ID: 532437
Sample Name: nhlHEF5IVY.dll
Cookbook: default.jbs
Time: 09:45:16
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

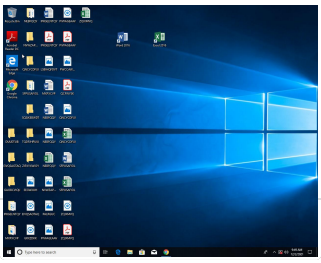
Windows Analysis Report nhlHEF5IVY.dll

Overview

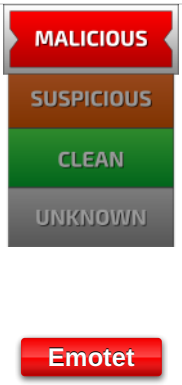
General Information

Sample Name:	nhlHEF5IVY.dll
Analysis ID:	532437
MD5:	222719bd9555a8..
SHA1:	b56136e6d14600..
SHA256:	81823e821dae4e..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

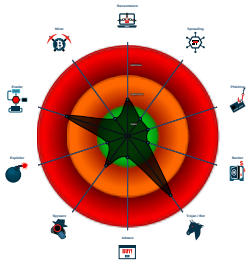


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Emotet
- Sigma detected: Emotet RunDLL32 ...
- Multi AV Scanner detection for subm...
- Hides that the sample has been dow...
- Uses 32bit PE files
- AV process strings found (often use...
- One or more processes crash
- Contains functionality to check if a d...
- Contains functionality to read the PEB
- Deletes files inside the Windows fold...
- Drops PE files to the windows direct...
- Uses code obfuscation techniques (...

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4612 cmdline: loaddll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 3792 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5228 cmdline: rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5104 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3112 cmdline: rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3080 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Rxalrmpxe\bkor.jtg",APfz MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5824 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Rxalrmpxe\bkor.jtg",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3000 cmdline: rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,ajkaibu MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3484 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4804 cmdline: rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,akyncbgollmj MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5356 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 3880 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4612 -s 304 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 2848 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4612 -s 336 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6032 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5916 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 472 -p 4612 -ip 4612 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1664 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 548 -p 4612 -ip 4612 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.970291608.00000000001C0000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000000.970291608.00000000001C0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000002.993619798.00000000005BB000.00000004.00000020.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.946676422.0000000000E30000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.946676422.0000000000E30000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.loaddll32.exe.1c0000.6.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.1c0000.6.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.5d3908.4.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.5d3908.4.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.32c2240.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 71 entries				

Sigma Overview

System Summary:

Sigma detected: Emotet RunDLL32 Process Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

E-Banking Fraud:

Yara detected Emotet

System Summary:

Hooking and other Techniques for Hiding and Protection:

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

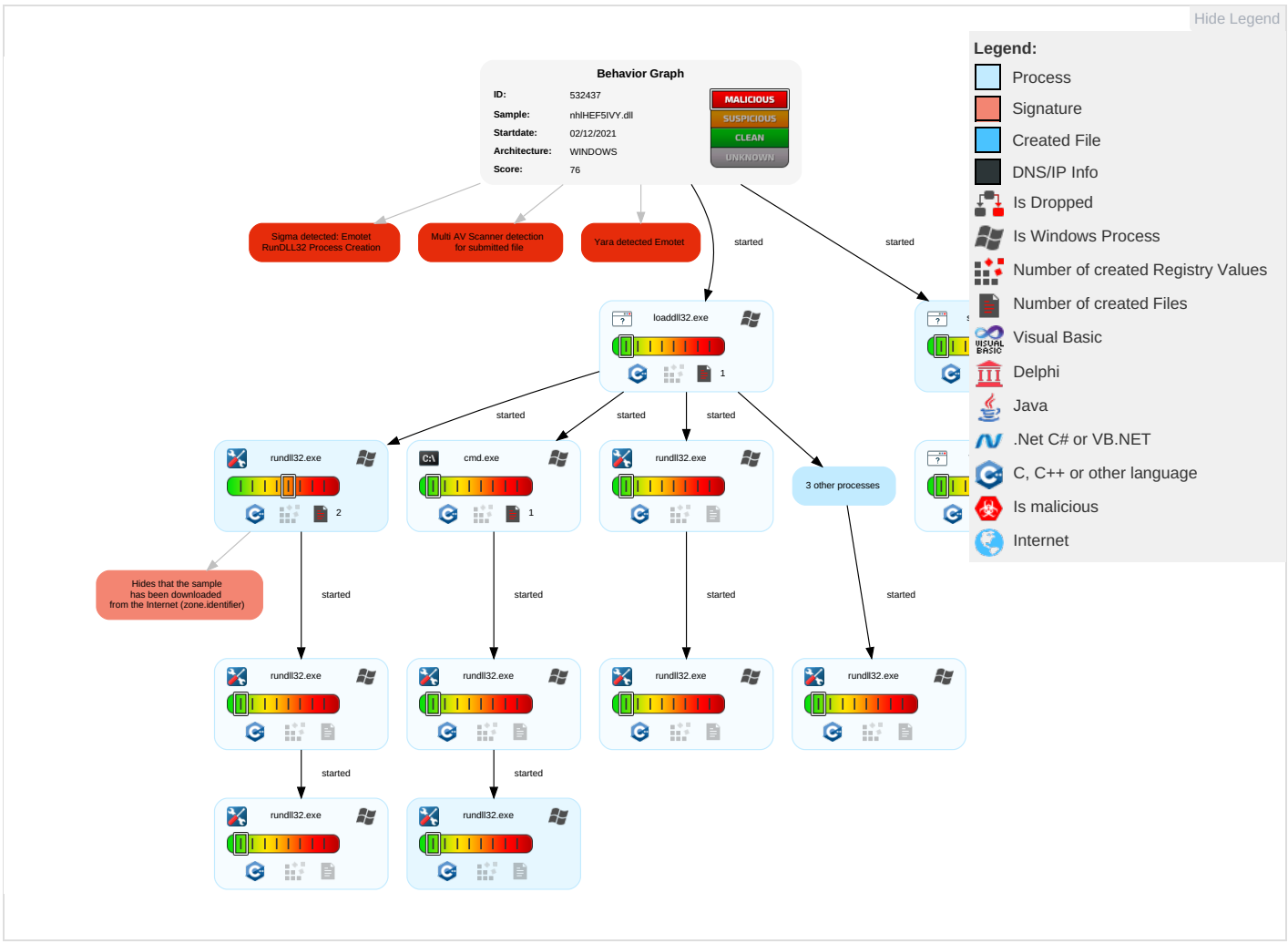
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 1 2	Masquerading 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 4 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

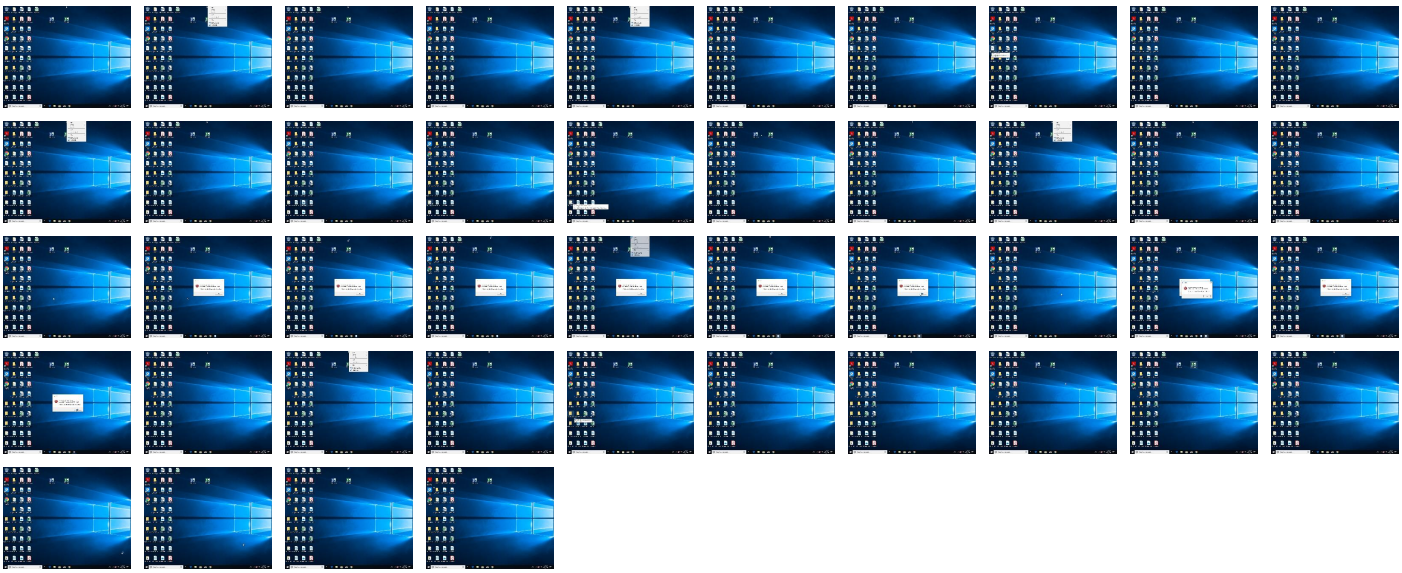
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
nhlHEF5IVY.dll	21%	Virustotal		Browse
nhlHEF5IVY.dll	18%	ReversingLabs	Win32.Trojan.Phonzy	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.loaddll32.exe.1c0000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.3400000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.1c0000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.8e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.e30000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.31a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.750000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.1c0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532437
Start date:	02.12.2021
Start time:	09:45:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nhlHEF5IVY.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:	16
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:	mal76.troj.evad.winDLL@32/14@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21% (good quality ratio 19.4%) • Quality average: 72.1% • Quality standard deviation: 27.5%
HCA Information:	• Successful, ratio: 70% • 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_88e9c9cb640b4f665f2020b110738337d7578_d70d8aa6_0e51d8a3\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):	0.6756145565292645
Encrypted:	false
SSDEEP:	96:02kzeRZqyUy9hkoyt7Jf0pXIQcQ5c6A2cE2cw33+a+z+HbHg0VG4rmMOyWZAXGn/:KCBDHnM28jjAq/u7szS274ltW
MD5:	7D72F4ABE55A3CF1934F6D538B8C2D86
SHA1:	D07087BD4AF3A72904384DF44EADEA44311991AE
SHA-256:	E78FAB3561446DCE38A125DCD8E916623245DD1BDF82AFB547FBF8896C410F10
SHA-512:	E26E509FB3D56DB5D83D6232AE74451605195FE55CE64678436DB53F51A90F83E4A4D0D7AE6F4FC618C71E84C145DB15AFF0439071C2824F602430B05EEE1467
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.=.1.3.2.8.2.9.0.8.5.1.6.6.6.7.4.8.6.3.....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.=.1.2.0.3.5.9.d.c.-.d.4.e.2.-.4.6.4.b.-.8.2.3.4.-.6.6.6.e.c.7.6.d.8.8.7.8.....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.d.b.c.d.8.b.7.-.f.f.2.e.-.4.7.1.d.-.9.3.7.3.-.6.b.a.f.5.9.6.6.d.6.a.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.0.4.-.0.0.0.1.-.0.0.1.b.-.2.2.d.b.-.0.d.1.6.5.9.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.8.:.1.1.:.5.3.:.0.5.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_c048235b2cbfcf49ff1eab6d2a64f8e0c646d63f_d70d8aa6_0a5a0f82\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

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_c048235b2cbfcf49ff1eab6d2a64f8e0c646d63f_d70d8aa6_0a5a0f82\Report.wer	
Entropy (8bit):	0.6822455764004985
Encrypted:	false
SSDEEP:	96:OvFyRieRZqyHy9hko47JAbpXIQcQfc6XOCecEccw3VF+a+z+HbHg0VG4rmMOyWZy:ModB2HROmTjAq/u7szS274ltWE
MD5:	964828FF6CE3A40D461A1AA086233179
SHA1:	767AA570C480EFC59C130DB76905A7EFDBB1FFFE
SHA-256:	A5DCE1E7509202FEED638DBBF2812B4A21817B2A7A413D7A30F61DC876C0CA55
SHA-512:	CE3DFFC6F8A60AE0C60C92A57A7565B0917CDBA8E7CDC72FAE3A96FA776611BD09666B8BC8B7FCE2E2B5DA80A0E5D373D5D59EC495C28E820B85161D7737FBC7
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.=.1.3.2.8.2.9.0.8.5.2.6.2.5.9.9.5.5.8.....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.=.1.3.2.8.2.9.0.8.5.3.2.3.5.3.7.2.0.2.....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.=.6.9.d.c.8.9.3.e.-.a.7.9.d.-.4.a.5.2.-.a.2.8.1.-.2.9.7.d.0.7.3.7.b.d.d.c.....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.a.e.7.5.2.4.9.-.f.4.8.2.-.4.d.5.0.-.8.8.c.8.-.f.4.2.f.1.3.1.f.1.d.9.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.=.0.0.0.0.1.2.0.4.-.0.0.0.1.-.0.0.1.b.-.2.2.d.b.-.0.d.1.6.5.9.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9086.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	48284
Entropy (8bit):	3.064575500594621
Encrypted:	false
SSDEEP:	768:faHAH2EE06gO/xN0Cc+fvx+o2kXN0Tt1UvCWKex:faHAH27z/xN0Cc+fZ+LkXN0TsvCw
MD5:	24DB966EEB0FC1CDAD34E833BC86926B
SHA1:	5A1F93E8E1BF7A7EEBFE42D60E9AA535F0427222
SHA-256:	DC67B0470D68EE39441441DFF45DC3188E7668BD9BDCEDF8E7D2220FD0F13261
SHA-512:	BD4E45874F8AB77602CB2A08DA9217DE5F74DEF1BD8C00B73DB3C273DF04EDEE51DE2F2B28ED5D90153B005DB74A05027311B06A3A4CAF9C4690817E05B094E
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\WER9411.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6947025218296834
Encrypted:	false
SSDEEP:	96:9GiZYWJiMCpY+YjWQf4Hv3YEZZ3t2i+qiDYwbwsDuaf+Nkit8yIrF7E3:9jZDaZKf0W/uaf+Nkit0xg3
MD5:	D7560271D5696DFF7E89E6D468B6566A
SHA1:	A176CE8E971A6B6F8FEFD4094FB014A1D3E40FBC
SHA-256:	6A69C27C6D833221AFDC1D68516B794DC20D7F0F32DC7F43F7C638B5E8DF20F8
SHA-512:	3C0F727637717489FCF8B812FBE8434814D91FE644818CE7778983C430D11FFEEF7A7DCFEFACFBE93E92DF652609EE4DD27BF2E879D3ABE62C13CE027885D7AA
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\WERBAB5.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	47916
Entropy (8bit):	3.0657592141709396
Encrypted:	false
SSDEEP:	768:zJH4H+q3EHAif/xA0CfRf1x+R2gXNsH9NvhBQ:zJH4H+qxk/xA0CfRfr+wgXNsdNvQ
MD5:	6665D9878FAF494911E6B7C62A58D2D7

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBAB5.tmp.csv	
SHA1:	1C01EA5588275E6120F02CB8D57FE7A861F3149C
SHA-256:	0EDD787812D978427BDAC58FB37EE3F9E5F0A123939834FA4506BA601F2F99EF
SHA-512:	AB04293F8C9C004785769819860150E8760FDB82000D0FCB82C1CB3FC9B448A6390C024978C6A44ED0CEE5ADAAC6CC44B2218EE2BD21BFF3AF46795D73B9A4 4
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\WERBE9E.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6943260976058023
Encrypted:	false
SSDEEP:	96:9GiZYWDlO34G+YAYTWQ5BfHv3YEZ6wt2irqsD1wkFHnaPDJB2aHIrC3:9jZDDdXakStaPDJB2aorC3
MD5:	F30AEAC73E31C150884479821895BC15
SHA1:	EEA9561078BCC7EA363674F656C41E4F3B07B649
SHA-256:	83647C24100343C5B10599031E032289A7D3446DF303F5A792396D9D0433548A
SHA-512:	CC6FC62F703A469A574A87DDA8AD9FF2E475185484E04631AF59381BF0DFD6A2296E738E9A9C8E5AB6ED2381B7AAB2A1218291DB3AA5596DA43C1B6DA10C5F 8
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\WERCD58.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 08:48:37 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	26720
Entropy (8bit):	2.4946307191848325
Encrypted:	false
SSDEEP:	192:OjP2djECpOcLy8kKfLvPe59JHtF2gKMKgESIWYQ0lwu:/dScLQKf7ePJHtFPKgESIWWd
MD5:	668299165E581DFB4EC56AF4DA29CC9A
SHA1:	9BC4E162C5CBFBA7F2B32A9A068801B6AD69DBC5
SHA-256:	8BBFDC90586F63AF686348E8F4253FB633BFF1B4719376B35D7CA2AC92AA3C35
SHA-512:	BD7E95E74D859B50D61BFDDE331841C0B26643FF24707583B22EE4D62019749071FB0D666B712CFF653E4FC844E00FE93BEA4836D1A4E37588699DEC33AFFC3
Malicious:	false
Preview:	MDMP..... .....e..a.....4.....H.....$.....`.....8.....T.....h....[.....U.....B.....p.... ...GenuineIntelW.....T.....a+.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e. .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD009.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):	8344
Entropy (8bit):	3.7012749138332923
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNij/616YrwSUAOS5gmfOSzC+pBO89bagsfiem:RrlsNi7616Y8SUAOS5gmfOSz7azfC
MD5:	9855971D4F8C6755C81CB40782196D2D
SHA1:	48B98CDE291834C7596C66B818023FA93BE6CD65
SHA-256:	A9A13C4F03943D81FE2068A2E68503982D0A8B0AD5FCC3FB6E0B284F3A7BD149
SHA-512:	A2DF6C7AB6DE0128939EF00E276A47E4A24A42D74C1346BC6B221D987432EC5FCF95C6114A50918AC5AD7C179D79820137E854909C28E33CA73A67416659B55
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD009.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.6.1.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD23C.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):	4.479031705373616
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUJgtWI9ZXVWSC8BaT8fm8M4J2yvZFy+q84WzAAKcQlcQwQjd:uITfS6XkSNRJBmw3KkwQjd
MD5:	B4A9DA433AC1D9E362A5DAD1943FE0D0
SHA1:	A5FA84A7B491F4F779C846441241683E7986F6C5
SHA-256:	095D6CC0CEDF6669C71FD8A4C722AE3776075F657E587FE6798C7E40B2891645
SHA-512:	ACBF62F688B398009A6D0ACD46C621FBA4BDD35BEA601E5561785662B88AC6CA9D5EAEF31351B4B997700697AA48652E94C32421DE14528ECEAED583778A0E0
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="1279799" />.. <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\WERF2D2.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 08:48:46 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1049284
Entropy (8bit):	1.3618305077272557
Encrypted:	false
SSDEEP:	6144:sZC+yOyIFsYRY5wv2idk9dIO9X4IfmF0Y:sZC+3yIFsYRY5wv2idk9dIO9X4Ifmf
MD5:	182EE711EFBB48A000D21A4025050EBA
SHA1:	F56E4490ED399160E4F462AC77833CD60E9D508D
SHA-256:	65D78BEF20AC7E6E685598076A3A2F0F16FC84F1CD2D525359824BFA8AD60D2B
SHA-512:	BA75A3F3575D3F97F3A81910B399A5FBDB42684A47B738C1023EB6C3D141017E03A6FF1EF1158835FFEF16D7AF094D61F4C8C07EA4F5E98BC4AE7E02F1B59AF
Malicious:	false
Preview:	MDMP..... .....n..a.....4.....H.....$.....`.....8.....T.....@.....U.....B.....p.... ...GenuineIntelW.....T.....a+.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e. .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA07.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):	8344
Entropy (8bit):	3.697976825375663
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNij86e6YrWSUaQMigmfMSr+pDE89b6gsfBrvem:RrlsNi46e6YaSUaQMigmfMSm6zfBT
MD5:	8FD8DB7F9A53E91CA59833375EFE8F0A
SHA1:	292DD396ADD6F4F9B2A932294BDA3BBEA729C6DD
SHA-256:	112BE52F4BA19CE115CD3B7A9DED401B89B60B1335C2F4CA8208A9A4D421B822
SHA-512:	6D843C1BD91F06744967550479F6F3791D317997CC0E0AB0BC0224A1EE62B0270262E5FC6BF7C4A06097B8FABACF1DBF4278A2EA598FF7D05F3EDBC7DC1854D
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.6.1.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC98.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):	4.471993005702466
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUJgtWI9ZXVWSC8BG8fm8M4J2yYSFs+q84tXTAKcQIcQwQjd:uITfS6XkSNlJKzBkKkwQjd
MD5:	29B3B0F36F70D8DCC36137B0E55629ED
SHA1:	36790ADAF12BB3533040208BB690B44DFBF4B565
SHA-256:	274E5FD94681AB1922D722D0CE3DFB8031667A71ADAE9108FB3A54221277F59E
SHA-512:	8CFF0507791544D2D10C805A866E312EBB8236C2FF8AE28B2311D960E9A5A27999F28B7580E7647A4E184E93EF789FF99FD84F488EF289A3019B29D25BDA727C
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="1279799" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\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):	4.239475479455116
Encrypted:	false
SSDEEP:	12288:WpTzoGkFsGCGs0BWF49FpiyRcoUlSDJrN/3Nih3JwAFBRZ66:kTzoGkFsGCx0BW+Lc
MD5:	5942A5349380C9C3CFAAFE1AB1AA7BF6
SHA1:	491E397ACAD84B01D2426760063F069A6297B40A
SHA-256:	D7D875CC7C0AD81C7119175FE75C9D5020633B565DA3D66463BAF70376C4DB1B
SHA-512:	096BE1DF130697E6DF60D63DB9252C85B606308422423A38EC1479416C9EA144817443DA7AA19F2ED483BE92566608D464D288C6687B3E40E1972D7E4748F9AD
Malicious:	false
Preview:	regfl...I...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.rmtmN..dY..... .....W.9..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.7210167206825284
Encrypted:	false
SSDEEP:	384:IM85K5ycv4KgnVVeeDzeh1NKZtjZT8GRFw5nZ:/KKpg/eeDzezNYtjeGRFw5
MD5:	88C16E7CDB64AF7249CD901E896336CD
SHA1:	D765FD096A3F68B62960E7ACC226D37B33EB386B
SHA-256:	F1AA2A23F3D3AD22B309C19A41AEA2602508D2DF0FC03E6C55BFA24B5E152807
SHA-512:	4F203C32CB0E6249BEE2D8E077349F88DA9004E52901DB00D1D28BB06174DE2C07C2E343A07CC1CCA6E6BA414F114ADDD3AB132A63FBC4E51798EC8700BF8(15
Malicious:	false
Preview:	regfH...H...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmN..dY..... .....Q.9HvLE.>.....H.....-.x..8.....hbin.....p.\..,.....nk,.N..dY..... ....&...{ad79c032-a2ea-f756-e377-72 fb9332c3ae}.....nk .N..dY..... ....Z.....Root.....lf.....Root....nk .N..dY..... .....*.....DeviceCensus..... ..vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.0673340607178154

General

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:	nhlHEF5IVY.dll
File size:	372736
MD5:	222719bd9555a8f48428737ab34a6fa6
SHA1:	b56136e6d1460055917dcb74ed849c59b35300c0
SHA256:	81823e821dae4e623a5f11ccbed6e628443301afd92c0ab 25e19d847927f5318
SHA512:	170c8e8ab85e18b97c6fe31d9ffb811fe2b67f92ca843d68 4ecaef75d3454bcf9584035746015305955e7f1b51281c8 dcf1b5476c1c55244c8205dfdf4d0dd82
SSDEEP:	6144:qRsMh9YQWtcgA70wgF7nJy46CQK+klVDRjudJ Mrt32fFcRmXIeJXjWMmAD:cvm9Y0HFLNRQKqV4epR mxAvAD
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....0...Q... Q...Q..E#...Q..E#...Q..E#...Q../$...Q...$...Q...$...Q...$...Q. .E#...Q...Q...Q...Q...Q../$...Q../$...Q..Rich.Q.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	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	7.43226452981	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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: 4612 Parent PID: 5256

General

Start time:	09:46:23
Start date:	02/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.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: 00000000.00000000.970291608.00000000001C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.970291608.00000000001C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.993619798.00000000005BB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.948659088.00000000005BB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.969710134.00000000001C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.969710134.00000000001C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.946894712.00000000005BB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.948115797.00000000001C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.948115797.00000000001C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.969859357.00000000005BB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.970456137.00000000005BB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.993327606.00000000001C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.993327606.00000000001C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.946627209.00000000001C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.946627209.00000000001C0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 3792 Parent PID: 4612

General

Start time:	09:46:24
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\nhlHEF5IVY.dll",#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 3112 Parent PID: 4612

General

Start time:	09:46:24
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,Control_RunDLL
Imagebase:	0x10b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000003.899666067.0000000000B2B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000003.899666067.0000000000B2B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.933922652.00000000008E0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.933922652.00000000008E0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5228 Parent PID: 3792

General

Start time:	09:46:24
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",#1
Imagebase:	0x10b0000
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: 00000003.00000002.930138580.0000000000750000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.930138580.0000000000750000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.936268035.000000000092A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 3000 Parent PID: 4612

General

Start time:	09:46:28
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,ajkaibu
Imagebase:	0x10b0000
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: 00000004.00000002.946359714.00000000031A0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.946359714.00000000031A0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.946802756.000000000371A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4804 Parent PID: 4612

General

Start time:	09:46:35
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nhlHEF5lVY.dll,akyncbgollmj
Imagebase:	0x10b0000
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: 00000005.00000002.946676422.0000000000E30000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.946676422.0000000000E30000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.947178520.00000000032AA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 3080 Parent PID: 3112

General

Start time:	09:48:12
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Rxalrmpxe\bkor.jtg",APfz
Imagebase:	0x10b0000
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: 00000006.00000002.1048939362.000000000373A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000002.1048437033.0000000003400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.1048437033.0000000003400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5104 Parent PID: 5228

General

Start time:	09:48:14
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\nhlHEF5IVY.dll",Control_RunDLL
Imagebase:	0x10b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 3484 Parent PID: 3000

General

Start time:	09:48:25
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\nhlHEF5IVY.dll",Control_RunDLL
Imagebase:	0x10b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5356 Parent PID: 4804

General

Start time:	09:48:31
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\nhlHEF5IVY.dll",Control_RunDLL
Imagebase:	0x10b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6032 Parent PID: 568

General

Start time:	09:48:32
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 5916 Parent PID: 6032

General

Start time:	09:48:32
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 472 -p 4612 -ip 4612
Imagebase:	0x1350000
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: 3880 Parent PID: 4612

General

Start time:	09:48:34
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4612 -s 304
Imagebase:	0x1350000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: WerFault.exe PID: 1664 Parent PID: 6032

General

Start time:	09:48:43
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 4612 -ip 4612
Imagebase:	0x1350000
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: 2848 Parent PID: 4612

General

Start time:	09:48:44
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4612 -s 336
Imagebase:	0x1350000
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: rundll32.exe PID: 5824 Parent PID: 3080

General

Start time:	09:49:16
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Rxalrmpxe\bkor.jtg",Control_RunDLL
Imagebase:	0x10b0000
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