ID: 532299
Sample Name: 5i3yQOSqTm.dll
Cookbook: default.jbs
Time: 00:16:52
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

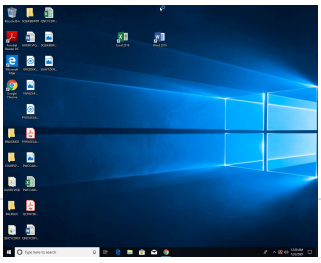
Windows Analysis Report 5i3yQOSqTm.dll

Overview

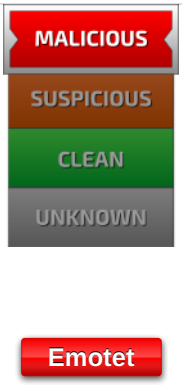
General Information

Sample Name:	5i3yQOSqTm.dll
Analysis ID:	532299
MD5:	1e3db971ac31b8..
SHA1:	8f47d8c2d75df49..
SHA256:	df1aec18655ffd0…
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection



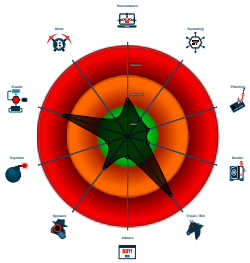
Emotet

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: 4340 cmdline: loaddll32.exe "C:\Users\user\Desktop\5i3yQOSqTm.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6140 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\5i3yQOSqTm.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5996 cmdline: rundll32.exe "C:\Users\user\Desktop\5i3yQOSqTm.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 1308 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\5i3yQOSqTm.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2220 cmdline: rundll32.exe C:\Users\user\Desktop\5i3yQOSqTm.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4144 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Pmleysyipg\sjdwpny.iso",qxtrVBTbrIKuSW MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 4784 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Pmleysyipg\sjdwpny.iso",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4708 cmdline: rundll32.exe C:\Users\user\Desktop\5i3yQOSqTm.dll,ajkaibu MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 336 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\5i3yQOSqTm.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5724 cmdline: rundll32.exe C:\Users\user\Desktop\5i3yQOSqTm.dll,akyncbgollmj MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4908 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\5i3yQOSqTm.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 6640 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4340 -s 308 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 476 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4340 -s 316 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6148 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6400 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- wermgr.exe (PID: 2016 cmdline: "C:\Windows\system32\wermgr.exe" "-outproc" "0" "572" "2360" "2316" "2356" "0" "0" "2352" "0" "0" "0" "0" "0" MD5: FF214585BF10206E21EA8EBA202FACFD)
- svchost.exe (PID: 3428 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6320 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 3744 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 504 -p 4340 -ip 4340 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6704 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 548 -p 4340 -ip 4340 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 7144 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5000 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 4840 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6096 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1756 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2960 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3912 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.594385432.0000000000B10000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.594385432.0000000000B10000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.539875956.00000000046D0000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.539875956.00000000046D0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.546111377.0000000000B10000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.rundll32.exe.940000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.940000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.d83b40.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.d83b40.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.b10000.0.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)

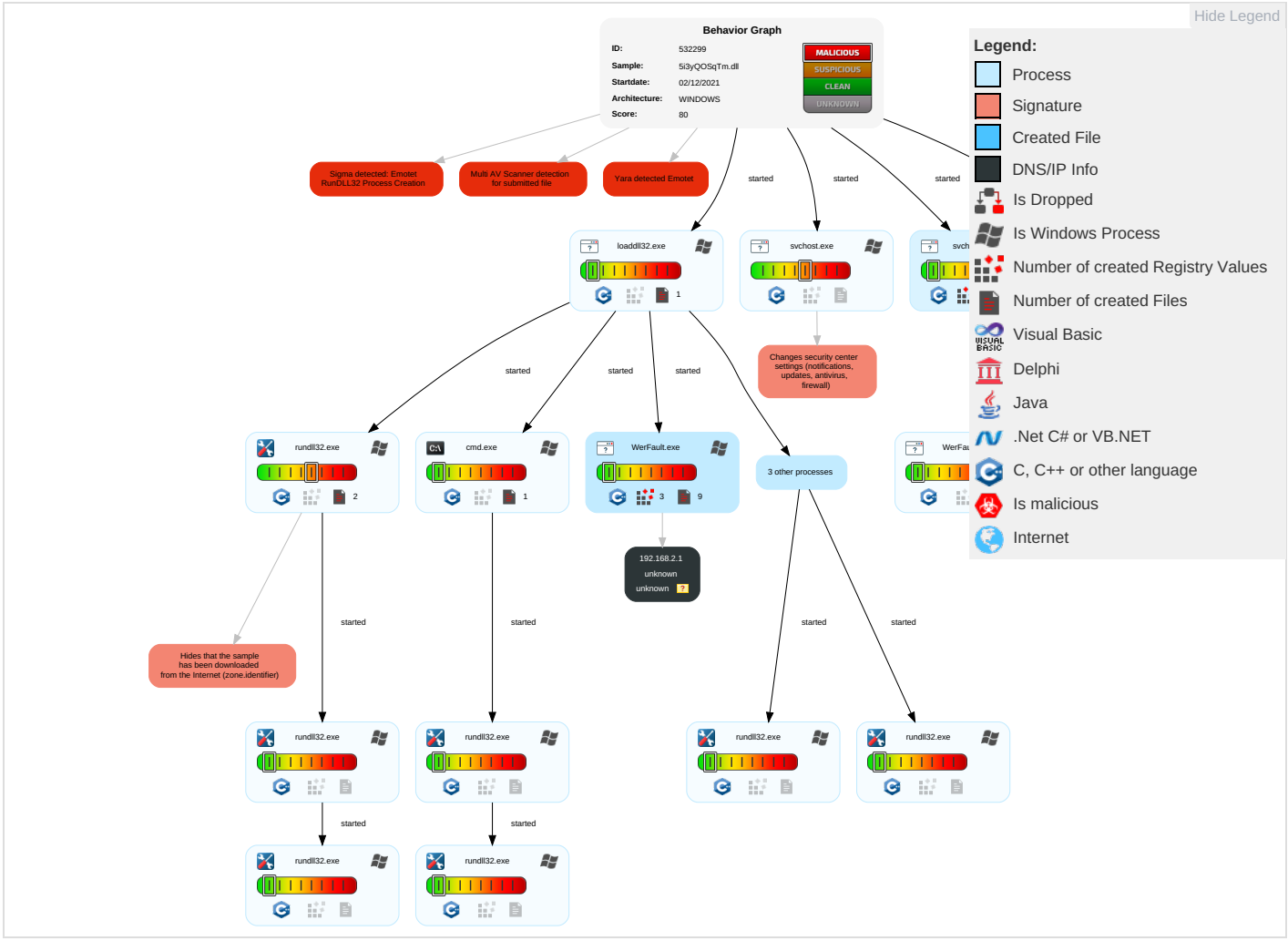
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 2	Masquerading 2 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Network Commu
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 5 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit S Redirect Calls/SM
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	Steganography	Exploit S Track De Location
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 Impersonation	SIM Car Swap
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	Manipul Device Commu
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 Communication	Jamming Denial o Service
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	Rogue W Access I
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 Protocol	Downgra Insecure Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base St

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
5i3yQOSqTm.dll	20%	Virustotal		Browse
5i3yQOSqTm.dll	18%	ReversingLabs	Win32.Infostealer.Convagent	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.b10000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.940000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.e70000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.4540000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.b10000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.b10000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.9e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.b10000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.46d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.b10000.0.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.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.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
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532299
Start date:	02.12.2021
Start time:	00:16:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5i3yQOSqTm.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:	33
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@43/26@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.1% (good quality ratio 24.2%) • Quality average: 72.4% • Quality standard deviation: 27.5%
HCA Information:	• Successful, ratio: 73% • 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

No simulations

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_187b1da8\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):	0.6754479704396386
Encrypted:	false
SSDEEP:	96:cX7tZqysy9hkoyt7JfapXIQcQ5c6A2cE2cw33+a+z+HbHgE2VG4rmMOyWZAXGngH:CvB1HnM28jjr9q/u7saS274ItW
MD5:	2AEE5E78EF26D162307A1F1E0ABBA548
SHA1:	2B758841F1E73ECDFAC5B7F9F91F81D57A2667D7

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_8c5962cbbdb13a8671f1f3c3793157e73bd5d897_d70d8aa6_187b1da8\Report.wer	
SHA-256:	1A130F4F2EF4420AE091604B05B2B4E3408CF1AA5909DC63495B094A56406495
SHA-512:	BDC4968FC52FA057CDDED8F9933313481F91FE10C1D2D17DDDC174B4AE8CF4422F2CE916892701D23F017C6935C5391C4BC37851EA4F6A0611E97F90BBB3BE4
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.=.1.3.2.8.2.9.0.6.7.9.1.7.2.1.6.9.4.2.....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.=.5.d.c.0.8.e.f.f.-.7.8.8.e.-.4.8.0.5.-.8.b.e.2.-.4.b.6.b.4.c.6.f.e.c.b.1.....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.=.3.0.6.f.0.9.3.7.-.e.e.7.e.-.4.4.a.2.-.a.8.3.7.-.1.5.6.4.5.3.6.8.f.c.1.a.....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.=.0.0.0.0.1.0.f.4.-.0.0.0.1.-.0.0.1.c.-.3.a.0.2.-.c.1.1.4.5.5.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.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_005759e6\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):	0.6791193075663844
Encrypted:	false
SSDEEP:	96:a2GCFz8dtZqyoy9hk1Dg3fWpXIQcQYc6ZcEKcw3u+a+z+HbHgE2VG4rmMOyWZAXR:agp8pBAHWdQAjr9q/u7saS274ItW
MD5:	8A4E68599049AF186936C4F0E82ABFCF
SHA1:	5CC56A10E379DB01F48D55FB5CBBC0E01975C69D
SHA-256:	0C97CF83364AF973017E966E9F35985D8F85532529E06201790B55C404ECE325
SHA-512:	73A221BD598B133EA781436FD7963485B6570BD7E9863EB73D82030C48E44317AF4A25C9AEE591649226D94E7D90C2F57673A8234DAEF9B0A5E4BD9CE22385AE
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.=.1.3.2.8.2.9.0.6.8.0.2.5.3.2.4.2.4.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.2.9.0.6.8.0.7.6.4.1.7.2.0.5.....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.=.7.3.f.b.d.2.a.7.-.b.7.f.3.-.4.3.5.3.-.8.2.7.0.-.a.d.a.0.6.8.a.a.7.c.3.b.....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.=.4.3.d.0.a.4.5.0.-.8.7.d.2.-.4.f.4.c.-.b.4.6.c.-.b.7.3.1.f.d.0.9.4.1.7.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.0.f.4.-.0.0.0.1.-.0.0.1.c.-.3.a.0.2.-.c.1.1.4.5.5.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.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\ReportQueue\AppHang_NcbService_c3fd3c3f830283a6ba0c7e839e220c16a1c8146_00000000_0785595f\Report.wer	
Process:	C:\Windows\System32\wermgr.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8231203080410965
Encrypted:	false
SSDEEP:	96:8Ydrw1MYSgGgkgOpXItJ+HbHgS3gePnMXh88WAfbNkqKjibkUDvLgWRN1mDjTcuI:brwStgY1jwHggN/u7s6S274lt
MD5:	EBD588E2B8A8F058E9FAA84704C0432A
SHA1:	2226A68A179C2E493958F76EFE20218CE0E1B390
SHA-256:	CD3344AC650DF1EA6E26B1AF3CD0E3068306A2F292FE22C3FD6B5C49687E7357
SHA-512:	205A317981953ACC3842D4C8C1492B0764EA9AC2217FEDAFB848EFB934A3426FEA2A207EECF6F4AE611E68002E8097D50BC400662B3BE718BE990B5C06B3C0FE
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.S.e.r.v.i.c.e.H.a.n.g.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.9.0.6.7.4.5.7.8.3.2.9.2.7.....R.e.p.o.r.t.T.y.p.e.=.3.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.8.1.3.5.6.2.a.-.5.a.9.a.-.4.7.d.5.-.a.d.a.a.-.d.5.5.3.6.8.6.f.4.2.0.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.0.4.-.0.0.0.0.-.0.0.1.c.-.e.3.c.f.-.8.5.1.5.5.5.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.6.6.0.b.7.6.b.6.f.b.8.0.2.4.1.7.d.5.1.3.a.d.c.9.6.7.c.5.c.a.f.7.7.f.c.2.b.a.c.6.!.s.v.c.h.o.s.t...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.5.6././.1.2././.1.2.:.0.8.:.2.8.:.3.4.!.1.7.e.f.9.!.s.v.c.h.o.s.t...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.I.d.=.4.0.4.....I.s.F.a.t.a.l.=.4.2.9.4.9.6.7.2.9.5.....R.e.s.p.o.n.s.e...t.y.p.e.=.4.....S.i.g.[.0.]...N.a.m.e.=.S.e.r.v.i.c.e.N.a.m.e.....S.i.g.[.0.]...V.a.l.u.e.=.N.c.b.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER10C7.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 08:19:52 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	26832
Entropy (8bit):	2.487781029339773
Encrypted:	false
SSDEEP:	192:tuewMH95S6OTNrKuC9FHBsqNfL8jWxytHbdb2mmriy2v:FP5SFTNuuvqNfL8aIHbdb2m/
MD5:	C142CF5441B5FD095938D19BFA67B29C
SHA1:	3226AEE79DA2177FEFCD20A9A712DFDBC09ACD43
SHA-256:	3AB114C2A8305EED101A1B215F6DEC3B0A0E33EF52938E075ECCF5D78CCBD43D
SHA-512:	6C5667C62E17E9264185E47646D9FCD8C936AEF9F6E5F9C6412C62255DFF6087A64E01847ABAD81F287B71FC8F38353A3E9C3140DB0ACFEF0E0348ED51569F2(
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER10C7.tmp.dmp	
Preview:	MDMP..... .....a.....4.....H.....$.....`.....8.....T.....h...h\.....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\WER11D8.tmp.xml	
Process:	C:\Windows\System32\wermgr.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4310
Entropy (8bit):	4.428102891708425
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtBI9nHWSC8B/s8fm8M4JFKfY2xAF8Lyq8veY2xVvhO8OTd:uITfJJ2SNVRJFKf/lWe/Vvk8OTd
MD5:	3768772510C55D2D721DCD8415F2E981
SHA1:	D8D82E31565ECD17DA1C16C5C6ED91760D472F0A
SHA-256:	62FD9372B0E6591C441A65D944DB2AEDC8D03960D88E660A5FEF5AEABAAD690C
SHA-512:	AAB7BFEDDD81A874F25E30C3725173C48CF9BA6DA64FA517B6B9FFA0E19FDF987987DC19670792A12C6CB285044769BC01D9F491F73BFF85BB65CC4452CA25D
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="1279769" />.. <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\WER14DF.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):	3.7009426535664662
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZf6eh6YFaSUGngmfsSzaCpBg89bkjN5sfL0vsm:RrlsNih6w6YYSUGngmfsSzdkjNSf6
MD5:	BD6D06D778585343D22E866C7E3CD76D
SHA1:	3E74E82462445437B6B1F8A1B3C5B00511AC258F
SHA-256:	B9375ACC1C8BEA51DD2CDAAEA1D784945163D6ABD3A0C51CDA774BB86238E1F8
SHA-512:	3DF19C390E692A5268F851A93A02F8CAA8A78B42993FD389EF1E5B79D812DAB22F97ED54AFE8BAD3CAA6B57BF3A69416CDAD5704E11C63DC2C24F3AEB476E191
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.3.4.0.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER167A.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51904
Entropy (8bit):	3.063864127660923
Encrypted:	false
SSDEEP:	768:CXHpHD1EnoZWM5yzDd5Gx47Iq5+CelaWikDIRP9JpmnH:CXHpHbD8zDd5Gx47Iq7elaWv0RPLpmnH
MD5:	77D811B50E4D1C8618A5D6333D89D833
SHA1:	1E36599108D5C49FCFCDE2EE2F18510F8F0B1908
SHA-256:	52199A0254D6DA0502DADBAC38073F872A5267D9EC41548AF342141E305895CC
SHA-512:	30FF6599C619C23392C17C13A97291A97C6FA2FFE508ABDFA27A45447A7B2CD3154A241CA330452C72CCA2DCFBDF6D2229556EE0E11FD6A64DEA6DE68F14605
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\WER17FD.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):	4.47213070071042
Encrypted:	false
SSDEEP:	48:cvIwSD8zsBJgtWI9nHWSC8Bu8fm8M4J2yzZFU+q84WvQFKcQIcQwQkd:uITfTw2SNdJJggQFKkwQkd
MD5:	A5D2DE991E9C4181F7D87E6BF34EAC8E
SHA1:	9AF1CFE85BBD332B0275D49AA6679936753A5693
SHA-256:	D6FB1783411A9C7BDA6E5F3B89EE8CF1ED276604E31D6C8223B5F69E71684554
SHA-512:	844E4CF6A237ECBB7E643F6AE214900823EE28D71F6C05FBB3E8299E6C0558C4155E938C41E95A3E3A1D1628648D3C29028F7A4BD6EBED0FCEDF16C8B154693
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="1279770" />.. <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\WER3AF4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 08:20:03 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1059828
Entropy (8bit):	1.3530089983506397
Encrypted:	false
SSDEEP:	1536:ZXFdb/P6k0tLmleDlPqwIXMena99UVLkJ/R9GuMDkUfaeF82c:p36k0tPDkTnO9UVLkJ59IkUfaeq2c
MD5:	B1F94BE55C0F42F0FF2A5F6C415429E2
SHA1:	169E355D35EBCBFD8EFD6BEF2C5862A228FA80E9
SHA-256:	97EC25DAF5EB2B1409BE0089BFFB84A97CB554E97383EC68A2D0AB91900A1124
SHA-512:	E9D35D52703FF5D7D38FCF0D82F2DB1725D916DFBB021A6A706D1537B0A0EE43B4754BC3F45BF2AD229FBB514144D075C33B37988D963D1C4228771C672993B
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\WER440D.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):	3.6937685783150376
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZA6Gd6YFgSUCpbHgmfL8GS4CpDi89bVjN5sfOnm:RrlsNie6s6YiSUCp7gmfLrSDVjNSfv
MD5:	8CF24AADB1EBEF2ECF8A54DE5292AE6A
SHA1:	F595A62079FDE24CFE7B887406F197797D16C579
SHA-256:	DD5BA2150BFA3633D0CEC4C22DCF9B16A2B89721C4EDD2527F4048205847AC20
SHA-512:	C22F29B1C543495BC05492FBD50C97F5CD0D310324EF07CCB7FA4A7C9BEABAC4AFFAA0B0EF1B00925593E4334DCAE01B1E966DF7F7591F6D2583EB817671F4C1
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.3.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER46BE.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):	4.4287797177293715
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER46BE.tmp.xml	
SSDEEP:	48:cvIwSD8zsBJgtWI9nHWSC8BC8fm8M4J2yGtFUoz0+q84tjMFKcQIcQwQkd:uITfTw2SNJJEUxMFKkwQkd
MD5:	E2F1593D590DD7D7233246C6B96BD3AA
SHA1:	B334DA2557D588DAD21FFB43D266B81FCFA21458
SHA-256:	99EBB65789E8E4CCB18E5ACDB6AD5470D866A736073E99213DE36CA6857E1C24
SHA-512:	26F986D3D7649BF152DC90D8D881C72426C597973897B0B0CC7575902959D275DD430D4549A9CB2928C8BA5B99620E22A17C138F803F0EE5442F9D2A0707E93A
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="1279770" />.. <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\WER5113.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6948692578008937
Encrypted:	false
SSDEEP:	96:9GiZYWV+y8TkUYiY5TWDH0YEZdiustk0i9OIfJw/dTA0a5AiB5QIA+23:9jZDV+flczcHa5AiB5np23
MD5:	F7C9BE7A47B6A71082ABBD44886C9A97
SHA1:	5D68824C3D0A78BBE40BBFB2F21B396BDDA4276E
SHA-256:	DBB6EBBFDBEF42D2C79A2C7C2712DA604823D4CFB92ACA804C0376731CA5F008
SHA-512:	37FF05D6A815EBC29409A90D8AC5E17E1CF375B85A36E19EE6CECEC149BB02B1400AE4B0B64F34208B6EDD632E6B846835E67C3C8D656D3A6F407A02A80ADC19
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\WERBEA3.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	52858
Entropy (8bit):	3.0647172817979955
Encrypted:	false
SSDEEP:	1536:pjHAfL68HDtn1xN7lqxkjyL0Nllq6LUAdBcb:pjHAfL68HDtn1xN7lqxkjyL0Niq6LUA6
MD5:	2296EEC040E24DE2405EEEB285C75D8A
SHA1:	ACD989DDB11DBDCBBA3F268A5D70039BA8968D92
SHA-256:	81805A10ACC2D67F498E0C0AF9620110689E2E48603F4BE48CB4B77BDD603B3C
SHA-512:	113C92F943A4A26D0B18223AB66A35D27FDAB807EB80E4F8A555D0FFD46110DED6AB3D39E47C888BE208FE9560FA51B0688F7A2CE9D193C7BA5C8FC4B16990I4
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\WERC22E.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6952272931168184
Encrypted:	false
SSDEEP:	96:9GiZYWVgn3eoeA/txYGYbWz0H7YEZSytk0iiO5fNw8QwNZaTnAneAIAp3:9jZDVgnxBxz7zaTnAneXAp3
MD5:	5591AF2B641FA11B50CFFFE0DE4BE472
SHA1:	40B75FAC1DDEB4E11772940F89A74C649177C273
SHA-256:	E12FB5AD22036B0CD38D72EB717B29D55C762EDBBAECA859717D701FA885B51C
SHA-512:	46AB30ED89B573B5FF385F591AE969004B8B906F7157F5ABFBFFE67C20FF10EC70FB7E09D8EF15C5CA9DE37867CA2B6BCBDB6DAE8FF06DB2AD028719047F4FAB

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC22E.tmp.txt	
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD33.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\System32\wermgr.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	4890
Entropy (8bit):	3.708335392466497
Encrypted:	false
SSDEEP:	96:RtlU6o7r3GLt3iMBj9XjDPYr74SfEGg0BCaMrZ4vm:Rrl7r3GLNiMBj9XPYr74STCp1Gm
MD5:	3915722ED951A0333D6C67A268A26E2B
SHA1:	4C2D32D9B8B8221D684F58DEF3EBE59F604E4837
SHA-256:	4A100A7D28DEF0B4A491111F502D4EFC8B32320FBAAB355174F8BA0B012574BF
SHA-512:	A2B24310BB7481FCFE698983A7087A7273076B6A487EFEE01C07C38E364BBABCE97D543557336165680A5B6AF0B6C7DF7F298698ACBA8BE9FED9EEC86ABF50D 3
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.4.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERED85.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	52488
Entropy (8bit):	3.0649859459697737
Encrypted:	false
SSDEEP:	1536:t/HTp9n6FyxtsaxN7IqSrJiyk0y9y/LVdxw:t/HTp9n6FyxtsaxN7IqSrJiyk0yA/LVU
MD5:	A8B96200EC520AF834608F1B814A6738
SHA1:	09AD85BF48A9B0DC4FAF29120DD48A2BAD28513A
SHA-256:	10E85ACF226EEBA554B709909874D841C9A5E84BD7D2117D2E9159CEC5973137
SHA-512:	9485F6B625D239A099A0F65191B3B2AA57A936415335DC23FF3C950BF4823A34E9C6A43461760AD3615436DEA08D347CFDD96946CEDA730CB0205B8B3FA1794D
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\WERF1DB.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.695644144475772
Encrypted:	false
SSDEEP:	96:9GiZYWVYI9IxQVYRzYoTWxHBYEZbotCigONfaw4qni0XakQtmTUIVl+l3:9jZDVYsSS54akQtmTDVUl3
MD5:	FDB1472D617482A4A58854E7DA268C2F
SHA1:	C64A71DE2CD2532A9E69C427CB32E109914FB3DD
SHA-256:	E12463D10E1AACEF100F458D67B307E61EEBFDF846CCC1A372016CB325122DFB
SHA-512:	1B82B04C6A9F7CD622AF326D3DD1B33579396A76C7D332F52D0153B14650025ECB92BD1FFEF0B08D9835B5113A39D67C43BD0FB9BEEBD57E203A5302AA7103C C
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):	0.10989502196543777
Encrypted:	false
SSDEEP:	12:26HjXm/Ey6q9995vq3qQ10nMCldimE8eawHjcof:266l68kLyMCldzE9BHjcI
MD5:	9A7463FA7D66CACD641F6DF3F1DEF198
SHA1:	83BD27E517A0BC26DDF16EB4DFBABE666147BBF6
SHA-256:	857B7E228D1417CB8450DEFEB211F9979A2788903FEFD70755724454C1021CAD
SHA-512:	2EB9E48CB47CF28C201B37AB2821550A9129F8C22E3235DA235FBE0C174579E18D4FD931ADEFA94D658060FD169E185CD5E48C17DFD1318E5C09100C0DD4E4A
Malicious:	false
Preview:	.....`.....7..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.....s..#~..... .....J..$U.....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.`.....g..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):	0.11241126566489497
Encrypted:	false
SSDEEP:	12:D/sjXm/Ey6q9995F1miM3qQ10nMCldimE8eawHza1miImP:D/Jl68v1tMLyMCldzE9BHza1tIm
MD5:	2FAF61572736CAEC65422E0233E7E1CA
SHA1:	243D9DDD93F2460606AB8F30A91B7C1C10E1ED6F
SHA-256:	7B10FE6044B8E71E7E1212752918657E5B7506938E03FF85E2F14B31EAB6852D
SHA-512:	A53C65E0F11053466763A06741B22412EB655BF26A9873FA57CAA5DA0A87B630D4ABBE5F1572E7487B9C4B10151DC20BEA00CAF7738E5E56CA32ACD70D7618EE
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.....s..#~..... .....{..$U.....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):	0.11234943753179523
Encrypted:	false
SSDEEP:	12:pjXm/Ey6q9995F1mK2P3qQ10nMCldimE8eawHza1mKoEP:El68v1iPLyMCldzE9BHza1/
MD5:	F8B7A841CDC339DBEF411695D08A049E
SHA1:	98058BC75A5BBB3BFED13D52696B45B8E9E432D3
SHA-256:	E978E51B32E584C41D72B5056454F03D79FC41F99728D2B805266570D59BA171
SHA-512:	A863159ED8D05D6C7373E010CF1F53A3598B7A858788DE91C0E08A4650AD79FA8842EA25E4B3EC4D01A4180DBA7BC23F17F3A91B08FC7049CCF7AB0DE7B7712
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.....s..#~..... .....{..$U.....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.`.....Y..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):	0.10989502196543777
Encrypted:	false

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001 (copy)	
SSDEEP:	12:26HjXm/Ey6q9995vq3qQ10nMCldimE8eawHjcof:266l68kLyMCldzE9BHjcI
MD5:	9A7463FA7D66CACD641F6DF3F1DEF198
SHA1:	83BD27E517A0BC26DDF16EB4DFBABE666147BBF6
SHA-256:	857B7E228D1417CB8450DEFEB211F9979A2788903FEFD70755724454C1021CAD
SHA-512:	2EB9E48CB47CF28C201B37AB2821550A9129F8C22E3235DA235FBE0C174579E18D4FD931ADEFA94D658060FD169E185CD5E48C17DFD1318E5C09100C0DD4E4A
Malicious:	false
Preview:	.....`.....7..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.....s..#~..... .....J..$U.....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.`.....g..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):	0.11241126566489497
Encrypted:	false
SSDEEP:	12:D/sjXm/Ey6q9995F1miM3qQ10nMCldimE8eawHza1miImP:D/Jl68v1tMLyMCldzE9BHza1tIm
MD5:	2FAF61572736CAEC65422E0233E7E1CA
SHA1:	243D9DDD93F2460606AB8F30A91B7C1C10E1ED6F
SHA-256:	7B10FE6044B8E71E7E1212752918657E5B7506938E03FF85E2F14B31EAB6852D
SHA-512:	A53C65E0F11053466763A06741B22412EB655BF26A9873FA57CAA5DA0A87B630D4ABBE5F1572E7487B9C4B10151DC20BEA00CAF7738E5E56CA32ACD70D7618EE
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.....s..#~..... .....{..$U.....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.0001Fa (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11234943753179523
Encrypted:	false
SSDEEP:	12:pjXm/Ey6q9995F1mK2P3qQ10nMCldimE8eawHza1mKoEP:El68v1iPLyMCldzE9BHza1/
MD5:	F8B7A841CDC339DBEF411695D08A049E
SHA1:	98058BC75A5BBB3BFED13D52696B45B8E9E432D3
SHA-256:	E978E51B32E584C41D72B5056454F03D79FC41F99728D2B805266570D59BA171
SHA-512:	A863159ED8D05D6C7373E010CF1F53A3598B7A858788DE91C0E08A4650AD79FA8842EA25E4B3EC4D01A4180DBA7BC23F17F3A91B08FC7049CCF7AB0DE7B7712
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.....s..#~..... .....{..$U.....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.`.....Y..F..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211202_081926_566.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.392411013136536
Encrypted:	false
SSDEEP:	96:0ClYZomo+ga5s+9ob/YMWCb/l2l2ikf/4u1T2IjFztNMCQ6JRcY5H:vinReNc2xqoCDf
MD5:	35326629B94BFF5EFA849C4406350B4B
SHA1:	9DA233CB6A8286DBF88BF47BB7D6285F30BD51EC
SHA-256:	1B339F2DEFCD9E6AD171084A72EC80546D89690485D305F02223C9DD9DBD8DE0
SHA-512:	37BE82619C80333FF821A8E61CB9667075BEE6944EBF148352E264A2D072E237B5F0BD6DF16B3E1DF8BFB2DC2107A4E579D8BBAC9C8BB3FE494F2AB0373BA858
Malicious:	false

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211202_081926_566.etl	
Preview:	....l.....d.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....I.RU.....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._.0.8.1.9.2.6._.5.6.6...e.t.l.....P.P.....d..... .....

C:\Windows\appcompat\Programs\Amcache.hve.tmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.8462688003400152
Encrypted:	false
SSDEEP:	24:JNuHVKJW1XUlE74AHslPoDdXw4ib3S82p0F+/uq:eHVKJW1XQEkAkYdAeT
MD5:	5339AB43691DF25CCD427698835019D2
SHA1:	DFBE02B060AB414AB9BB05ECF6C9C8C747D11684
SHA-256:	EB9B417EE8C3DE1245324EF335500CDB5853FCE285E5870CF7F711792D5C7EF9
SHA-512:	8F7D8C99FDA21D0241B745250CF349184AF8F848C9A5C56260C23A84A753067AFA47AFE61B21FC354069D83478D1FF2A1C6491004BF74CACCC74838BE214F853
Malicious:	false
Preview:	regf.....-`U..... .....C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...t.m.p...9..M.....-.9..M.....-.....:..M.....-.rmtm.y.`U..... ....N..... .....

C:\Windows\appcompat\Programs\Amcache.hve.tmp.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.8842972054145841
Encrypted:	false
SSDEEP:	24:BuHVKJW1XUl9CuO74AHslPoDdXw4ib3S82p0F+/uq:IHVKJW1XQLOkAkYdAeT
MD5:	E323EFAD3A271A1F157ED6C649AA8812
SHA1:	DEB76FC77B61F584A7489FAF103ADC758F3573B9
SHA-256:	5FE5C57E34487315469A6B6E54D7BA885E5E5C91F7A74683E12F28A2CF99FDFB
SHA-512:	7BEE939F8CCBCFFC2C1198EB901561272DECD1F6336284FDEEA9A8039341997C6A3E663D6D2D1A5C3B5A922509BCDF3989A185EF90EAB8DC6C7B86B61F1178 4
Malicious:	false
Preview:	regf.....-`U..... .....C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...t.m.p...9..M.....-.9..M.....-.....:..M.....-.rmtm.y.`U..... ....NHvLE....._..tF.2u$.j.....hbin.....-`U.....nk,..y.`U.....0.....&...{11517B7C-E79D-4e20-961B-75A8 11715ADD}.....sk.....(.....8.....1.?l.cL<.P...b....~z.....8.....1.?l.cL<.P...b....~z.....?..... .....?.....?..... ... .

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.067333612631272
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:	5i3yQOSqTm.dll
File size:	372736
MD5:	1e3db971ac31b856864c12b55bcc4435
SHA1:	8f47d8c2d75df496a20b5ddaec949f9524c60a66
SHA256:	df1aec18655ffd091bac7e217ad7334c30d99bd906ec926 9d0a38c5c92267fbd
SHA512:	66f9cf44cc85cba27c2194ae0803bd3914926763455a387 1b5c452720a5815bf04aba4753dde4ffa274e7abb98f259f ac24543201bcc74ce2485805ac9352c99

General

SSDEEP:	6144:qRsMh9YQWtcgA70wgF7nJyq6CQK+klVDRjudJMrt32fFcRmXIeJXjWMmAD:cvm9Y0HFLPRQKqV4epRmxAvAD
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	7.43224405131	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: 4340 Parent PID: 2976

General

Start time:	00:17:43
Start date:	02/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\5i3yQOSqTm.dll"
Imagebase:	0x1290000
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: 00000000.00000002.594385432.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.594385432.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.546111377.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.546111377.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.566017355.0000000000D7C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.566017355.0000000000D7C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.565844645.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.565844645.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.544809627.0000000000D7C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.544809627.0000000000D7C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.564089777.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.564089777.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.564150952.0000000000D7C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.564150952.0000000000D7C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.594452020.0000000000D7C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.594452020.0000000000D7C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.546379647.0000000000D7C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.546379647.0000000000D7C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.544682886.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.544682886.0000000000B10000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6140 Parent PID: 4340

General

Start time:	00:17:44
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\5i3yQOSqTm.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: 2220 Parent PID: 4340

General

Start time:	00:17:44
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\5i3yQOSqTm.dll,Control_RunDLL
Imagebase:	0xf10000
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: 00000002.00000002.539257826.00000000009E0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.539257826.00000000009E0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000003.513866249.0000000000BD5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000003.513866249.0000000000BD5000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5996 Parent PID: 6140

General

Start time:	00:17:44
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\5i3yQOSqTm.dll",#1
Imagebase:	0xf10000
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: 00000003.00000002.539875956.00000000046D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.539875956.00000000046D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.532223099.0000000000DBA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6148 Parent PID: 572

General

Start time:	00:17:45
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: svchost.exe PID: 6400 Parent PID: 572

General

Start time:	00:17:46
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: 4708 Parent PID: 4340

General

Start time:	00:17:48
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\5i3yQOSqTm.dll,ajkaibu
Imagebase:	0xf10000
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: 00000006.00000002.539444017.0000000000940000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.539444017.0000000000940000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.539407249.000000000081A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5724 Parent PID: 4340

General

Start time:	00:17:53
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\5i3yQOSqTm.dll,akyncbgollmj
Imagebase:	0xf10000
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: 00000007.00000002.544278858.000000000328A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.543487140.0000000000E70000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.543487140.0000000000E70000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wermgr.exe PID: 2016 Parent PID: 572

General

Start time:	00:19:05
Start date:	02/12/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\wermgr.exe" "-outproc" "0" "572" "2360" "2316" "2356" "0" "0" "2352" "0" "0" "0" "0" "0"
Imagebase:	0x7ff7f36b0000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 3428 Parent PID: 572

General

Start time:	00:19:06
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: 6320 Parent PID: 572

General

Start time:	00:19:09
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
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 7144 Parent PID: 572

General

Start time:	00:19:26
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

Analysis Process: rundll32.exe PID: 1308 Parent PID: 5996

General

Start time:	00:19:32
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\5i3yQOSqTm.dll",Control_RunDLL
Imagebase:	0xf10000
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: 4144 Parent PID: 2220

General

Start time:	00:19:36
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Pmleysyipg\sjdwpny.iso",qxtrVBTbrIKuSW
Imagebase:	0xf10000
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: 0000000E.00000002.661436675.0000000000C4A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.662192713.0000000004540000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.662192713.0000000004540000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 336 Parent PID: 4708

General

Start time:	00:19:40
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\5i3yQOSqTm.dll",Control_RunDLL
Imagebase:	0xf10000
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: SgrmBroker.exe PID: 5000 Parent PID: 572

General

Start time:	00:19:45
Start date:	02/12/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff612b70000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4908 Parent PID: 5724

General

Start time:	00:19:45
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\5i3yQOSqTm.dll",Control_RunDLL
Imagebase:	0xf10000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 3744 Parent PID: 6320

General

Start time:	00:19:47
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 504 -p 4340 -ip 4340
Imagebase:	0x280000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4840 Parent PID: 572

General

Start time:	00:19:48
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: WerFault.exe PID: 6640 Parent PID: 4340

General

Start time:	00:19:49
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4340 -s 308
Imagebase:	0x280000
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: 6096 Parent PID: 572

General

Start time:	00:19:50
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: 6704 Parent PID: 6320

General

Start time:	00:19:56
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 4340 -ip 4340
Imagebase:	0x280000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 1756 Parent PID: 572

General

Start time:	00:19:58
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: 476 Parent PID: 4340

General

Start time:	00:19:58
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4340 -s 316
Imagebase:	0x280000
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: 2960 Parent PID: 572

General

Start time:	00:20:22
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:	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: 3912 Parent PID: 572

General

Start time:	00:20:34
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: 4784 Parent PID: 4144

General

Start time:	00:20:41
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Pmleysyipg\sjdwpny.iso",Control_RunDLL
Imagebase:	0xf10000
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