



ID: 444650
Sample Name: 570000.dll
Cookbook: default.jbs
Time: 14:25:37
Date: 06/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 570000.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 5
Memory Dumps 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
E-Banking Fraud: 6
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 15
Rich Headers 15
Data Directories 15
Sections 15
Imports 15
Network Behavior 15
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: loaddll32.exe PID: 5428 Parent PID: 5624 16
General 16
File Activities 16
Analysis Process: cmd.exe PID: 4396 Parent PID: 5428 16
General 16
File Activities 16
Analysis Process: rundll32.exe PID: 5400 Parent PID: 5428 16
General 16
File Activities 17
Analysis Process: rundll32.exe PID: 5372 Parent PID: 4396 17
General 17
File Activities 17
Analysis Process: WerFault.exe PID: 6048 Parent PID: 5400 17
General 17
File Activities 17
File Created 17

Copyright Joe Security LLC 2021

File Deleted 17
File Written 18
Registry Activities 18
Key Created 18
Key Value Created 18
Analysis Process: WerFault.exe PID: 3276 Parent PID: 5372 18
General 18
File Activities 18
File Created 18
File Deleted 18
File Written 18
Registry Activities 18
Key Created 18
Key Value Modified 18
Analysis Process: WerFault.exe PID: 4036 Parent PID: 5428 18
General 18
File Activities 18
File Created 19
File Deleted 19
File Written 19
Registry Activities 19
Key Created 19
Key Value Modified 19
Disassembly 19
Code Analysis 19

Copyright Joe Security LLC 2021

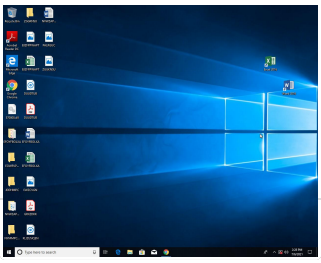
Windows Analysis Report 570000.dll

Overview

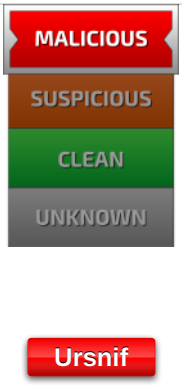
General Information

Sample Name:	570000.dll
Analysis ID:	444650
MD5:	6577b858178214..
SHA1:	c6420b09963f9cc..
SHA256:	0314e12bc1cb1e..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection



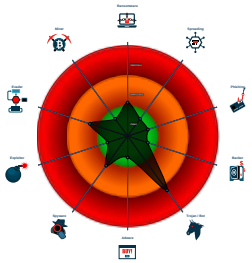
Ursnif

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Yara detected Ursnif
- Machine Learning detection for samp…
- Checks if the current process is bein…
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- One or more processes crash
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5428 cmdline: loaddll32.exe 'C:\Users\user\Desktop\570000.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4396 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\570000.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5372 cmdline: rundll32.exe 'C:\Users\user\Desktop\570000.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 3276 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5372 -s 644 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5400 cmdline: rundll32.exe C:\Users\user\Desktop\570000.dll,#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6048 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5400 -s 640 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4036 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5428 -s 272 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Ursnif

Copyright Joe Security LLC 2021

```
{
  "RSA Public Key":
"uiTXezezuapGKYR5Hmb7kdSK6au8TKB7wW9g5rwW5i1COxT1S+zuTy9YoTvI7hEm3kZdxYsJDG0+aStAKO8pzy41ZgWbaYpVgP+XSgAT7qWoXdAS/gVbMTJCCqNHkAtniUmHicelSYpHYminzht/W5i+89jC9sbo8vwV/qG0cnCdraqU
qpCPQT4N25ybpFXm",
  "c2_domain": [
    "cdp.geotrust.com",
    "217.12.221.28",
    "195.123.247.51",
    "195.123.213.89",
    "qpwoeirutyzmxncbp2.xyz",
    "pqowieurytalskdjp2.xyz",
    "wopqrituysakldfap2.xyz"
  ],
  "dns_server": [
    "107.174.86.134",
    "107.175.127.22"
  ],
  "DGA_count": "10",
  "ip_check_url": [
    "api.wipmania.com",
    "ipinfo.io/ip"
  ],
  "server": "12",
  "serpent_key": "10291029JSRABBIT",
  "sleep_time": "1",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "120",
  "time_value": "120",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "120",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "120",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "120",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "5456",
  "capture_window_title?(CRC_KEYLOGLIST)": "",
  "SetWaitableTimer_value": "60"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.231677722.00000000048B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000002.251665430.00000000017D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000000.236700469.00000000017D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000000.232967522.00000000048B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000000.237506792.00000000017D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 7 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Found malware configuration

Copyright Joe Security LLC 2021

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

E-Banking Fraud:



Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection:



Yara detected Ursnif

Stealing of Sensitive Information:



Yara detected Ursnif

Remote Access Functionality:

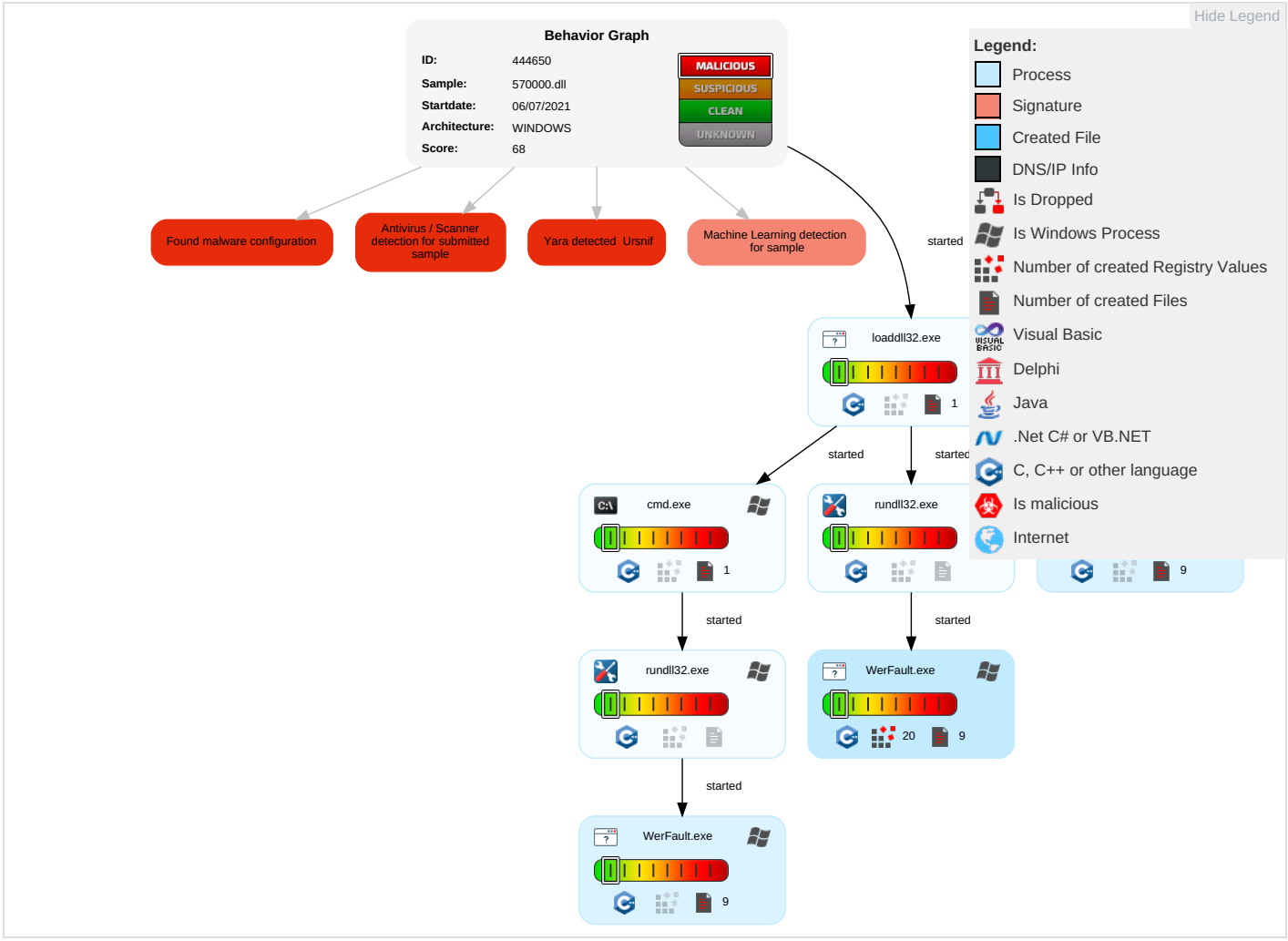


Yara detected Ursnif

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	Path Interception	Process Injection 1 2	Virtualization/Sandbox Evasion 1	Input Capture 1	Security Software Discovery 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rundll32 1	LSASS Memory	Virtualization/Sandbox Evasion 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	Process Discovery 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)	Binary Padding	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

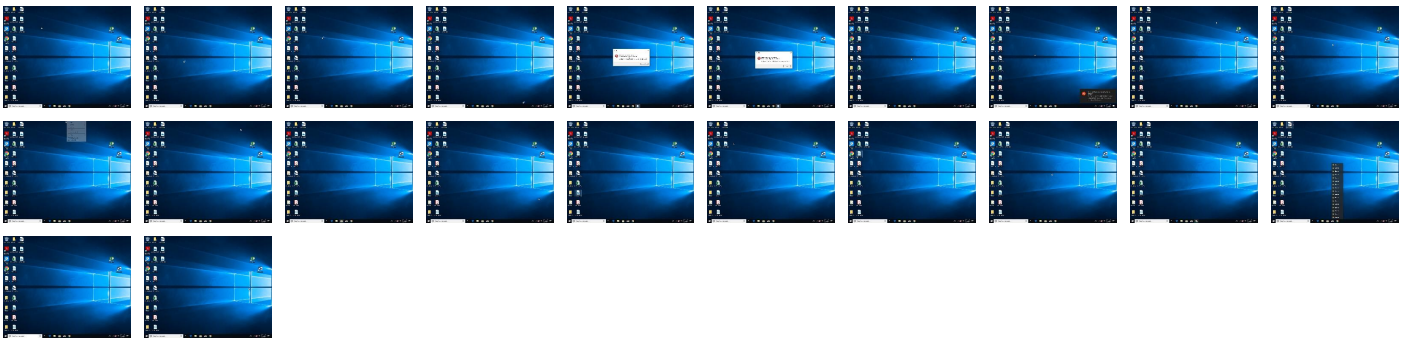
Behavior Graph



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
570000.dll	100%	Avira	HEUR/AGEN.1129335	
570000.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.loaddll32.exe.570000.0.unpack	100%	Avira	HEUR/AGEN.1129335		Download File
4.0.rundll32.exe.570000.2.unpack	100%	Avira	HEUR/AGEN.1129335		Download File
5.0.rundll32.exe.4280000.1.unpack	100%	Avira	HEUR/AGEN.1129335		Download File
1.0.loaddll32.exe.570000.1.unpack	100%	Avira	HEUR/AGEN.1129335		Download File
4.0.rundll32.exe.570000.0.unpack	100%	Avira	HEUR/AGEN.1129335		Download File
5.0.rundll32.exe.4280000.3.unpack	100%	Avira	HEUR/AGEN.1129335		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2021

URLs

Source	Detection	Scanner	Label	Link
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	444650
Start date:	06.07.2021
Start time:	14:25:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	570000.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
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:	mal68.troj.winDLL@10/12@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • 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_b9c034d6e73140d94d9c5167efb89cacf8f015e_160cf2be_0f231808\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7432
Entropy (8bit):	3.750752303561917
Encrypted:	false
SSDEEP:	96:hjkl4Xyuy9hAol7Rm6tpXIQcQSc6mcE4cw3U+a+z+HbHgGZAXGng5FMTPSkvPkpG:lk9DHsiiejl/u7sSS274Itb2i
MD5:	A9181BA09A7819806524C46D923422F2
SHA1:	3F1DC5F60334059FF52E47BD53A22BE08594EF98
SHA-256:	721A98C7ECF91F0129F360AE0EF489870E1A9991395E08507BFCAF928691B89E
SHA-512:	AFD48A95E60C51BAD2BC6C8F7499AB8467DCED9E61EA70CFE83C98104CCECF2CAB22B25CD4B77B11804F4852A3F7C7CFDD8C10BF9E2EBC5B08F00E4E9B69CD89
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.0.0.8.0.3.9.3.8.0.4.8.5.4.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.b.8.d.0.5.1.2.-.4.b.2.1.-.4.5.d.f.-.8.d.0.7.-.8.b.c.1.d.4.0.d.f.7.7.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.=.6.6.0.5.8.3.6.6.-.1.4.2.a.-.4.f.f.9.-.9.a.a.8.-.b.0.c.5.6.e.c.e.c.0.5.6.....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.=.0.0.0.0.1.5.3.4.-.0.0.0.1.-.0.0.1.6.-.b.9.f.c.-.b.a.9.3.a.d.7.2.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././.0.4././.0.4.:.1.0.:.5.0.:.5.4.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3793dfb461ce22140462de4a1a2617bff1862a_82810a17_174714fb\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11068

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3793dfb461ce22140462de4a1a2617bff1862a_82810a17_174714fb\Report.wer	
Entropy (8bit):	3.765165349786157
Encrypted:	false
SSDEEP:	192:b9iV0oX3HKvgsv5yjed+M/u7sSS274It7ca:b9i7XXKvgsv5yjep/u7sSX4It7ca
MD5:	CBA19611DD7605DC5C05AF5A042DD74E
SHA1:	67FB87F054B9DC2EC834F4488BFB93FC6B50FBEE
SHA-256:	8872EE0A9142C5E60F93C6A760D73AA6DB95CA4B68C4CBEF600555E6573669B3
SHA-512:	9AC870E476D142F2CF3ADE8876B745C9CF3F05E3A5EBE04616A53BBF61CC622DA66770FD3BC9B5C58885D3D1F632A3CCC45BC5112484D01677B9210FB03788
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.0.0.8.0.3.9.2.2.1.1.1.0.9.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.5.8.5.d.9.0.8.-.7.5.b.3.-.4.9.e.4.-.a.f.3.a.-.5.d.f.0.d.6.e.e.a.d.6.8.....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.=.3.0.4.c.a.5.6.1.-.d.4.1.0.-.4.5.7.9.-.8.8.2.b.-.d.5.c.9.b.a.0.c.8.8.c.1.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.1.8.-.0.0.0.1.-.0.0.1.6.-.5.a.4.7.-.4.5.9.4.a.d.7.2.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.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.u.n.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.8.6././.0.1././.3.0.:.1.1.:.4.2.:.4.4.!.1.0.3.d.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_441129e8c7f959a6d52d59f5a8a654c6d5f532_82810a17_0c2b1bb2\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11104
Entropy (8bit):	3.769527911879011
Encrypted:	false
SSDEEP:	192:Ji00oX4HKvgsv5yjed+M/u7sSS274It7c3:JiCXgKvgsv5yjep/u7sSX4It7c3
MD5:	52A18BC61C2979E6ED08AA05BBF6C72B
SHA1:	7EBD7B8C64422567B1B38C6A167DBA7766388B2A
SHA-256:	6D86491928C93FD2FA14778F05A51CC60CE9EAA15F764A8E2B22440BB51FF1B7
SHA-512:	E1D8AA9CB7D17C894A56D7ECA3A7EC6E11E372AA8388CED82F808C6D53DF59890BDF418E1D2D01DFFD6908F19F5C10C69335CC1371E2B084CEE5484F5BF6FA7
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.0.0.8.0.3.9.3.4.2.6.7.3.1.8.....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.=.9.c.e.e.d.6.a.0.-.0.1.7.f.-.4.b.c.2.-.8.1.1.c.-.a.1.c.2.2.4.8.5.7.6.2.0.....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.4.5.6.4.d.4.8.-.d.b.9.a.-.4.b.9.c.-.8.e.9.3.-.6.7.d.1.2.6.d.5.8.5.f.0.....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.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.f.c.-.0.0.0.1.-.0.0.1.6.-.8.1.b.e.-.4.8.9.4.a.d.7.2.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.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.u.n.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.8.6././.0.1././.3.0.:.1.1.:.4.2.:.4.4.!.1.0.3.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER10C7.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4735
Entropy (8bit):	4.451422638619334
Encrypted:	false
SSDEEP:	48:cvIwSD8zsFJgtWI9pprWSC8Bj8fm8M4JCdsInFxZ+q8vjsIR4SrSFd:uITffeESNyJCFK5RDWFd
MD5:	C16061F58AE005018CD213661408345B
SHA1:	6047398DE37F13975F155F9437F1BB686A953A24
SHA-256:	6A78023DA4A0F006D6BF31110A340B6943FD2304377BD34E8DDAA2E510517428
SHA-512:	BCA8AA8D25C0FE2F6CCC0006B9621F564B8955F9CA849660DBC56F3EAFD12432622DB4A64D8D02579DB811B19634F1631E86421205BF44054FC79BCCEBAEA24
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="1065997" />.. <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\WER10E5.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):	8388
Entropy (8bit):	3.693736111663003

C:\ProgramData\Microsoft\Windows\WER\Temp\WER10E5.tmp.WERInternalMetadata.xml	
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipp63tP6YIHSUpU+cgmfqSECpBv89bSEsf/Gm:RrlsNin6V6YISUm+cgmfqS+S3fX
MD5:	07D72089FD9510558559207ED2DA2FDA
SHA1:	F5FEEEF8961D43186F4DED260E11D3EEF47A70AD
SHA-256:	37BFE66B11DE15B84650C69F48B296CF18AE268DF731796164B114498E7D2FDC
SHA-512:	F64DF7528791043C6A476D8D5998A8D43219CC5858A4E3A2F4E5F3210F0C6D5B4DF034481E0DD962E664D853EBDED39A98CBD0DBA81194564877531743E5D44
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.>.5.4.2.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER13D4.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4699
Entropy (8bit):	4.4536420043951646
Encrypted:	false
SSDEEP:	48:cvIwSD8zsFJgtWI9pprWSC8BT8fm8M4JVqMFyn+q8v7qwKcQlcQw6UrBd:uITffeESN+JIrnK2wKkw68Bd
MD5:	6272BEA01D2125410BFD76ECDCE94A48
SHA1:	3AD2F347CD2DF3BCC2A4F0F38D76B406324A9A0B
SHA-256:	82A0AF0AC2A4671CA9D400AC2F7447B2F5B1F1E040A9029308D77AD97940DF67
SHA-512:	E5067DEE2D86061EADF2A00A234892742352B050A39F74194E60F57C1B6436DDE3E941D5304E80C20C0904A0D3E57D465DACE6B534145ED09A917CCEB118560
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="1065997" />.. <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\WER1402.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):	8362
Entropy (8bit):	3.6909913993731576
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi246j6YbXU6Ggmf8ESJgCpBs89bbwsf3Jm:RrlsNiJ6j6YbE6Ggmf8ESJDbDf0
MD5:	5CEAB6E4BDCB4314E98EB5394F36F160
SHA1:	5B96A49D214B7511F8CDB4F41077B4716F4B271A
SHA-256:	A6629917AA8D7D3D7D4719FFEB06BD224E12326931F21D9633BE0443C98A1B91
SHA-512:	02C4EF7DFF002916AC2DCC2077669E9FCDE21D2AD3C53F6EE0ADA5C879CCBA7568D60C0F4223DC978770361A2AE14292AB8128E6E4E5565FE786E6CE6D2D7FC
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.>.5.3.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1720.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.482166845224432
Encrypted:	false
SSDEEP:	48:cvIwSD8zsFJgtWI9pprWSC8Bm8fm8M4JCdskMFP+q8vjskX4SrSyd:uITffeESNtJ2+KJXDWyd
MD5:	E782277AB38BC5E6B711463C97748C33
SHA1:	17522802454586FF55AECA11F38F20FE25B88F12
SHA-256:	638D1F8F9A8AC69FC2B11E2472CE0D9728F65DEE013FB44159013104BE274C78

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1720.tmp.xml	
SHA-512:	ED65198D28EAEB9F7C4BEEC63F23CB8F42BA6340A191C31A3BD43C678ED92D252B40B39989977D2649B5F14E17CE9881020C296E42ABBD97E3FC056A511209C 5
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="1065997" />.. <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\WER888.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Jul 6 21:26:33 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	37500
Entropy (8bit):	2.3326554532891626
Encrypted:	false
SSDEEP:	192:yXp26IPl96D6YAs5vTTCiTAIUR5hL4IfLZoXGnUNq:RI/AsZqNX5hL48ZoWUc
MD5:	4FCAFBAC0DA75B0581A217CA5A1399DB
SHA1:	EFA1BF2F084E745FC8301F7B8AF7AA18DEA98FA7
SHA-256:	83F69794D20CFE5BD73CB6726A7DAF64B5FDA8E332464E58CDA296EC79E4835B
SHA-512:	6DD5AD56004DC3E4C3B8CE6068FF3A7A15D9D5951A0955C6D195732F5BEDD6703E055C67E0FB15FDDEE903DB1B9DB03A6B3C7B8F717B642F076498857175B7 5
Malicious:	false
Preview:	MDMP..... .....`.....U.....B.....@.....GenuineIntelW.....T.....`.....0..1.....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..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Jul 6 21:26:35 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	37488
Entropy (8bit):	2.2692876743516033
Encrypted:	false
SSDEEP:	192:3tu7i7Da7mnrsjcCfX5CiTAIUR5hDO4rxxUpOhnev:d97uArB0X0NX5hDOQxxUpAs
MD5:	B180252C60E4AB7DB01C11CCF13A8695
SHA1:	CFDC9B06D38A1067FA490FDBB646F000FF5F83B5
SHA-256:	32FFBE0E9902A8BD0637085ECFCA6CFB686F306E791BBA20570C2C48211C17ED
SHA-512:	BA6B72583006DC7A498FE0EC9CAF5D76637D0EDDF704E68CF6DE8273A5AD57303B5E2765644F271A554E367DB926CDFD0702CF301DF20D942EEDBF15585658
Malicious:	false
Preview:	MDMP..... .....`.....U.....B.....@.....GenuineIntelW.....T.....`.....0..1.....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..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE65.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):	8338
Entropy (8bit):	3.687237742408262
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi8K6746YpB6XlPgmf8HhSJgCpB089bSDsfdGm:RrlsNih6k6Y/6Ngmf8HhSJrSofF
MD5:	C3EB18DF92409A94C4882AB2BF7EA133
SHA1:	90940CE887CCD6F53849BAE6B3323EE15DE0EC44
SHA-256:	39601900722626DA80F7709E9572BE104CCB0D6F6ED0FE8BB580E35BF64C955E
SHA-512:	824140B103FA6777523F7964ABA5CF4935485F153AF9A953C07252CD98415302F04F30F4B152448377DB0B67BC9BD08877D03792522BD7A849E09230D280B059
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE65.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.>.5.4.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Jul 6 21:26:34 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	21880
Entropy (8bit):	2.278955504813094
Encrypted:	false
SSDEEP:	192:rYXrl3hQetweBP1hsX3EGLFTuKkfklaKx9mUwL1:+BhQetnXhsXbrZx9mU4
MD5:	FFA8A447B5F3ADC2289D07E1C2963DF8
SHA1:	22463D911D05D392719A9990B8556EACA5936A34
SHA-256:	07DDDDE86711110B1B8F227B3B1CFEFA4843491317020714DC3B071F95F51D07
SHA-512:	15071612EC1B304E353B925E936DF82CEA7B2588E6161E024DC66CF75B2408213434E6F2E100731E8CF945B2FB6C6439B5B9AAF62FF81425583E7663EB57E5F7
Malicious:	false
Preview:	MDMP..... .....`.....U.....B.....|.....GenuineIntelW.....T.....4.....`.....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.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.749839880542537
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 98.32% • Windows Screen Saver (13104/52) 1.29% • 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:	570000.dll
File size:	179200
MD5:	6577b8581782142e658f404003f240ab
SHA1:	c6420b09963f9cc8db489b477238374448b11de8
SHA256:	0314e12bc1cb1e046282a7933eab7e5fa7ec39c9ceaa78e233c7648904af5c28
SHA512:	87fadabf617e0d31a231bd49b8f33d0174092c9d4ae7784b3b2259627ca1240962416b7411b5dafd69bd35fad9caabbbb4bc79507176fffa423f5b972be87568
SSDEEP:	3072:x3dMfAlx6C82qlalrbnwEBQS8TxyEAJ5dtjCklcvdIwC7cP2fJN/:xNUA2OqlalrtQoEAJ5v1lcvd+c
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.....lz.....l|.....ll.....+...L.....L.....L.....lf.....l}.....l~.....Rich.....

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x5780c6
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x570000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x60C0F889 [Wed Jun 9 17:21:13 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	3e5a5960a954602a0f374a91077473ac

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x221e3	0x22200	False	0.590537717491	data	6.55963979258	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x24000	0x2b17	0x2c00	False	0.445490056818	data	5.28724104951	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x27000	0x13cc	0x1000	False	0.4931640625	data	4.84088151062	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0x29000	0x20e8	0x2200	False	0.954733455882	data	7.86292109355	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x2c000	0x4000	0x3800	False	0.660435267857	data	6.09371034777	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5428 Parent PID: 5624

General

Start time:	14:26:26
Start date:	06/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\570000.dll'
Imagebase:	0xc00000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.251665430.00000000017D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000000.236700469.00000000017D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000000.237506792.00000000017D8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4396 Parent PID: 5428

General

Start time:	14:26:27
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\570000.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5400 Parent PID: 5428

General

Start time:	14:26:27
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\570000.dll,#1
Imagebase:	0xe10000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2021

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000000.231677722.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000000.232967522.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.255343857.00000000048B8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5372 Parent PID: 4396

General

Start time:	14:26:27
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\570000.dll',#1
Imagebase:	0xe10000
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_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000000.233920310.00000000046C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000002.264420353.00000000046C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000000.232287785.00000000046C8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: WerFault.exe PID: 6048 Parent PID: 5400

General

Start time:	14:26:30
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5400 -s 640
Imagebase:	0x7ff797770000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

Copyright Joe Security LLC 2021

File Written

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: WerFault.exe PID: 3276 Parent PID: 5372

General

Start time:	14:26:30
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5372 -s 644
Imagebase:	0x8a0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Key Value Modified

Analysis Process: WerFault.exe PID: 4036 Parent PID: 5428

General

Start time:	14:26:32
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5428 -s 272
Imagebase:	0x8a0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Copyright Joe Security LLC 2021

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Modified

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021