ID: 447090
Sample Name: lj3H69Z3Io.dll
Cookbook: default.jbs
Time: 11:34:57
Date: 12/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

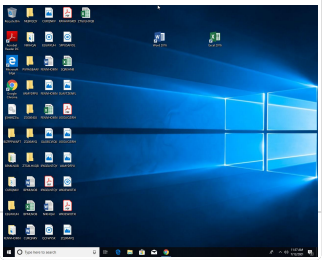
Windows Analysis Report lj3H69Z3Io.dll

Overview

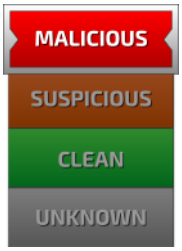
General Information

Sample Name:	lj3H69Z3Io.dll
Analysis ID:	447090
MD5:	0bb29556ece1c5..
SHA1:	324cc356a56c68...
SHA256:	af1b052362469a6.
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection

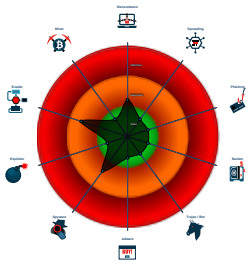


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Checks if the current process is bein...
- Contains functionality to access load...
- Contains functionality to call native f...
- Contains functionality to check if a d...
- Contains functionality to dynamically...
- Contains functionality to query CPU ...
- Contains functionality to query locale...
- Contains functionality to read the PEB
- Creates a process in suspended mo...
- Detected potential crypto function
- Found potential string decryption / a...
- One or more processes crash

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 2392 cmdline: loaddll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 2200 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6068 cmdline: rundll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6072 cmdline: rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Busysection MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 644 cmdline: rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Dealthis MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 3860 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 644 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5776 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 644 -s 644 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 1312 cmdline: rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Sing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2924 cmdline: rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Teethshould MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4840 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2924 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 2948 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2924 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

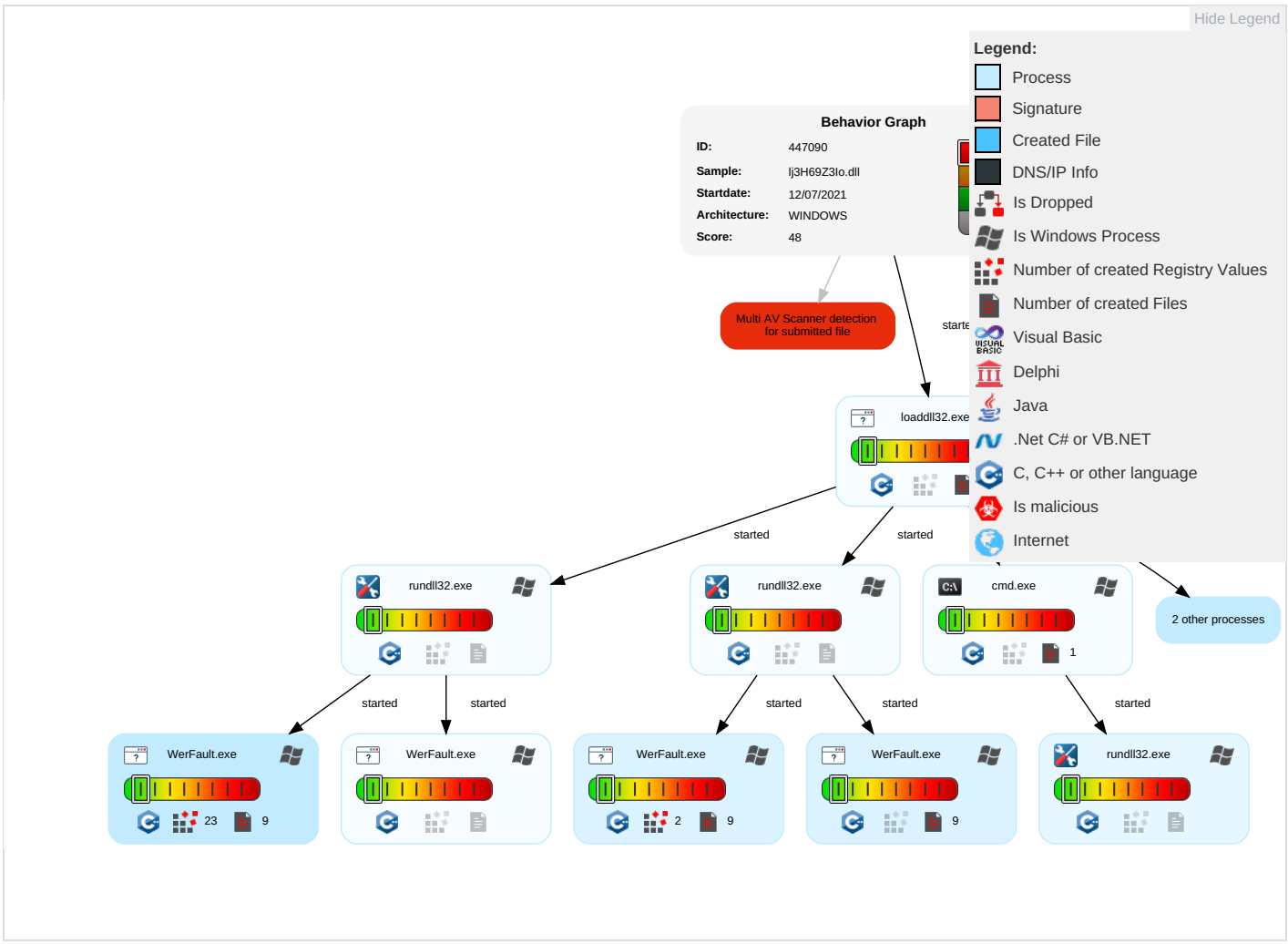
AV Detection:

Multi AV Scanner detection for submitted file

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	Virtualization/Sandbox Evasion 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 2 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)	Deobfuscate/Decode Files or Information 1	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)	Obfuscated Files or Information 2	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	Rundll32 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatior
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Remote System Discovery 1	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	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 3 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station

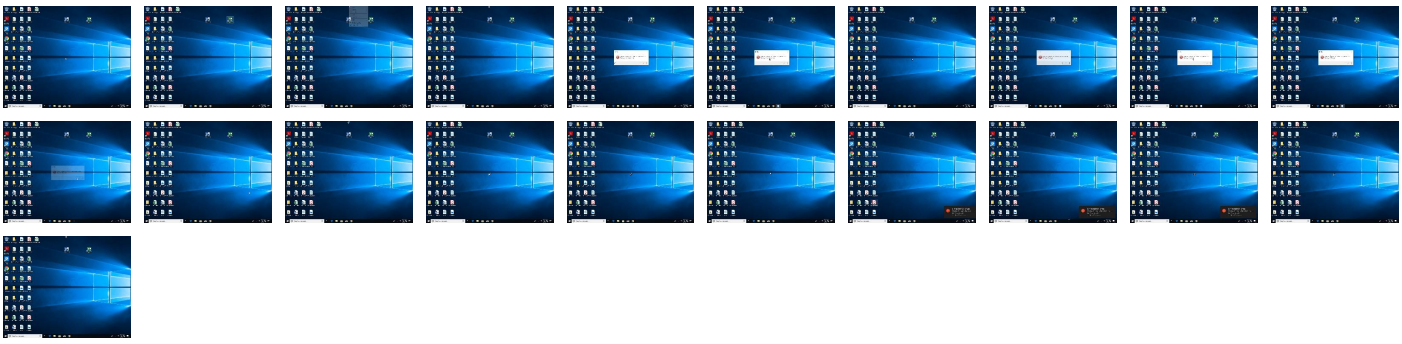
Behavior Graph



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
lj3H69Z3lo.dll	42%	Virustotal		Browse
lj3H69Z3lo.dll	6%	Metadefender		Browse
lj3H69Z3lo.dll	31%	ReversingLabs	Win32.Trojan.Ursnif	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.3090000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.rundll32.exe.2a70000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	447090
Start date:	12.07.2021
Start time:	11:34:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	lj3H69Z3Io.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:	22
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:	mal48.winDLL@17/12@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64% (good quality ratio 58.3%) • Quality average: 73.9% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:37:35	API Interceptor	2x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e10347d3010a05cec57e2a7338104047e76f62_82810a17_0b7b5422\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11844
Entropy (8bit):	3.772182897781727
Encrypted:	false
SSDEEP:	192:FvIij0oX0ZyHVFeMjed+C/u7sJS274ItWcV:Oi9XwKVFeMjen/u7sJX4ItWcV
MD5:	98764053EC0F511D8C5D96513783CA3D
SHA1:	B40C1D4874A55B3691F6919F017472F07B5C07F4
SHA-256:	E7264BFE9EC16F603004FCE25B9BDCF28B7DF62B2787B779B3C2A51BC1F13782
SHA-512:	9349228CE8477F1957230E07E2668FDCF12CB302471B7CCE5CD840C7AD379C3C62AD353C6026060034A6BF2218FE84B9E83F5C167CBAA4006873B8F466E911C7
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.=.1.3.2.7.0.5.8.8.6.6.2.6.8.8.9.5.3.6.....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.=.1.3.2.7.0.5.8.8.6.7.1.3.4.1.5.3.7.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.b.d.3.1.f.7.2.-.4.4.5.6.-.4.9.7.a.-.b.4.3.4.-.2.2.6.5.b.3.e.6.1.a.a.e.....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.=.8.5.9.e.6.1.f.1.-.3.6.6.4.-.4.9.7.2.-.b.e.f.7.-.f.8.8.5.6.0.e.d.4.5.c.b.....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.=.0.0.0.0.0.b.6.c.-.0.0.0.1.-.0.0.1.7.-.4.1.9.3.-.f.d.c.7.4.c.7.7.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.!.0.0.0.0.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.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e10347d3010a05cec57e2a7338104047e76f62_82810a17_0feb1257\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11852
Entropy (8bit):	3.7724877771622407
Encrypted:	false
SSDEEP:	192:pIPtip0oXPZyHVFeMjed+C/u7sJS274ItWc5:UtiHXhKVFeMjen/u7sJX4ItWc5
MD5:	9D46E94DE0C102E2B188098887BC46C4
SHA1:	72324E1311D110D5BC7AE91020192E7F328B1046
SHA-256:	6D5582D44934F0D865C3C291EC1079CF39BEF84CC58C7BEA256459B3E521390E
SHA-512:	99D956F51312CA9999FE24C58B0366A5E9C305F55895F270394451D79B46DA0393065410F03DBF3F0958F25CAC2B3FDF2D0A4A47F94ED8520B8ACD271CE92F7B
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e10347d3010a05cec57e2a7338104047e76f62_82810a17_0feb1257\Report.wer	
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.=.1.3.2.7.0.5.8.8.6.4.4.5.0.1.4.5.6.3.....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.=.1.3.2.7.0.5.8.8.6.5.3.0.4.8.2.9.2.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.4.7.3.c.1.9.f.-.2.5.4.2.-.4.1.6.6.-.a.a.0.b.-.2.5.5.6.5.5.4.8.8.4.5.0.....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.=.6.f.7.f.4.f.9.c.-.b.c.3.7.-.4.9.6.1.-.b.9.e.9.-.a.f.b.4.b.3.5.0.0.0.d.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.=.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.=.0.0.0.0.0.2.8.4.-.0.0.0.1.-.0.0.1.7.-.6.f.0.f.-.1.f.c.0.4.c.7.7.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.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.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_a0d4b84b30b3d4d6122ce7696ca9e3f4f1b52d_82810a17_1216fb83\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11476
Entropy (8bit):	3.768875643122173
Encrypted:	false
SSDEEP:	192:Sij0oXXHKvgsv5yjed+f/u7sJS274It7cf:Si9X3Kvgsv5yjeS/u7sJX4It7cf
MD5:	73201D26AA92F253283D7E2FA80EA01D
SHA1:	9E33A897F2DCE37B89DB00563A4086BB7556FAFC
SHA-256:	71E9DD74E26CDADE6B461668A99FDD0605C20A216266864A73348EAB95CCD0CA
SHA-512:	943F2925D4808EA255075E83293628CB26631DCF08AB07F32E12B47AB8EE5B6EC578887264E46524B6A6529041A99591EEE1ADE79CDFF41FF03621FF401C1173
Malicious:	false
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.=.1.3.2.7.0.5.8.8.6.4.4.8.2.5.5.1.6.3.....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.=.2.7.e.3.9.4.2.1.-.5.c.7.2.-.4.f.3.3.-.9.7.b.7.-.5.2.3.f.0.7.3.8.5.c.3.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.1.d.b.7.0.c.f.-.8.b.a.3.-.4.a.f.f.-.a.9.8.8.-.a.b.3.7.c.5.f.b.3.6.8.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.=.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.=.0.0.0.0.0.b.6.c.-.0.0.0.1.-.0.0.1.7.-.4.1.9.3.-.f.d.c.7.4.c.7.7.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.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\WER2D51.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Jul 12 18:37:45 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	279610
Entropy (8bit):	1.6742774830215899
Encrypted:	false
SSDEEP:	768:eSFnI+naA6a7Q2AsUTusC7lSMWxJ6OXKBMg2VBlwqo:eSFBdAhCxOXKAIdo
MD5:	D253E3147DCE1CF34D14F0D50E09528C
SHA1:	B24900CE0D71CFBFEC6DF206ECD88E35F673CC45
SHA-256:	05BB24CDB6C52AA788043E98B9DD621B3BC9DBE3C7F8FF62ED95A308F23E7565
SHA-512:	64B83B9686358846A9E879B7A80BC471AAC954065E46239CF50E8F95AB70544F34F2D6C12915A6C6E2412A0C1728430F3ED3EDE407E1FDAD483353F0C300B486
Malicious:	false
Preview:	MDMP..... .....`.....U.....B.....GenuineIntelW.....T.....l.....`.....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\WER3996.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):	8288
Entropy (8bit):	3.693305788190394
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiYi6t9Xp6Ylu6DaZbgmfTk8GSLCpDd89bQCsfrUwm:RrlsNil6t9Z6YB6DalgmfTkrSRQBfu
MD5:	EA67DF723579F9F5F17E692A8CA9BD24
SHA1:	46461B5E60EB40D89F7985FC5D56A2913BBFA3D4
SHA-256:	10F07CFB58F20FEB633C899E53FF866F7B9B74C943429F5292A41A9B90A375F8
SHA-512:	5814A115B08F81F593888CD61ECDA2E280CF969B36BEE529F3CE82B8D5916D2B394468CDD0D7B500B9FCE95A4CA11BCD9AFB68BB9DEFDDEF22AFDA32F3234FB2
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3996.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.9.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3E1C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.457541334543927
Encrypted:	false
SSDEEP:	48:cvIwSD8zsqJgtWI9asWSC8BT48fm8M4JCdsGtFB+q8/5jcs4SrSMd:ulTf4hFSNR1JgZ2csDWMd
MD5:	E6CCF4A3AA610785C50C173E1A7976C7
SHA1:	2FB6559D3E8D2EA6B7AF0574980772C232F7C077
SHA-256:	740A09BBBA4C0B2B302AAA3102D617B8D35CE09CADD1E068AF8EB0604AB7A089
SHA-512:	FD299617B050E254D4ECBBA43686E43BA56D1A6D3215A7F084E86E57546B4A4BB46BFB685A416B2CF863E9EB764FF4D6944EFAC73CA627FBFB2E3201E31AF6E4
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="1074468" />.. <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\WERE636.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Jul 12 18:37:26 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	280962
Entropy (8bit):	1.6190396470705883
Encrypted:	false
SSDEEP:	768:B03QgVkiA5gchbjEVUyDX6OaEJpSWp6cEj/qsWDyNVBMg2Vllg:BoQgVk/gcFEV5XgEJpY3qjmNVslg
MD5:	9AC78DF002B515CB73811D2CA5C3D41C
SHA1:	DD93200FFE9ABCDC1BF6D163CA61B947941C9319
SHA-256:	E67D5006C7D713C404C95F8E58B68B4FE52989D913671F3E4EBF595315E9A41E
SHA-512:	6AFC6E40C33C66FEA6A828C44CB79E7C2A377829C3F8608FCEC8A824749BB6127A41641A91A5617C77F2162F90E1571917B25F21FF39FF116A3AC26A43DAADA1
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\WERE77E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Jul 12 18:37:27 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	31730
Entropy (8bit):	2.5908843139629227
Encrypted:	false
SSDEEP:	192:NLnXZTgxJ6P4LMI2+2dCF2V6qkIHPpsI5xWGnx:FJTmwIBl2g2V6q4l5lx
MD5:	B62BFAF733B3B9DB4873EB60FEC6812D
SHA1:	215947439972F9A2ADE25E26F1B35F9C5E201BE1
SHA-256:	6D66F2709120D2E6DCB4B0B1AD4E7F04AA8E47FF099E89E682518470DED7F018
SHA-512:	58804ED5C76A0A51962B999E0BA8DBE6B87A52DEEBB64466AE1BBED6BCCF1B81FE6079F48ED863664230432C47196FF339E73969B8188D3985B8336967BCF2E
Malicious:	false
Preview:	MDMP..... .....`.....U.....B.....GenuineIntelW.....T.....l.....`.....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\WERF0F5.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):	8282
Entropy (8bit):	3.6946242951270065
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNijb6qU/6YIK6+aJbgmfTk8GSLCpDu89bfLsfULVm:RrlsNi/6qU/6YN6+aVgmfTkrS8fQfX
MD5:	78A9B2639FBEB484496E0DD30F14E7A1
SHA1:	43BC95135E8C35ED12BB8D4CA4F58DB5ABEB879D
SHA-256:	E941E743CDC9F5AD163B9A90C879B798E5A3BF1000FED157808962EF70BE1DAA
SHA-512:	CD43799611CC01456BBAE8927318BC352085682861B3B57FA3D223B10A8FE7492EDC241EA257D87FA7A1991AB97485C0F79DA13EB9DB27353D343E28A38876A5
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.>.6.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF152.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):	8350
Entropy (8bit):	3.690539983955562
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiYM6uAEd6Yim6+aJbgmf8lSJLCpBE89bfCsfDVm:RrlsNib6uAu6Yx6+aVgmf8lSJQfBfs
MD5:	8270ACC93A90BBC69A9E4C6E322D4123
SHA1:	448CB0408C15E46CC084445FA3A9D536DCEC8653
SHA-256:	7319A54E282E1C3850C36D98F55B4E923FAB4BCBBFD2A88EE8CBD28C84B4AB10
SHA-512:	F6A404AF9D1300A325277CBC0644EB00F4E1977A104A991E7F89B6971F907E5D150A8E094E2FF28B2BABEB509F1411EACC46799B676F5ADEACD86E0C7653837
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.9.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF53B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.45574569896631
Encrypted:	false
SSDEEP:	48:cvIwSD8zsqJgtWl9asWSC8BNs8fm8M4JCdsGtFtJ+q8/5jH4SrS6d:uITf4hFSNTRJgFJ2HDW6d
MD5:	9CE1A35D608471E1CB4FC7B9D3E1677F
SHA1:	197E73863977B19EC31B551B1258363E311CF6F0
SHA-256:	78E8A937C8C36917C51CAEF293069B9D8677E176DD4E4799AB53B025755CAEFA
SHA-512:	608737A72FBA6E73EB41181E84EE29202D4C6AB7BAB6B259B6557E7EF9181BAB08853EA7586C8038DDE5AB426AFDC0639E03928ED0975A62D48B742F5C4EB00
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="1074468" />.. <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\WERF5D8.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4731
Entropy (8bit):	4.450261196501411
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5D8.tmp.xml	
SSDEEP:	48:cvIwSD8zsqJgtWl9asWSC8Bo8fm8M4JCdsqFn+q8vjsDs4SrSMd:uITf4hFSNLJOKOsDWMd
MD5:	4C6796B08FFA1674376D69F88821DA34
SHA1:	C03827CB15E533002B3B3D291686985CD0382C0C
SHA-256:	99B1663F2E16E493E0CF5BC04A097D6EF5D1A53108DB3C099A61980B6DEBDF6B
SHA-512:	0D7C06F0FF244FA5A78AED9BC3BFA8630D1B0E9A03DA56D4BC1BD806693E12791D5BE8460DD4F696D1B74F46B6B3E06B2F324231F7C2E527412517BE21B5D35 0
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="1074468" />.. <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" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.767213059044483
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:	lj3H69Z3Io.dll
File size:	512000
MD5:	0bb29556ece1c51c751cb4e7c8752ddc
SHA1:	324cc356a56c68e51f09348e91405001e68e4a08
SHA256:	af1b052362469a67fcd871558b24efa2be44a4b29f88112e5c2d2295a1dc4252
SHA512:	33d9a2b92f209ed7fea50bc388d34d7cce773217f73d58fda98ad94c13cd64621b92525602e87c016bab424f438ae96655af8d8250d642d9d7fc7a080f936c79
SSDEEP:	12288:pvlT2EsAw96epX+uHfa7Z5svN/RM2ZcV8TFITzhz3VFVUJcXH4nw7P1N:ZsN96cfKFVUJQu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H..5...f...f...f.z.f...f.z.f...f.z.f...f^..g...f^..g8..f^..g...f..}f...f...fv..f...g...f...g...f...g...fRich...f.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10340e7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5B2B4D21 [Thu Jun 21 07:00:49 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0

General

Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	df95180b6da9d16cb69b63ca8bb7f332

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4f1c7	0x4f200	False	0.639085332741	data	6.65199808864	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x51000	0x2936e	0x29400	False	0.621620501894	data	6.09428205246	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x7b000	0x98ad0	0x1000	False	0.2373046875	data	3.49060216778	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x114000	0x3530	0x3600	False	0.748191550926	data	6.69710092848	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

UDP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 12, 2021 11:37:32.306720972 CEST	8.8.8.8	192.168.2.6	0xf4ff	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 12, 2021 11:37:34.045018911 CEST	8.8.8.8	192.168.2.6	0xdc08	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 2392 Parent PID: 5888

General

Start time:	11:35:51
Start date:	12/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.dll'
Imagebase:	0x8a0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2200 Parent PID: 2392

General

Start time:	11:35:51
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.dll',#1
Imagebase:	0x2a0000
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: 6072 Parent PID: 2392

General

Start time:	11:35:52
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Busysection
Imagebase:	0x1c0000
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: 6068 Parent PID: 2200

General

Start time:	11:35:52
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.dll',#1
Imagebase:	0x1c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 644 Parent PID: 2392

General

Start time:	11:35:56
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Dealthis
Imagebase:	0x1c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1312 Parent PID: 2392

General

Start time:	11:36:03
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Sing
Imagebase:	0x1c0000
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: 2924 Parent PID: 2392

General

Start time:	11:36:10
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Teethshould
Imagebase:	0x1c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 3860 Parent PID: 644

General

Start time:	11:37:21
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 644 -s 652
Imagebase:	0x190000
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: 5776 Parent PID: 644

General

Start time:	11:37:21
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 644 -s 644
Imagebase:	0x190000
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: 4840 Parent PID: 2924

General

Start time:	11:37:21
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2924 -s 652
Imagebase:	0x190000
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: WerFault.exe PID: 2948 Parent PID: 2924

General

Start time:	11:37:39
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2924 -s 660
Imagebase:	0x190000
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

Disassembly

Code Analysis