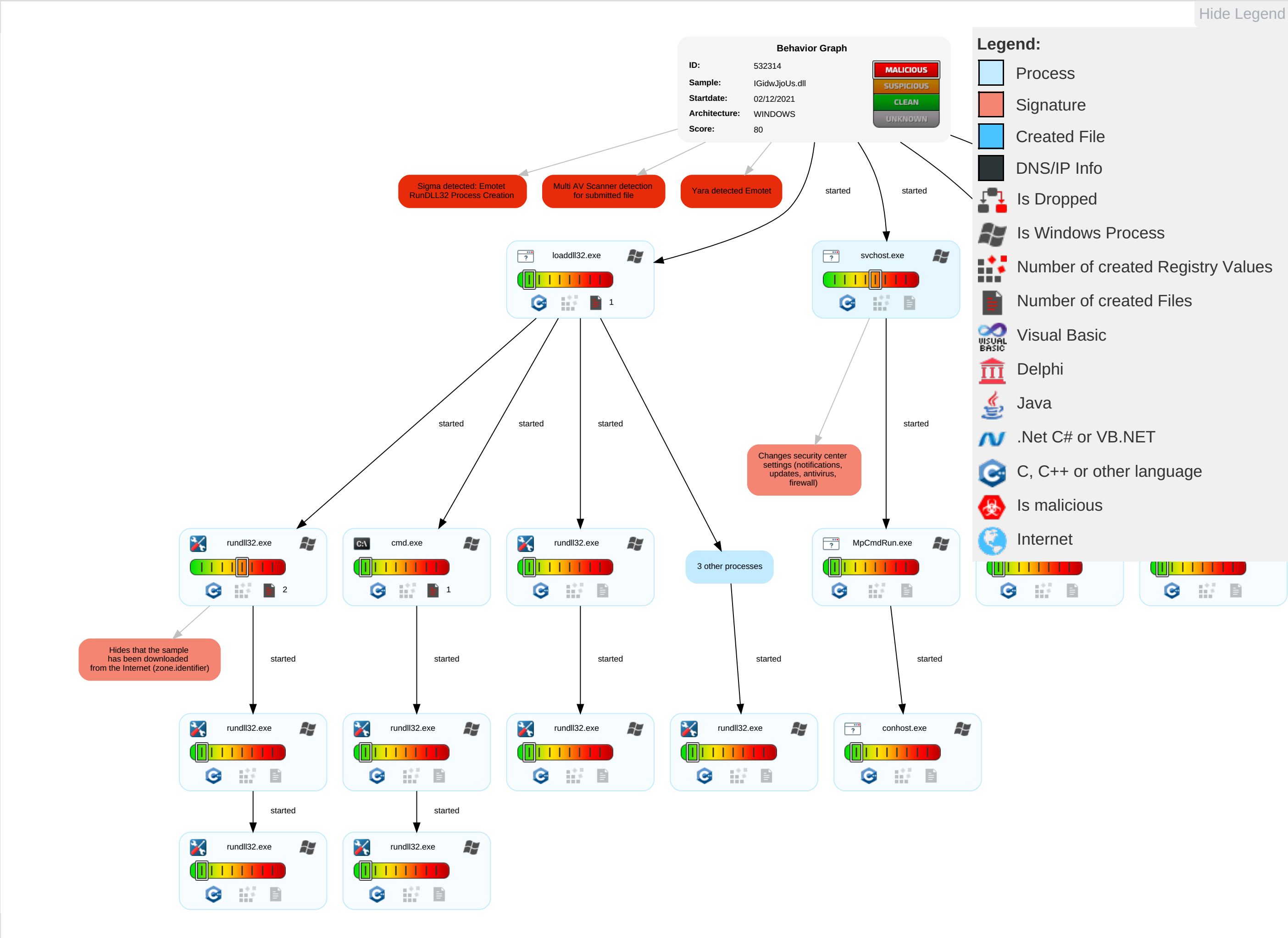
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contrc
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 1 2	Masquerading 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 6 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganogra
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonati
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 3 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfe Protocols

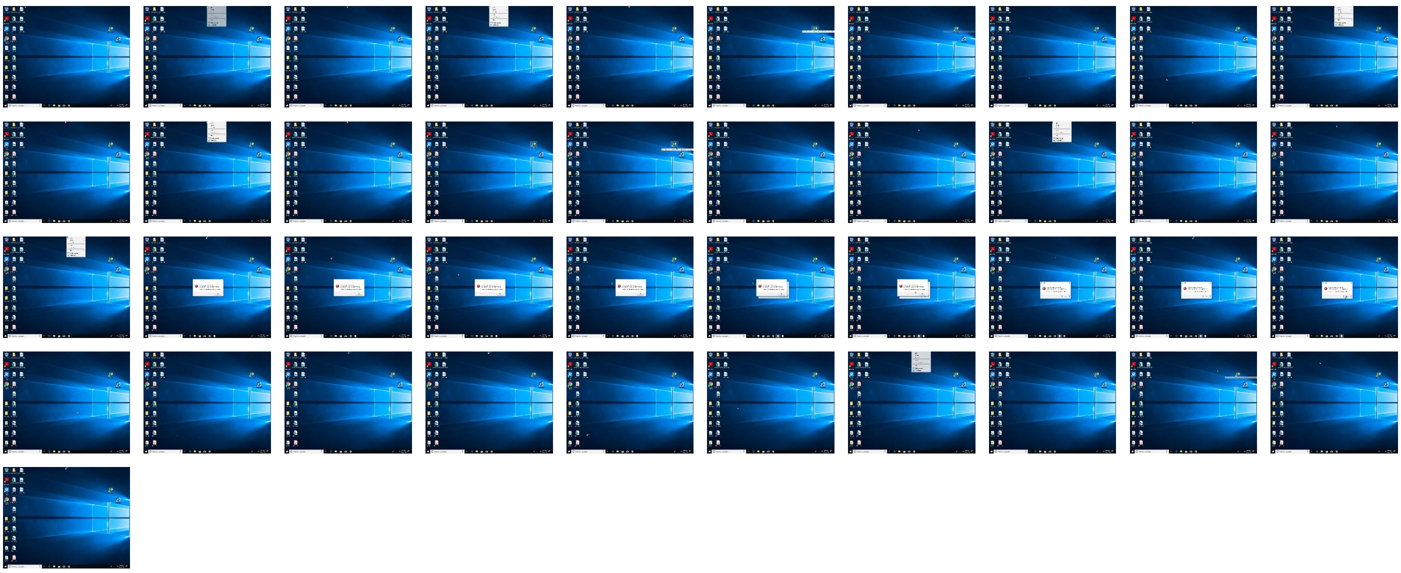
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
IGidwJjoUs.dll	18%	Virustotal		Browse
IGidwJjoUs.dll	18%	ReversingLabs	Win32.Infostealer.Convagent	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.loaddll32.exe.1050000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.1050000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.f10000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.1050000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.f00000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.740000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.4d10000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.1050000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.1050000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.6e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532314
Start date:	02.12.2021
Start time:	01:04:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IGidwJjoUs.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:	30
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@43/21@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.3% (good quality ratio 15.9%) • Quality average: 72.1% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 69% • 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
01:05:38	API Interceptor	1x Sleep call for process: svchost.exe modified
01:08:26	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false
Preview:	............*..........3...w.................C:\ProgramData\Microsoft\Network\Downloader\.. ....C:\ProgramData\Microsoft\Network\Downloader\.. ....0u.................@...@..*.. ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.2494337766405648
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4Y:BJiRdwfu2SRU4Y
MD5:	1D7C749070A76718EDB705A748225B24
SHA1:	34418F0352D91400DDCA472FE731D1FEE57A98D9
SHA-256:	C31EDD64EEB97EBA4914F3362A1B22EE6D054373CEE51633462D4E50375EDF6A
SHA-512:	D16DDE4F537558127EC1DBA2B0EEBA5DD531C5DA23650AA8A21BB592DD1DA6F63F492318239F5894ED771B78A124F78188F3D7E156CDCD8D4B9122DF5DC6A D1
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 0x65aa9c6a, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25044634437712565
Encrypted:	false
SSDEEP:	384:2Tn+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:2TMSB2nSB2RSjlK/+mLesOj1J2
MD5:	263CC3300D13EBFB3E11F4E2FC00E3AB
SHA1:	C04212DF955862740F9AF09DE83C6B9AFF3ACBA8
SHA-256:	791308D7694CBD313658875490C1259A450140271719A579115E84B0F144F3B3
SHA-512:	9045EB4810489E11D27B23ECE6CABBE402B075C09C6193529676E8833B046377C3DFB8BDDD77889CD869B71C3333C423024ED2AEA60BFFDA5F17F20E94539DD B
Malicious:	false
Preview:	e..j... ....e.f.3...w.......................).....:....y..&....y..h.(.....:....y....).............3...w..B...........@............. ....e..:....y......................:....y.. ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07447489620535531
Encrypted:	false
SSDEEP:	3:iGZ7vDpyWt3pbtlB5YG5e3qiH35tlill3Vkttlmlnl:vr9F5pbtlB5jwqiX5tlG3
MD5:	791F708AEDFA55D8084646C8EA2BF2D5
SHA1:	4BBE3A21CBE1369444DDF0CACD45B66144773BF8
SHA-256:	F708BD670876184BDAD24686576CD570C75CDF3DAF6503905D29C5A8F1F389E1
SHA-512:	49A77CFB352F885502A6E580EFB7701D0A453A4BA05FD9488A188B14E21CB4E49F83642A569D740959BD5D6A5E4F000BAF6FD3DBE23E3AC0622C047B6BB1135
Malicious:	false
Preview:	.D.......................................3...w..&....y..:....y..........:....y..:....y....89....yG.....................:....y... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_747b3d3843a661accc8c92924ccfd5a2e2d128_d70d8aa6_0544eac9\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):	0.6752057296335741
Encrypted:	false
SSDEEP:	96:jxnY1ZqyQy9hkoyt7JfqpXIQcQ5c6A2cE2cw33+a+z+HbHgXVG4rmMOyWZAXGngm:6bBpHnM28jjjq/u7sVS274ItW
MD5:	A6D0DA876FCAC1E722DB32168A12BC49
SHA1:	E574ECFC6B972211BC53CF5E79859F9C7E25E856
SHA-256:	7CDA9CF225E6316CCBF2196A34127188D1D0A60782F86CB61B892B4E23E9A25D
SHA-512:	28EF7A64CA822C8E73139BA68CDE4396C450ABE0211B59961EE6F12B9DC75C725D8CFD36E41303379335E96335D8CFD8190E06AF101E851109BCF81ACE84B40
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.=.1.3.2.8.2.9.0.9.6.7.0.2.4.2.0.7.4.4.....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.=.f.7.1.c.4.9.a.e.-.a.6.c.b.-.4.e.0.8.-.a.4.8.4.-.1.8.2.2.f.1.2.a.0.9.b.5.....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.=.1.4.a.9.e.2.a.6.-.0.8.1.a.-.4.0.2.9.-.8.1.3.f.-.6.7.5.9.b.7.0.c.1.2.f.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.b.4.8.-.0.0.0.1.-.0.0.1.6.-.1.a.6.7.-.a.3.b.f.5.b.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_113d29f5\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):	0.6764663920259035
Encrypted:	false
SSDEEP:	96:s8F1HyY1Zqysy9hk1Dg3fWpXIQcQ55c65HcETcw3k+a+z+HbHgXVG4rmMOyWZAXQ:VvLbBkHpt5Ojjq/u7sVS274ItW
MD5:	E5397BA905AE60667648C2C29BB90469
SHA1:	0C68884F7E2E081320B76FAC92BF897D0BF1EE13
SHA-256:	9190EE0BB0584E39D5775B13A9209EA3F8FBF97BA994B9CAD2199E395CF7AD95
SHA-512:	7F8C8FFA2815EE0F401888BD3D888BD3CE6F5C8D9826BF53348A6870B377F72BF89456FDBFBF5E2B97A61273E5F58DD0023F02B6DE478B42A7ADEAFFFF960E0 0
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.=.1.3.2.8.2.9.0.9.6.7.8.0.0.9.0.9.9.5.....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.=.1.3.2.8.2.9.0.9.6.8.8.2.5.9.0.8.8.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.c.b.7.8.7.9.2.-.8.1.1.6.-.4.9.1.e.-.9.c.6.9.-.a.6.3.e.7.e.7.3.d.c.3.5.....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.=.b.5.6.7.b.d.f.a.-.b.8.7.7.-.4.3.f.6.-.8.0.9.2.-.e.e.f.9.8.5.c.e.9.7.6.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.b.4.8.-.0.0.0.1.-.0.0.1.6.-.1.a.6.7.-.a.3.b.f.5.b.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\WER1277.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):	4.431407289465291
Encrypted:	false
SSDEEP:	48:cvIwSD8zsyJgtWI9EKWSC8Bc8fm8M4J2yGtFc+q84tjVKcQIcQwQjd:uITfADrSNPJEkxVKkwQjd
MD5:	75A2D329370D843C52B3B4231710E1BC
SHA1:	812CBE21C7DAA7F06701389DC5C8B11C29950279
SHA-256:	71A271CDC3014F4B5F734A67BC7A2B73F162DF1B6524AA12B21E5DF815679806
SHA-512:	41450AFEEA0391FDE03606A67BB75D569BEE61AD26A5400A73DA7D6A69B74B18F3665B0398DF8E7DCD4B23AD70006E556743037444D5B1678131024744DAA17D
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="1279818" />.. <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\WER247C.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	49554

C:\ProgramData\Microsoft\Windows\WER\Temp\WER247C.tmp.csv	
Entropy (8bit):	3.0785599241529242
Encrypted:	false
SSDEEP:	1536:uVHz6CF22+wD1BSfEZhSiLLsz/4J75J//k3dAQtK:uVHz6CF22+wD1BSfEZhSiLLsz/4JdJ/P
MD5:	9CF6247D5F8C39964C1D993647678FD1
SHA1:	D33A988398CDA516AB1FC217116412954EB5C6F8
SHA-256:	C20B1C089ECCAF8F6899B4294E85A3E9CAC799AA6900DDC6F877640FDCF72769
SHA-512:	017F0CCB212D0DA92E29A385861D567AD8D546BCFDA231D6B04C6A5CD48CB3CBF1A10D96BB57DADE97F3B7909C1B8946C8CA06D0A87DF281E0D8068DB511 99
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\WER2865.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.693829373205794
Encrypted:	false
SSDEEP:	96:9GiZYWqP7ucv+YHqYoWJHWYEZc8tCiyZOOkw7tYDav586q2I6a3:9jZDYydiJ6Dav586qx6a3
MD5:	F3F608A1DE84107FC3AF740BDF5CAD65
SHA1:	A9091B6A08F72BC248C8E4D32E4ECB126E2D1E84
SHA-256:	BCD2445D9DD8CFD94A38B8466C5849F02430283009737AF56BFBC7978BACB9EF
SHA-512:	C428F2C9A74AE7261E8CBA7159BB28BA7150409406CD2155FD6BB0854CBE0F4F2B87A1862AD898A4DC6C7F50387A6DA0E64E97C46B77C0F8396C9D1BD6735F 9
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5264.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	49188
Entropy (8bit):	3.07934217006445
Encrypted:	false
SSDEEP:	1536:B7Hhl+a22dwD0eSfEZcoiN6qJ5DcMXjdDvH2:B7Hhl+a22dwD0eSfEZcoiN6qHDcMXjdK
MD5:	A44253BCA0FA4C66E306BCC2457535A7
SHA1:	FB7D16053992432048E52C8E5D062B7B951B9152
SHA-256:	ED3CF6A7C1D24EB47D0A25EE227A7CA373FFB85B1E7917899A3FA0A7EC818AD4
SHA-512:	7F0E5A586A88B78FEDB66EAE203564717BFE33E75827F8A104B00F91A226CFC6E8142AB661388E6F5BCDAA8212A8F3D2B33A07FF1125EA4FEB5C44B4282EC50 C
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\WER5A35.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6940697525652326
Encrypted:	false
SSDEEP:	96:9GiZYW7fbTrveYOYJW5vH9VYEZCmstCiIZdXywkASPaRvVwbaNI353:9jZDmJmBPaRvVwbaS353
MD5:	8D98D97BECC0B68E92E82022B901A9CE
SHA1:	F297E1BA0C544BB43AAF041EBA44F3FF4471F036

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A35.tmp.txt	
SHA-256:	B3D79C36FBC3790E7DB5EFC6AA38E26E9860098F8DA976B0C5B67907A256CE6C
SHA-512:	5FB4A7A07D86EB9DE4027EE1883BC1AB8481674B1B561CDDCCB3AA42F84C2DCAB1B9B4AD7996C20D9988DC48D568D01CEBBA1E9D3ACC90B4E110197064F92EB
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\WERD94.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):	8300
Entropy (8bit):	3.6932628061268984
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiQO6A6YIkSU9kgmfL8GSpCpDk89bpvsfWrDm:RrlsNiJ6A6YbSU9kgmfLrSYpUfWe
MD5:	02FA653E3B7FF9EF1D6796762EB77295
SHA1:	573A4EB940EB826B95EE84C29B2D01324E129C8E
SHA-256:	B8AC546F0CB99F5380DC9860FAC50535FA5AA7C03539EF757AA7EC1787846D3F
SHA-512:	92C0A82FED8D7F71BCB09139B526A81EE0BD7AB71321042FA091E1032B051E8786AC1064A2B5D15CAA7CE4EEF67FBF09DD10A257BBF0AB03F3109DADE1A6EDBB
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.>.2.8.8.8.<./.P.i.d.>.......

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDDAA.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 09:07:50 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	26864
Entropy (8bit):	2.4866896064953266
Encrypted:	false
SSDEEP:	192:BmGiwUAOKCr6ZEH3ahNorXhaQ+wdmaXKCq2O:CHXKCr6ZQ3ahEXwQ+wdmBH
MD5:	FE5BD39AB26CDA1804F7F937A1176177
SHA1:	24A15841BACC713D43170C3AA8CB91506EE5CC76
SHA-256:	1DE04EAA45370725A9199C5CFA9E64A6D09E094F51F7A81F34BD89C5D27B4CBD
SHA-512:	414A31EBF14BC6D404CE72186454162766EE64C5CD856E91A39CADBB92E3AD68D7FE3F9B1603E714859D61489E1035820696F369DF6859F4A69035E610CC48A4
Malicious:	false
Preview:	MDMP....... ....a............4...............H.......$...........................`.......8...........T...........h....\...U...........B......p.......GenuineIntelW...........T.......H...W..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\WERE135.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8340
Entropy (8bit):	3.702006072530342
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiQp6S6YIiSU/LTgmfcSz3CpBV89bw1vsf6mNm:RrlsNiu6S6Y9SU/LTgmfcSzvw1UfjQ
MD5:	8E0A6A995B2D956DA93DD39059CB5752
SHA1:	5180E6BD8ED2642E3C4F39036C00095750650F7D
SHA-256:	95299B052DF549084F0DE58598398EB067D31C1BCB3A22A0718EA3988C822CD4
SHA-512:	E26852D7083C5F5244DCDBB592292F467B250ECD86E148C2265AEF6F368749D4BB7A02132DF4E12F644415594E639779F1856BB5131E57CC506E06A6ED236732
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE135.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.>.2.8.8.8.<./.P.i.d.>.......

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE4B1.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):	4.472304047501401
Encrypted:	false
SSDEEP:	48:cvIwSD8zsyJgtWI9EKWSC8BN8fm8M4J2ynZFa3l+q84WD5KcQIcQwQjd:uITfADrSNEJ1+3lY5KkwQjd
MD5:	EF9504954F5FBC01AD8AF184205DA2E0
SHA1:	AE2030D98BD2401908FABF9A8C5D965C69674474
SHA-256:	C5CD86556983C8354D010911D51E16151A63D12F4F3D9381F40CF0B74DD4E48C
SHA-512:	C3BA6F4420F0DFE39A6BAAA7766FEB12F806B1A4008185D2774DE36111E50F930357CDA9C38115AA193A619665D1DB497F326842675422B1601B6C0F474587C5
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="1279818" />.. <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\WERFBFF.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 09:07:58 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1059880
Entropy (8bit):	1.3561638552122937
Encrypted:	false
SSDEEP:	24576:uV92esKSlTrTBAzDZFaXulVKppAyqB8yU/xzUE6fRgLFIk14VOx0l+SYDuEcVZ2R:uV92esKSlTrTBAzDZFaXulVKppAyqB8Z
MD5:	E3EC2015DCAC2E09BAD1E5ADAF32CAC1
SHA1:	2CCEB55290055E82AFC4CFE5D8FAB061289C5DE3
SHA-256:	4B3BDCA2BA688BCE27652FC689720AD30BC788FDBA3CA11C14256AEFF8EC2B91
SHA-512:	16BF97F08C8EE745EA31B73844769403481D7D4C45449611EE04D1CF6181FC5E76B6C1761EB44D497FD70B000CF69AFB476475FD9F57792C5CE141CF03838D5E
Malicious:	false
Preview:	MDMP....... ....a............4...............H.......$..........................`.......8...........T...........@...U...........B......p...... .GenuineIntelW...........T.......H...W..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:\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:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBAA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Size (bytes):	7250
Entropy (8bit):	3.1654479336762034
Encrypted:	false
SSDEEP:	96:cEj+AbCEH+AbuEAc+AbhGEA+AbNEe+Ab/Ee+AbPE6w9+Ab1wTEM+AbF:cY+38+DJc+iGr+MZ+65+6tg+ECX+M
MD5:	F20D42D5300A3200C61317A17DFF3C33
SHA1:	8248C42AA3951053D458CBFFC736928DACB53EA5
SHA-256:	C62BB147293301D13842355BD0DCFF6D65656ADDDBD2F0B4FA01C1C4E03306EE
SHA-512:	135AE4E0F3B4521ED93E8F6435C14C4CE16F7FC447BB23A63ADBA1D6B5E84E10D44AA7CA07A324B9AFD9B366D440C37B98D6C333AA59D097FF9D2E76BBE202EC
Malicious:	false
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:. 4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7. 0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211202_090623_120.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.3851779095548746
Encrypted:	false
SSDEEP:	96:WCp2o+xY5T09a/Y0QC81I2lhQkk544hjT2ZjFz/NMCjdJRgj5H:1YfAjB2MZZCfw
MD5:	43B55D5108D146B68FD69AAC21C14970
SHA1:	E00EF50AFD4ECCD3EF226676ACF699845DA84F05
SHA-256:	0F39740266A2B9068C80326ECABA18BA549FC11FE6285AAB4FBC23CBE4EF4220
SHA-512:	3CB242C68BB59A6D91E9108474A5AAFC139350FC5CC41778991B67F0281E397443F668D444F35C10A238FA85372D12CE397042E52415361FDDE9E325CBA9EE2F
Malicious:	false
Preview:	....!......................................8......................B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2.. ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.../_8..... .....)...[..........8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.1.1.2.0.2._.0.9.0.6.2.3._.1.2.0...e.t.l.........P.P...........8.. ....

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):	4.262174448540009
Encrypted:	false
SSDEEP:	12288:oQdWPEaAskcbIckr6re3K35JCmEji6nnTkrGMqzHdU1mLbmcJqDsAML/:jdWPEaAskcbIckrPGLa/
MD5:	89ED9A0DFDE794600247CBB8BAFA8FBB
SHA1:	BCF2F0D3C3F95F0EFD9E17C14628B81E00E6AA07
SHA-256:	A3D51C5C9258BEB30A73C894C1C553DDAF1DB6CA02B289DE453DD7D093FB9825
SHA-512:	74A40097A0AA6CF70FDEF76C1CF6E18CDEC13F22C4300629E8A4CFAC8203D92D95D65853BC5792A996E20410905236FF67C01C97F0F32FBFAB0A20A41CC153A
Malicious:	false
Preview:	regfR...R...p.\..,.................. ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4............E.4............E.....5............E.rmtm..7.\.. ....3l.. ....

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):	3.0448280007830952
Encrypted:	false
SSDEEP:	192:yzxbi18bjzFMTYw5FSE9lMqXyQVWnxuYW2oSKqe8mxwp3uN5J:upG5TXQnxuf2oSPmxwp3uN5J
MD5:	241B84D689B48DD472F434F5FC25B815
SHA1:	52D593F046E75DBBABB014EB0C33A3B69E432ACA
SHA-256:	50F40D9F0CBEF90CA794DAD92E73E15AA0C6CF2CDF0CB05E2E4762EC0937C9F9
SHA-512:	C1443FDA12AA3E40E3CA2E93140C291EEADCA4ACE36485C41B9FFCDCC6163560CE94CB3B33FFDBC5B78F9A94EB7CCC90B7D9D23A0E6CB11F4C8474E82C7A ADCC

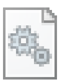
C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Malicious:	false
Preview:	regfQ...Q...p.\..,................... ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4............E.4............E.....5............E.rmtm..7.\.. ....3IHvLE.>......Q...........g.;L[y.a.4k.<...........................hbin................p.\..,...........nk,...:.\................................... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}......nk ...:.\....... ....P............... ....Z.......................Root........lf......Root....nk ...:.\....................}.............. ....*...............DeviceCensus.................... ...vk..................WritePermissionsCheck.......p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.067319727198819
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:	IGidwJjoUs.dll
File size:	372736
MD5:	daf0060326338fd3d153248ca89b40e5
SHA1:	b11244a64678d1e8280b7daf273cb0563ee51803
SHA256:	e9f7e82f30ad5350adb0ad37ac11bc26ae7f3b0879fe33e2a23c97f158c85780
SHA512:	727ab782457d503480cb9e4991634be013effac466daa6431045bbda9f252f36c74b17ba5f94a4438781f950f3fe5e2076ae1b8cc39e273b3746842dc239d71a
SSDEEP:	6144:qRsMh9YQWtcgA70wgF7nJyj6CQK+kIVDRjudJMrt32fFcRmXIeJXjWMmAD:cvm9Y0HFLORQKqV4epRmxAvAD
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........0...Q...Q...Q..E#...Q..E#...Q..E#...Q../$...Q...$...Q...$...Q...$...Q..E#...Q...Q...Q...Q...Q../$...Q../$...Q..Rich.Q.........

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1001a401
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:	0x61A7100E [Wed Dec 1 06:02:54 2021 UTC]
TLS Callbacks:	0x1000c500
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	0x264f4	0x26600	False	0.546620521173	data	6.29652715831	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x28000	0x313fa	0x31400	False	0.822468868972	data	7.43223852179	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5a000	0x1844	0xe00	False	0.270647321429	data	2.60881097454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x5c000	0x66c	0x800	False	0.3583984375	data	2.21689595795	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x5d000	0x1bb0	0x1c00	False	0.784598214286	data	6.62358237634	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: 2888 Parent PID: 1768

General

Start time:	01:05:27
Start date:	02/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll"
Imagebase:	0xad0000
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, Description: Yara detected Emotet, Source: 00000000.00000000.554615326.000000000116C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.554615326.000000000116C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.536378557.000000000116C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.536378557.000000000116C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.553224532.0000000001050000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.553224532.0000000001050000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.537869940.0000000001050000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.537869940.0000000001050000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.553425697.000000000116C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.553425697.000000000116C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.586675822.0000000001050000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.586675822.0000000001050000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.586734813.000000000116C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.586734813.000000000116C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.554273398.0000000001050000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.554273398.0000000001050000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.535907567.0000000001050000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.535907567.0000000001050000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.538443258.000000000116C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.538443258.000000000116C000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 244 Parent PID: 2888

General

Start time:	01:05:27
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4408 Parent PID: 2888

General

Start time:	01:05:28
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,Control_RunDLL
Imagebase:	0x1060000
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, Description: Yara detected Emotet, Source: 00000002.00000003.487102902.000000000327C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000003.487102902.000000000327C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.497144538.0000000000F00000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.497144538.0000000000F00000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 1752 Parent PID: 244

General

Start time:	01:05:28
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",#1
Imagebase:	0x1060000
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: 00000003.00000002.495947216.000000000343A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.496002665.0000000004D10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.496002665.0000000004D10000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5852 Parent PID: 2888

General

Start time:	01:05:32
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,ajkaibu
Imagebase:	0x1060000
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, Description: Yara detected Emotet, Source: 00000004.00000002.533240678.0000000000F10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.533240678.0000000000F10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.534996717.000000000325A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 4876 Parent PID: 556

General

Start time:	01:05:37
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6224 Parent PID: 2888

General

Start time:	01:05:40
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,akyncbgollmj
Imagebase:	0x1060000
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, Description: Yara detected Emotet, Source: 00000006.00000002.536076698.00000000006E0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.536076698.00000000006E0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.536480862.00000000009AA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6388 Parent PID: 556

General

Start time:	01:05:47
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6620 Parent PID: 556

General

Start time:	01:06:05
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6804 Parent PID: 556

General

Start time:	01:06:23
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 6908 Parent PID: 556

General

Start time:	01:06:48
Start date:	02/12/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7bdc40000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 7044 Parent PID: 556

General

Start time:	01:07:10
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 7124 Parent PID: 1752

General

Start time:	01:07:24
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_RunDLL
Imagebase:	0x1060000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5300 Parent PID: 4408

General

Start time:	01:07:25
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Zataohhmydsvookq\ujdgr.cef ",FwwsJBocT
Imagebase:	0x1060000
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, Description: Yara detected Emotet, Source: 0000000E.00000002.627627786.0000000000740000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.627627786.0000000000740000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.627859326.00000000007BA000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6260 Parent PID: 5852

General

Start time:	01:07:39
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_ RunDLL
Imagebase:	0x1060000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6240 Parent PID: 6224

General

Start time:	01:07:45
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_ RunDLL
Imagebase:	0x1060000
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: 4568 Parent PID: 556

General

Start time:	01:07:45
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 4540 Parent PID: 4568

General

Start time:	01:07:46
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 420 -p 2888 -ip 2888
Imagebase:	0x7ff6bbfa0000
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: 1240 Parent PID: 2888

General

Start time:	01:07:48
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2888 -s 316
Imagebase:	0xb30000
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: 4464 Parent PID: 4568

General

Start time:	01:07:54
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 500 -p 2888 -ip 2888
Imagebase:	0xb30000
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: 4256 Parent PID: 2888

General

Start time:	01:07:56
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2888 -s 324
Imagebase:	0xb30000
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: 4692 Parent PID: 556

General

Start time:	01:08:06
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 2320 Parent PID: 556

General

Start time:	01:08:22
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 6124 Parent PID: 7044

General

Start time:	01:08:25
Start date:	02/12/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff6c5670000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5268 Parent PID: 6124

General

Start time:	01:08:26

Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5004 Parent PID: 5300

General

Start time:	01:08:28
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Zataohhmydsvookq\ujdgr.cef ",Control_RunDLL
Imagebase:	0x1060000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

 Joe Sandbox Cloud Basic 34.0.0 Boulder Opal