ID: 532296
Sample Name: Zd9TtpY4Kh.dll
Cookbook: default.jbs
Time: 00:11:07
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

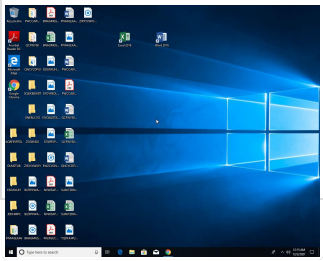
Windows Analysis Report Zd9TtpY4Kh.dll

Overview

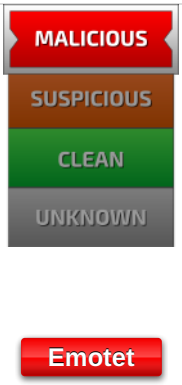
General Information

Sample Name:	Zd9TtpY4Kh.dll
Analysis ID:	532296
MD5:	71eea35f36f3642..
SHA1:	25bcd5a134df55a.
SHA256:	bbadafe48d63d23.
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection



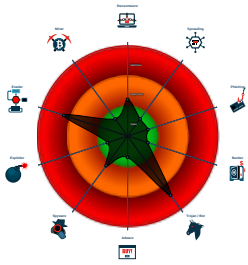
Emotet

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
- 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…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7160 cmdline: loaddll32.exe "C:\Users\user\Desktop\Zd9TtpY4Kh.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 5704 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Zd9TtpY4Kh.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3648 cmdline: rundll32.exe "C:\Users\user\Desktop\Zd9TtpY4Kh.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 7080 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Zd9TtpY4Kh.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5688 cmdline: rundll32.exe C:\Users\user\Desktop\Zd9TtpY4Kh.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3024 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lklkgjuftglvvvqq\zogfgblopvxymh.tnq",YYthscLHd MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6956 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Lklkgjuftglvvvqq\zogfgblopvxymh.tnq",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3180 cmdline: rundll32.exe C:\Users\user\Desktop\Zd9TtpY4Kh.dll,ajkaibu MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 2316 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Zd9TtpY4Kh.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2960 cmdline: rundll32.exe C:\Users\user\Desktop\Zd9TtpY4Kh.dll,akyncbgollmj MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3156 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Zd9TtpY4Kh.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 4488 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7160 -s 320 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1060 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7160 -s 328 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6160 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4072 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5780 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6120 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6668 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5348 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 4020 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 3088 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5676 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5672 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 7160 -ip 7160 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3544 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 548 -p 7160 -ip 7160 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6640 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5696 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4888 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
00000000.00000000.551258636.0000000000C3C000.00000004.00000020.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000000.551258636.0000000000C3C000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.549497176.0000000002F70000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.549497176.0000000002F70000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000F.00000002.662460484.00000000032CA000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.af0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.af0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.c43b40.4.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.c43b40.4.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.2f80000.0.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)

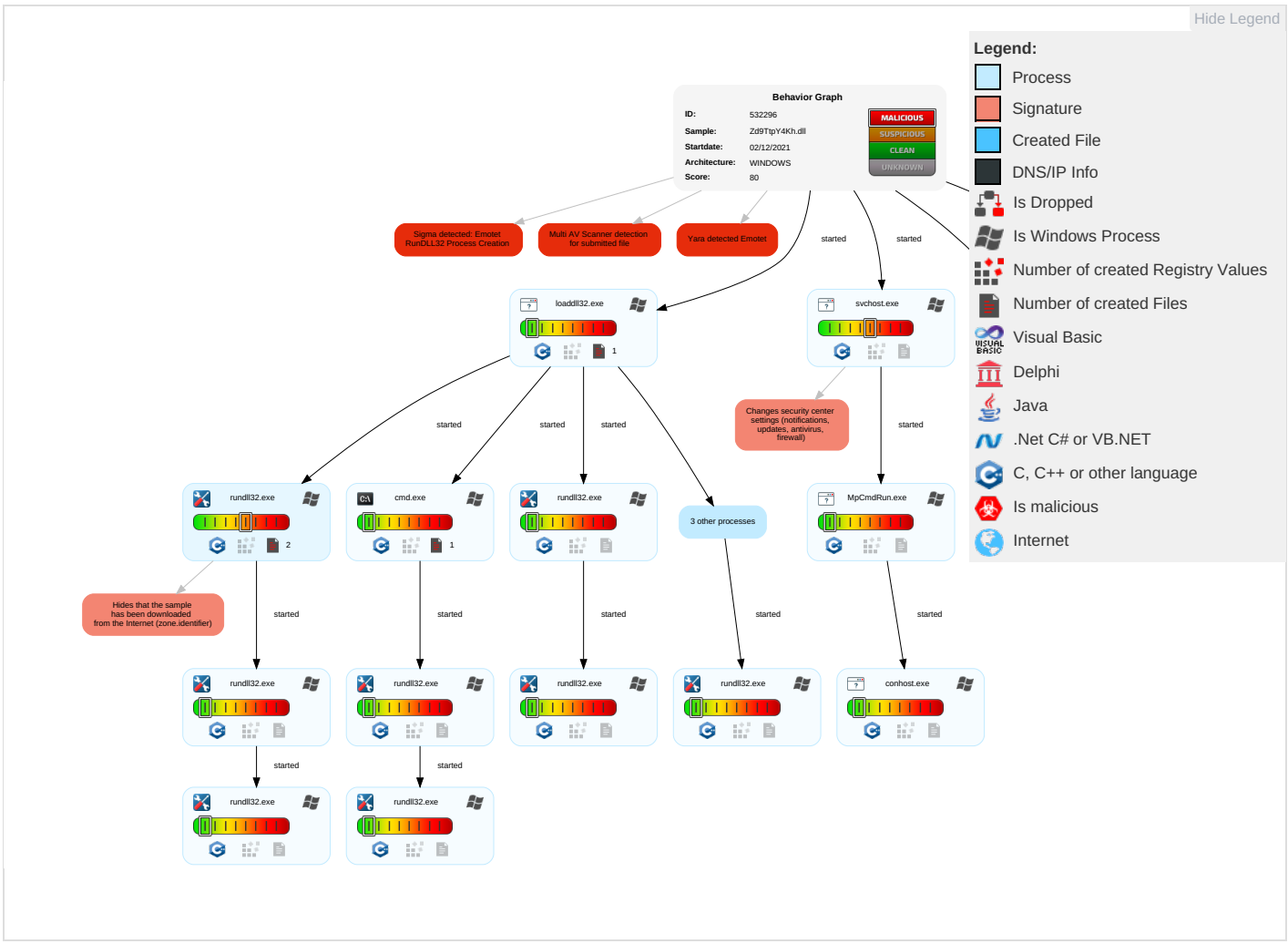
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 1 2	Masquerading 2 1	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 5 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 2	Security Account Manager	Virtualization/Sandbox Evasion 2	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 1 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

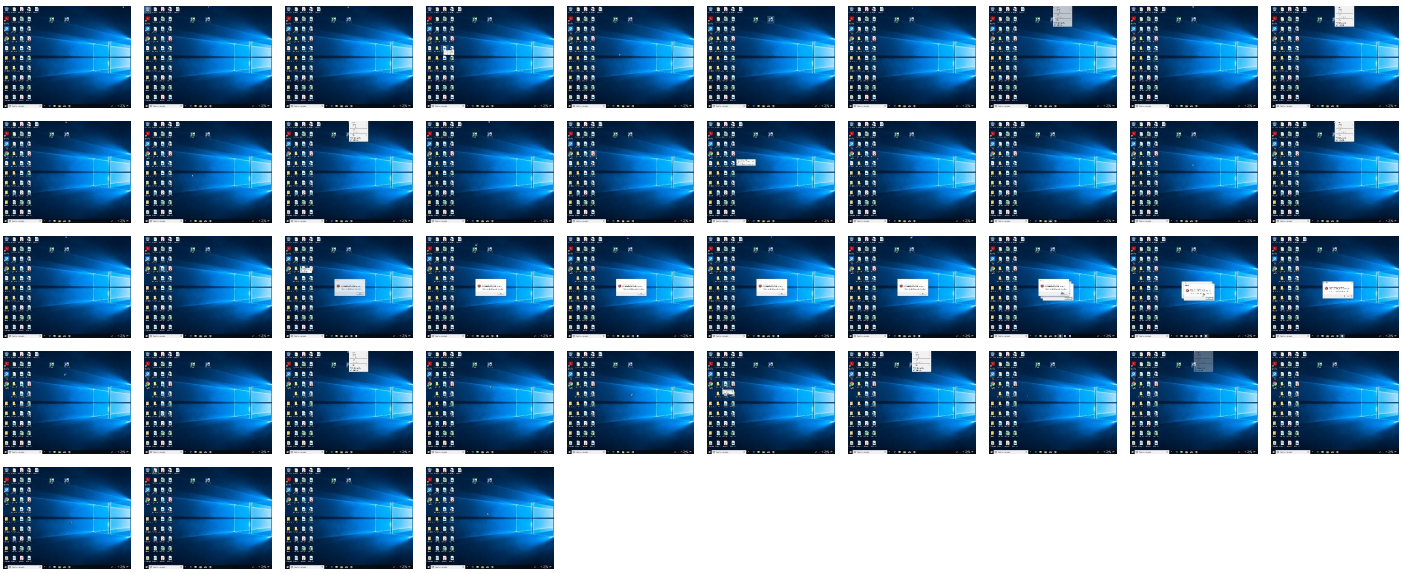
Behavior Graph



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
Zd9TtpY4Kh.dll	19%	Virustotal		Browse
Zd9TtpY4Kh.dll	18%	ReversingLabs	Win32.Infostealer.Convagent	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.2f80000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.3210000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.af0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.af0000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.af0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.2f70000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.2e40000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.af0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.3370000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.af0000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://%s.xboxlive.comlCount	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.comt	0%	Avira URL Cloud	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.com.	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

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532296
Start date:	02.12.2021
Start time:	00:11:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Zd9TtpY4Kh.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:	34
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@45/22@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.3% (good quality ratio 9.7%) • Quality average: 71% • Quality standard deviation: 26.1%
HCA Information:	• Successful, ratio: 78% • 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
00:14:31	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\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_8c5962cbbdb13a8671f1f3c3793157e73bd5d897_d70d8aa6_100270af\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):	0.6753320867819554
Encrypted:	false
SSDEEP:	96:wgrTlZZqyHy9hkoyt7JfapXIQcQ5c6A2cE2cw33+a+z+HbHgfVG4rmMOyWZAXGn1:1XB2HnM28jjzq/u7sxS274ItW
MD5:	2942AEA7B8AF82EB6ECFF7903CFFF142
SHA1:	3712EB77A46D0E9F2D990667AFA57B8D83FECDBF
SHA-256:	E662C417B79C01C77F5B029D02D8EA8B7BDB9D38CC268D9927E8F125CD66BEB1

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_8c5962cbbdb13a8671f1f3c3793157e73bd5d897_d70d8aa6_100270af\Report.wer	
SHA-512:	B6889CDABC5E50C87C2B47BC28DC046A3418D9B2F9B76FECE31F3FE42AA57A38BE131C40F002D50A469C56FA3F89828476C805838EF93A135B124BD05429968
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.=.1.3.2.8.2.9.0.6.4.5.0.0.1.6.1.9.6.6.....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.=.d.1.4.3.c.a.0.5.-.0.2.6.e.-.4.d.8.c.-.a.b.6.3.-.0.1.7.f.c.f.1.1.e.b.d.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.2.f.4.1.0.8.6.-.8.e.9.4.-.4.c.b.a.-.8.e.c.d.-.1.c.4.0.5.e.f.0.b.7.6.8.....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.b.f.8.-.0.0.0.1.-.0.0.1.c.-.d.e.0.0.-.7.4.4.8.5.4.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.8.:.1.1.:.5.3.:.0.5.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_05aea82a\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):	0.6787196257300817
Encrypted:	false
SSDEEP:	96:a1FWsdAlZZqyfy9hk1Dg3fWpXIQcQhc6tcEMcw32+a+z+HbHgfVG4rmMOyWZAXG0:GtdwXBfH/pGojzq/u7sWS274ItW
MD5:	8646FF598D4FC06150C2CF7E8EDF33C5
SHA1:	2CACDDA84AF3B5E580A8A60284208683B22DAE76
SHA-256:	B8480BA00BC4996460F0462BAAA38FD304991DBF6F7C1BF1DE6A90812B02EF01
SHA-512:	4E25AA52C4A879DC37C11AA456B42967A08D2DADD6BD5B4AF6974AA2240BF67234311D5C9BD428C5EADCBF23956E857386B1FEF8B0601AECD7EBC61ECFBEEFF1
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.=.1.3.2.8.2.9.0.6.4.5.8.3.1.8.3.4.1.9.....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.=.1.3.2.8.2.9.0.6.4.6.6.4.7.4.5.4.9.1.....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.=.c.d.3.6.d.b.4.3.-.a.9.b.5.-.4.2.3.7.-.8.4.c.9.-.e.c.2.1.d.a.3.9.8.a.f.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.b.0.0.1.f.3.e.-.a.e.5.7.-.4.2.7.3.-.b.3.8.5.-.3.0.c.9.3.8.d.e.7.8.4.2.....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.b.f.8.-.0.0.0.1.-.0.0.1.c.-.d.e.0.0.-.7.4.4.8.5.4.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER619B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 08:14:10 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	27296
Entropy (8bit):	2.4496135500113585
Encrypted:	false
SSDEEP:	192:B/uQnOF7sxmwUdC1f4q/2zZqgRV+u/X3nMjL:VOF4xxUzq/IZqgRV+tL
MD5:	48BAB300890DD1EF75CD3CC584DF13D2
SHA1:	7C7201885E93459325C4E5B3940C563DE8F05058
SHA-256:	2B5204A506A8CD877068233DF71590DE7797443342876C3764F48F1A2F2AFB47
SHA-512:	4CE15DF79846F4C325D55B9525424C9E213AD6FCDC30533DE365B677D4AA3A696F4EA4B0716165AE7022C442F8F34F0E3F7732CFFB3A020981EACCD936D2794
Malicious:	false
Preview:	MDMP..... .....R..a.....4.....H.....$.....`.....8.....T.....h...8^.....U.....B.....p.... ...GenuineIntelW.....T.....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\WER6621.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):	3.7009428538679376
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiyg6wF6YFlSUXUogmfsSzrCpBH89b/xsfu1m:RrlsNiV6K6YHSUXUogmfsSz5/qf9
MD5:	1D77C71A5367724D9CEB685C9F5CC434
SHA1:	3AE81F517F3A3EF16F847303F91D5AEA332EBBB9
SHA-256:	95A4D059393BC6FC0A63AFB231B1825654BD5F8A87D31688B3E733190DC71AE2
SHA-512:	D899EE2077987092EA9B4986DA129E3470E2623F3BCC942F0AD4505391203DEB3EF31D8DB1A6445F7DC210772A469653AB4042CE0ADB18E991B58DD1D8E6B9E
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6621.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.>.7.1.6.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER693F.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):	4.476303673243138
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI9LfrWSC8Bd8fm8M4J2yzZFhqS1+q84WviKcQIcQwQjd:uITfikfaSNcJJNqS1giKkwQjd
MD5:	347129E1AB29C723F836D648A022B855
SHA1:	97E8F1243FDE920242988D77A8F1B18E97BBEC39
SHA-256:	7AD8C4F631EE463D470BE14DAB32A0CA37B441CE4E8FA3B81378416D94C184CB
SHA-512:	178DD584E30F8DD7469185BBE5EDF4063311E82757D245B0E5C80D5B1D38C21D975FCC8CD368DACC219D3BA36D161FAECA3312A786DA4236435F23ADEAA96 77
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="1279764" />.. <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\WER8214.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 08:14:22 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1060392
Entropy (8bit):	1.3584266274072105
Encrypted:	false
SSDEEP:	1536:Ykl8bZzasOdOwq6r+P3wLBAtC1fFlKG4x5PHslEQw2UW6qXxSBnsGZJMRAEAcE4g:YkqY4GStTx5yEQxUW5SxFJDjcv5q
MD5:	2E3157B5FAEA804ADA457C35B7025DEB
SHA1:	9CF23A66D8083A264727710D6C9953F540DEBF97
SHA-256:	CDAABCB34EE2755616A5B2829C6F64AFCBB6A66BC12C95F8FFD730E7794A5EB4
SHA-512:	69C5CBD63769AFE71CCC860D6328C07FD370DF1AB3BC88EBAC614B262B004B340A890CFE0130B46D07782F49908F4A10DBF9ED7105DA04D26BD94AE81B0C3F A
Malicious:	false
Preview:	MDMP..... .....^..a.....4.....H.....$.....`.....8.....T.....@....!.....U.....B.....p.... ...GenuineIntelW.....T.....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\WER9733.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):	3.6933591103329553
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiyU6T6YF/SU5D3ZeLgmfL8GSaCpDa89buxsfw6m:RrlsNiB6T6Y9SU5rZeLgmfLrS5uqfs
MD5:	E63F177331952091E6513CB7985728BD
SHA1:	68C187A2A2CFBFF03E8A93BD5FFE2CAA529028D4
SHA-256:	67127BB111BE435AB9B421A30247504A6DEBD0C9AFCC28A1C57C360E95666C9A
SHA-512:	9D965BFC6C13784145D53D96BA2339DC938E41637FDF3B6DD1399A2D1B7019DE50066FD1B67BAD66A4F60D90D6BEC1BC6C99589D946D7712D62AB5A457E56D 1
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.6.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER99E3.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	52524
Entropy (8bit):	3.0562160554441116
Encrypted:	false
SSDEEP:	1536:I8HQ0ake2NRDoBBlWqUqzSoPKT2gAfbqiqFRFElX8KpHtA:I8HQ0ake2NRDoBBlWqUqzSoPKKgAfbq/
MD5:	F86FF9E6E88A1012FE6DFE79E7420048
SHA1:	2904DB59CC28796D2CAC4EB8867EF6234C12A2C4
SHA-256:	6A3A7CB5D6FCF190D902D69C202CB56DF7C10BFE9CE09285E94AF9BBA10D7715
SHA-512:	75C1FB763027766730F3913AD2AF55E3F2157690F85D5DC747EB15E58808BF7E8945D3EB8E0D1DD68E268E6192271D47E945151CE45FB989BAA9838451F2101F
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\WER9A80.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):	4.432852489939999
Encrypted:	false
SSDEEP:	48:cvIwSD8zsHrJgtWI9LfrWSC8BW8fm8M4J2yGtF34+q84tjuKcQIcQwQjd:uITflkfaSNtJE/4xuKkwQjd
MD5:	9F71DF08B6FF40D4938B4645A43E11D3
SHA1:	46441D798F65ACAA5E3EDABE76438DFE82E7CE70
SHA-256:	438B6C622C11262F8E3AB730ED9D0D6C9D9E003FC988A09165A8BB10CEF64049
SHA-512:	67E5970DACD8EA0D4C9F1847501FA2994E481FE7A8E1745DF7C1C89AB79AFA2B8FF04B49BEF0B2CA9CEF397035715422EA24E5B8E7D60A79CAE3D90E2EE59075
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="1279765" />.. <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\WER9E0A.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6959719835051303
Encrypted:	false
SSDEEP:	96:9GiZYWZX1an5YoYls/WcdiHqUYEZUjCtFiKOYzpw123zAa5PyFGIIMH3:9jZDYv5j7Aca5PyFGvMH3
MD5:	7493BE388D7B1361500832A523ECEB35
SHA1:	7CEDD802AA324CE0A1275288587E93590EF32ED6
SHA-256:	255E49837035B5A12CA74F2DB96A6937FC7C725AFD44BAB7610402145C5F90F0
SHA-512:	13D0496625673581E4D4E644CBC3759D27237103287731BEC5AD8E76714E07A0601EF71A21D29182626667A46FC53E1D8327C5F2AB63E3BE293ADF25928B599C
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\WERCBB3.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51736
Entropy (8bit):	3.0572069490916234
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBB3.tmp.csv	
SSDEEP:	1536:f8Hmfebm2PRzBBlWquy0SYxT4QC5ZKnfFbkvyxfePYfr:f8Hmfebm2PRzBBlWquy0SYxTlC5ZKnfD
MD5:	5A2C103E88C340429F27B7BCBA7F4F2A
SHA1:	1E4AB9E888BED85E4C46249C7DF289C4F6AEE50B
SHA-256:	F94B19FB0B0624653553F24F20B6BD3E7F1A71178755D5360FBD398A10F41DC8
SHA-512:	4C894A5418DC58E0A535C6426567ADAF931F78FD05FBEB103D7D19A94B52F5189C8016175E04A9E783295ECE2E71062EEEB9AE2397F0DB6B1BF72F7F5CB4237
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\WERCF9C.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	modified
Size (bytes):	13340
Entropy (8bit):	2.695808825745679
Encrypted:	false
SSDEEP:	96:9GiZYWIUQ1kj4Y9YoemWoywiHAUYEZKqtrinO7zpwZT2awoHf9jxIi+UI3:9jZDIrqPrr6awoHf9juLb3
MD5:	C7B504A897028671DB87C540106E01A4
SHA1:	D9DF308551597C154A145D9720E577FEC8555F55
SHA-256:	F54378E366A7EE979EA6BF8CACB629B85A9885429C4D33F4F26548FD7ECC68F4
SHA-512:	060F7834E16080F35FB07F9C21E0E5F60F15485A77A408152523005472AB3A86D372BA011B150761D8C5702BA4822B693752F51466E70219DBFD7F8C91B84DF8
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:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1101727836969861
Encrypted:	false
SSDEEP:	12:26OXm/Ey6q9995wNq3qQ10nMCldimE8eawHjcWY:26bl689LyMCldzE9BHjcWY
MD5:	3CE7F38F89EF417650ECF65996A5FEAF
SHA1:	E09EE7E0D824A631FC3455C83B8260AEC891F0DB
SHA-256:	38903E98E296A605F337345380C3412BEB053B92E851A2E8A93902D33EDC6482
SHA-512:	2415752F9A16E1B704CDF1F08CFFC040AF67FEEB472B6C2B1EB7C4CDA8C92DC35B331D538F522DE969D8C2745BF2B1EB98B6934938CD6E9D5B7A45786FD3920
Malicious:	false
Preview:	.....C.&F.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2.....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....*~..... .....o.!\T.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....&F.....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11282471699365751
Encrypted:	false
SSDEEP:	12:/jXm/Ey6q9995qL1miM3qQ10nMCldimE8eawHza1miIJiP:yl68U1tMLyMCldzE9BHza1tIJC
MD5:	0F00364F438F5B4D13D69737547D320F
SHA1:	D28AF2306FE5325E04B78DF47E6D04B80E4A6727
SHA-256:	AF0D283BF1284D6752F83B1247E066048BB34E33159C6E26123040AE16E3AB6A
SHA-512:	D26DE87258C870EB7DFDF7ECDC20F5D43BC444F1BB7E60A9C016FDDE90573DE52B4515425D9B9A2889E656F3A8567479EC3C05F2CB81F4BC407D5530EB258E5
Malicious:	false

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Preview:	.....!F.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....*~..... .....\T.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....!F..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11276288886055777
Encrypted:	false
SSDEEP:	12:E6jXm/Ey6q9995s1mK2P3qQ10nMCldimE8eawHza1mKwVP:E/l68K1iPLyMCldzE9BHza1Et
MD5:	053D031988020BD2FDC75BBB73C241F5
SHA1:	12BECAE5329157EA3F42CE1CD28D35FC777FFDB2
SHA-256:	DA5E6DEF835D0B360ACDD0416C828251C2404BE2A97490BF30C6247A62647F03
SHA-512:	C4C1242685B183DD9CB62E86E33E08D6BAE045BDB95E87E45B6E24317CEF889A9F58DC00CA9B9A9F36F40EBC480BA41AB5B2566CD9F0E8C48C75925268D3B2 0D
Malicious:	false
Preview:	.....c.F.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....*~..... .....[.[T.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....j.F..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001.@ (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1101727836969861
Encrypted:	false
SSDEEP:	12:26OXm/Ey6q9995wNq3qQ10nMCldimE8eawHjcWY:26bl689LyMCldzE9BHjcWY
MD5:	3CE7F38F89EF417650ECF65996A5FEAF
SHA1:	E09EE7E0D824A631FC3455C83B8260AEC891F0DB
SHA-256:	38903E98E296A605F337345380C3412BEB053B92E851A2E8A93902D33EDC6482
SHA-512:	2415752F9A16E1B704CDF1F08CFFC040AF67FEEB472B6C2B1EB7C4CDA8C92DC35B331D538F522DE969D8C2745BF2B1EB98B6934938CD6E9D5B7A45786FD392 0
Malicious:	false
Preview:	.....C.&F.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....*~..... .....o.!\T.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....&F..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11282471699365751
Encrypted:	false
SSDEEP:	12:/jXm/Ey6q9995qL1miM3qQ10nMCldimE8eawHza1miIJiP:yl68U1tMLyMCldzE9BHza1tIJC
MD5:	0F00364F438F5B4D13D69737547D320F
SHA1:	D28AF2306FE5325E04B78DF47E6D04B80E4A6727
SHA-256:	AF0D283BF1284D6752F83B1247E066048BB34E33159C6E26123040AE16E3AB6A
SHA-512:	D26DE87258C870EB7DFDF7ECDC20F5D43BC444F1BB7E60A9C016FDDE90573DE52B4515425D9B9A2889E656F3A8567479EC3C05F2CB81F4BC407D5530EB258E 5
Malicious:	false
Preview:	.....!F.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....*~..... .....\T.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....!F..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11276288886055777
Encrypted:	false
SSDEEP:	12:E6jXm/Ey6q9995s1mK2P3qQ10nMCldimE8eawHza1mKwVP:E/l68K1iPLyMCldzE9BHza1Et
MD5:	053D031988020BD2FDC75BBB73C241F5
SHA1:	12BECAE5329157EA3F42CE1CD28D35FC777FFDB2
SHA-256:	DA5E6DEF835D0B360ACDD0416C828251C2404BE2A97490BF30C6247A62647F03
SHA-512:	C4C1242685B183DD9CB62E86E33E08D6BAE045BDB95E87E45B6E24317CEF889A9F58DC00CA9B9A9F36F40EBC480BA41AB5B2566CD9F0E8C48C75925268D3B2 0D
Malicious:	false
Preview:	....c.F.....................B.............Zb...@.t.z.r.e.s...d.l.l.,.-.2.1.2.. ....@.t.z.r.e.s...d.l.l.,.-.2.1.1...*~..... ......[.[T...........U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.......P.P..........j.F... ....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.1622931047337053
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zN+C:j+s+v+b+P+m+0+Q+q+W+C
MD5:	FC3AFFCF97A1A5733C72E7F0DC6F1AD0
SHA1:	7D6B5F184B0276AF67E2879629FB1AD21E1AFC7A
SHA-256:	FEBCA5E4725467FB260B0F828509F83926E3C2A5614772C0885135229862404F
SHA-512:	4DEBB3A0F3B9EC42D3C15E2E362905EFD3D3A53306B19D21468D79A7EA566593E06D163F91B0B8A1CEAC1D52050CC252FFFD6A422D7089F7E4F16B57F9DE39 9
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_081236_088.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.812286787040644
Encrypted:	false
SSDEEP:	96:eClL/o+JY5D09X/Y3QChIl2la1kjO4Q8T2ojFzfNMCxdJRBj5DvJNMC+j5KNMCEj:dxDP8N2urZCVyCACdCdCHCZ
MD5:	EFEE713F3ACA51F7ED7129B8E4F6FC18
SHA1:	2BA88756ADD0CB0D3953EE56C1B2E4236250655E
SHA-256:	745C4C76F9C660FA985E9ABB55A39F4CECAADB9300D32D95B0BB72AD2639DACA
SHA-512:	97CA3203AF07516908CE86ED4906F0C925A183FAF2EE885E53D926BDA1AAB1975F7C1F681CA2F730E84554F052C2D4C7BC960CF9BFE80C68FF7CF017C3F33BE C
Malicious:	false
Preview:	....!...................................S.7......................B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2.. ....@.t.z.r.e.s...d.l.l.,.-.2.1.1... ....j]T...........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._.0.8.1.2.3.6._.0.8.8...e.t.l.........P.P.........S.7... ....

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):	4.274090843410231
Encrypted:	false

C:\Windows\appcompat\Programs\Amcache.hve	
SSDEEP:	12288:ILoa5fBuPHoEyz8F0TokuhNNblFkoZyuQCWHLeIO/Nn3qGc1wRhmg:0oa5fBuPHoEyz8XY
MD5:	B456D5F1DC4A07CE35BCAAD0ABD74B5F
SHA1:	AEC31AF5685FD9FA0DCB94CD7FD673CC60CD1685
SHA-256:	EB2B7FAE1AAD7513B2E03518CE9FBB2D4E9B0937E0F1ACB85B449225567B1264
SHA-512:	B5EB675086BC8162C8EBDCE659162ADF5C3AAD1D3C79FAA5C1A3C0F9451BC5B9268867075264069CA17089D4477E3ADC79D0C5C0E299777E8E2651B73FBF809
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.rmtm....T..... ....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.4022660043043857
Encrypted:	false
SSDEEP:	192:RdUMc1G2e9XiUYq5FSEsWftx18xgoJ4X7aJNSdkyFn6yvRrsftWfYjdsiDoXzC5:P7p5Rftx18PJ4X77FFn7WZd1DoXzC5
MD5:	33571DE23356636B568AB4C7C2EB62CF
SHA1:	7A2C34637F41F28753839E8218ECB3E68ED666EF
SHA-256:	9303B44A797C6A567D519B8A57C0B41F292A5CCDDD90BB7DBF8017DA5E808E28
SHA-512:	5A399F2A564E4A8EC7833F4E48A81D1EB97D5872BC5CC3D0B482CCC956ABE08BB4AD25CC166C5AAC0479C30A4AC536D1BB088847DDBF4CE1D7536790E1C82C3
Malicious:	false
Preview:	regfZ...Z...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm....T..... ....<...HvLE.>.....Z.....P.<w..-.bd.L.....0.....hbin.....p.\..,.....nk,.....T..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .....T..... ....Z.....Root.....lf.....Root....nk .....T.....}..... .....*.....DeviceCensus..... .vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.0673548336573475
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:	Zd9TtpY4Kh.dll
File size:	372736
MD5:	71eea35f36f3642fdbb94d9310e87747
SHA1:	25bcd5a134df55a5465ebe39f57bf758d5672197
SHA256:	bbadafe48d63d23d3a2ebb4a4103e32646d314d5ffb8e2551d62270f8b3ec352
SHA512:	c6d3628bc45cd0cf237d82f31b170dbffd117e13b6f9ba22f51c81ad91eeb6e992cd253b7b27c0d868078e8686c3b21e6f03ecbe9f8ef9c9725b920eb9f462d0
SSDEEP:	6144:qRsMh9YQWtcgA70wgF7nJyk6CQK+kIVDRjudJMrt32fFcRmXIeJXjWMmAD:cvm9Y0HFLFRQkqV4epRmxAvAD
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	7.43227552322	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: 7160 Parent PID: 4620

General

Start time:	00:12:01
Start date:	02/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\Zd9TtpY4Kh.dll"
Imagebase:	0x1150000
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: 00000000.00000000.551258636.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.551258636.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.552293543.0000000000AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.552293543.0000000000AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.568744360.0000000000AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.568744360.0000000000AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.552423599.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.552423599.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.569816044.0000000000AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.569816044.0000000000AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.569948888.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.569948888.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.568827402.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.568827402.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.598491073.0000000000AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.598491073.0000000000AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.551169265.0000000000AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.551169265.0000000000AF0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.598587675.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.598587675.0000000000C3C000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6160 Parent PID: 572

General

Start time:	00:12:01
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
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

Analysis Process: cmd.exe PID: 5704 Parent PID: 7160

General

Start time:	00:12:01
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\Zd9TtpY4Kh.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: 5688 Parent PID: 7160

General

Start time:	00:12:01
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Zd9TtpY4Kh.dll,Control_RunDLL
Imagebase:	0xba0000
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: 00000003.00000002.549497176.0000000002F70000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.549497176.0000000002F70000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000003.518552205.00000000030C5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000003.518552205.00000000030C5000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 3648 Parent PID: 5704

General

Start time:	00:12:01
Start date:	02/12/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\Zd9TtpY4Kh.dll",#1
Imagebase:	0xba0000
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: 00000004.00000002.548909255.0000000002F80000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.548909255.0000000002F80000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.549093887.000000000313A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 4072 Parent PID: 572

General

Start time:	00:12:01
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:	0x7ff70d6e0000
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: 5780 Parent PID: 572

General

Start time:	00:12:02
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 3180 Parent PID: 7160

General

Start time:	00:12:05
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Zd9TtpY4Kh.dll,ajkaibu
Imagebase:	0xba0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.547372307.000000000340A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.547342704.0000000003370000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.547342704.0000000003370000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 2960 Parent PID: 7160

General

Start time:	00:12:10
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Zd9TtpY4Kh.dll,akyncbgollmj
Imagebase:	0xba0000
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: 00000008.00000002.547349453.0000000002E40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.547349453.0000000002E40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.547377185.0000000002E7A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6120 Parent PID: 572

General

Start time:	00:12:19
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:	0x7ff70d6e0000
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: 6668 Parent PID: 572

General

Start time:	00:12:36
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:	0x7ff70d6e0000
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: 5348 Parent PID: 572

General

Start time:	00:12:55
Start date:	02/12/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff62f470000
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: 4020 Parent PID: 572

General

Start time:	00:13:13
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7080 Parent PID: 3648

General

Start time:	00:13:50
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\Zd9TtpY4Kh.dll",Control_RunDLL
Imagebase:	0xba0000
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: 3024 Parent PID: 5688

General

Start time:	00:13:53
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lklkgjuftglvvvqq\zogfgblopvxymh.tnq",YYthscLHd
Imagebase:	0xba0000
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: 0000000F.00000002.662460484.00000000032CA000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.662344438.0000000003210000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.662344438.0000000003210000.00000040.00000010.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2316 Parent PID: 3180

General

Start time:	00:13:59
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\Zd9TtpY4Kh.dll",Control_RunDLL
Imagebase:	0xba0000
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: 3156 Parent PID: 2960

General

Start time:	00:14:04
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\Zd9TtpY4Kh.dll",Control_RunDLL
Imagebase:	0xba0000
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: 5676 Parent PID: 572

General

Start time:	00:14:06
Start date:	02/12/2021
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: WerFault.exe PID: 5672 Parent PID: 5676

General

Start time:	00:14:06
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 7160 -ip 7160
Imagebase:	0xa70000
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: 4488 Parent PID: 7160

General

Start time:	00:14:08
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7160 -s 320
Imagebase:	0xa70000
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: 6640 Parent PID: 572

General

Start time:	00:14:11
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:	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: 3544 Parent PID: 5676

General

Start time:	00:14:14
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 548 -p 7160 -ip 7160

Imagebase:	0xa70000
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: 1060 Parent PID: 7160

General

Start time:	00:14:16
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7160 -s 328
Imagebase:	0xa70000
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: MpCmdRun.exe PID: 3088 Parent PID: 4020

General

Start time:	00:14:31
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:	0x7ff6cdb30000
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: 5216 Parent PID: 3088

General

Start time:	00:14:31
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5696 Parent PID: 572

General

Start time:	00:14:40
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:	0x7ff70d6e0000
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: 4888 Parent PID: 572

General

Start time:	00:14:53
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6956 Parent PID: 3024

General

Start time:	00:14:55
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Lklkgjuftglvvvqq\zogfgblop vxymh.tnq",Control_RunDLL
Imagebase:	0xba0000
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