ID: 537742
Sample Name:
1.2.javaw.exe.22e0000.2.exe
Cookbook: default.jbs
Time: 12:15:12
Date: 10/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

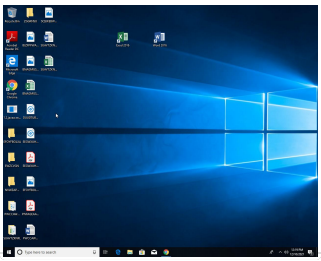
Windows Analysis Report 1.2.javaw.exe.22e0000.2.exe

Overview

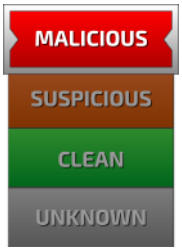
General Information

Sample Name:	1.2.javaw.exe.22e0000.2.exe
Analysis ID:	537742
MD5:	c47bfe4e43d258b.
SHA1:	eb2c417a29d2f08.
SHA256:	f4d742d82698f53..
Infos:	

Most interesting Screenshot:



Detection

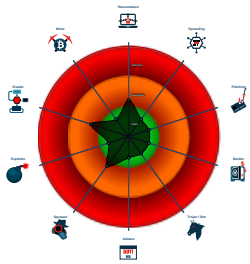


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Creates autostart registry keys to la…
- Machine Learning detection for samp…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- AV process strings found (often use…
- PE file does not import any functions
- One or more processes crash
- Contains functionality to read the PEB
- Checks if the current process is bein…
- PE file contains sections with non-s…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- 1.2.javaw.exe.22e0000.2.exe (PID: 6984 cmdline: "C:\Users\user\Desktop\1.2.javaw.exe.22e0000.2.exe" MD5: C47BFE4E43D258B87C6CECE9DE90C89F)
  - WerFault.exe (PID: 2060 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6984 -s 212 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:

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

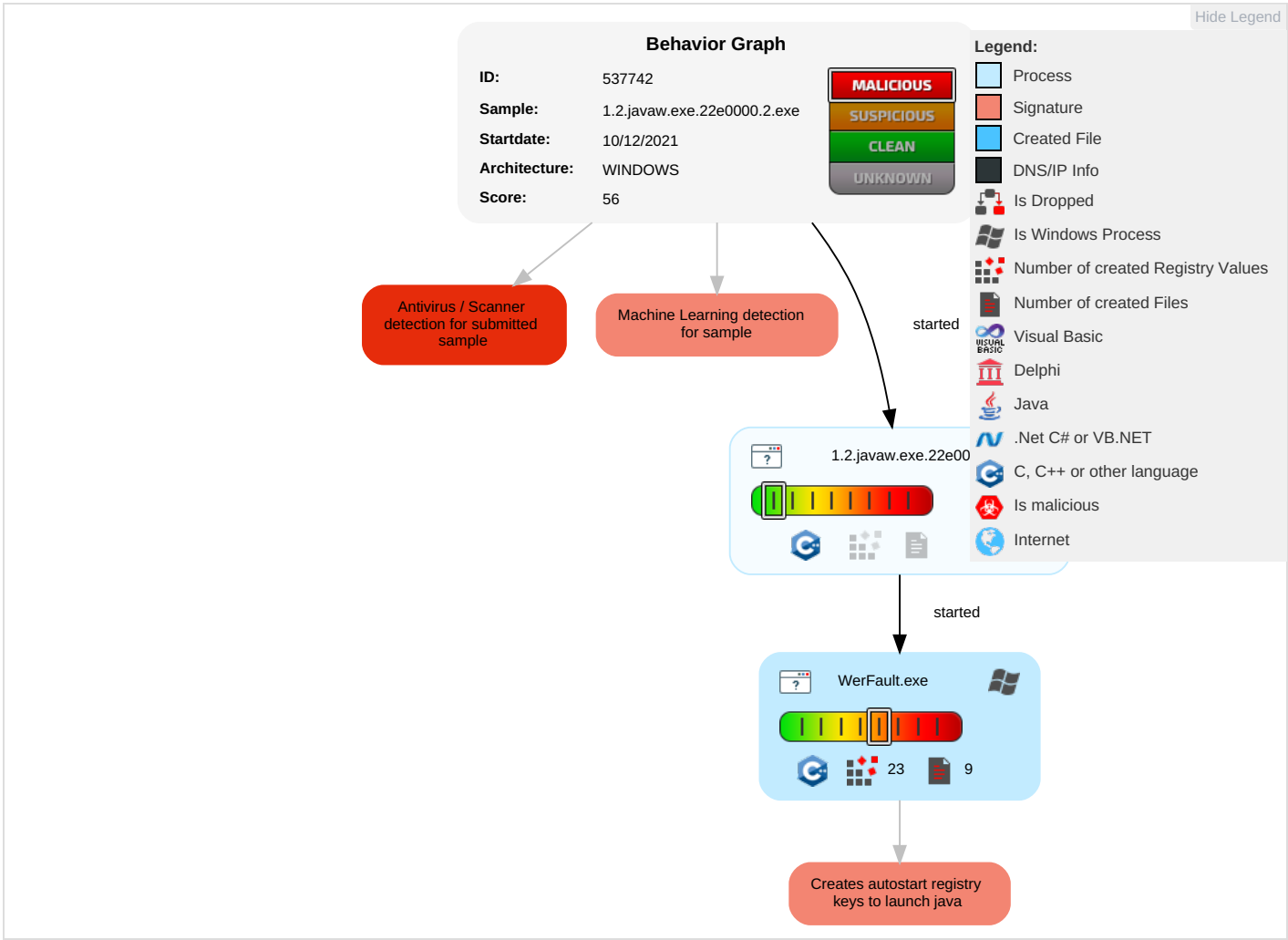
Boot Survival:

Creates autostart registry keys to launch java

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 1	Virtualization/Sandbox Evasion 1	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Software Packing 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Ob De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

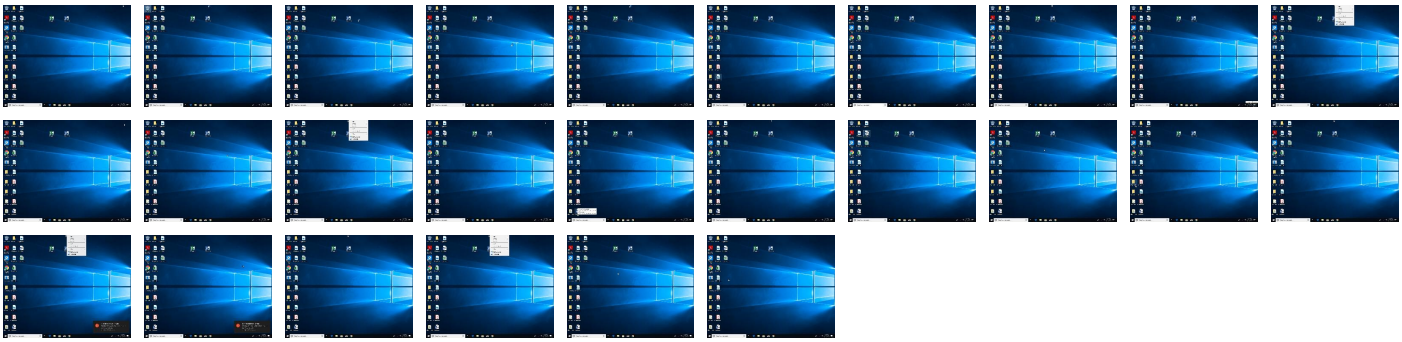
Behavior Graph



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
1.2.javaw.exe.22e0000.2.exe	100%	Avira	TR/Crypt.XPACK.Gen	

Source	Detection	Scanner	Label	Link
1.2.javaw.exe.22e0000.2.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.1.2.javaw.exe.22e0000.2.exe.22e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.1.2.javaw.exe.22e0000.2.exe.22e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.1.2.javaw.exe.22e0000.2.exe.22e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.1.2.javaw.exe.22e0000.2.exe.22e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		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:	537742
Start date:	10.12.2021
Start time:	12:15:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1.2.javaw.exe.22e0000.2.exe
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:	26
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:	mal56.winEXE@2/6@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 94.7% (good quality ratio 47.4%) • Quality average: 36.5% • Quality standard deviation: 41.2%
HCA Information:	• Successful, ratio: 100% • 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: .exe
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_1.2.javaw.exe.22_e816a0737e58b9c4a7ce791273f8931c044f28_358f4505_09668aab\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):	0.6387115446126613
Encrypted:	false
SSDEEP:	192:4nlgLpUmqHBUZMXW1xjE/u7svS274ltJ6H:+yQBUZMXIjE/u7svX4ltE
MD5:	259D7D09E351671F850950A54F800028
SHA1:	8163D0665B803B97847B84CF528E4E9ED55BBA1F

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_1.2.javaw.exe.22_e816a0737e58b9c4a7ce791273f8931c044f28_358f4505_09668aab\Report.wer	
SHA-256:	073CFD100EC7746447AD2EB1CC08A7D9899BF378ECC7B85BE52EAE01CBB96826
SHA-512:	665EB00CC8653950101549C144E409E4BED71E19164682B37459E60CC06C9A7C8C14DDFD59CF2CFC0A230DFEED79A61EF78FCB5F58170387EAE1E71F734925
Malicious:	false
Reputation:	low
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.=.1.3.2.8.3.6.4.0.9.7.3.0.8.4.1.3.2.5.....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.=.1.3.2.8.3.6.4.0.9.7.6.3.8.1.0.0.3.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.5.e.3.1.8.a.2.-.7.8.b.b.-.4.3.6.7.-.b.3.2.2.-.2.a.0.a.a.e.e.6.f.5.d.d.....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.d.4.f.e.9.6.3.-.c.d.c.2.-.4.c.1.e.-.8.8.d.6.-.7.3.1.d.5.a.e.e.5.b.7.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.=.1...2...j.a.v.a.w...e.x.e...2.2.e.0.0.0.0...2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.4.8.-.0.0.0.1.-.0.0.1.c.-.e.e.9.0.-.4.7.c.4.0.2.e.e.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.c.4.9.c.8.6.c.a.b.9.5.e.7.6.6.2.d.e.d.8.0.3.a.3.f.1.0.6.b.3.f.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.2.c.4.1.7.a.2.9.d.2.f.0.8.e.3.7.d.6.3.f.3.b.7.5.c.d.c.6.1.b.4.2.8.5.5.e.9.1.!.1...2...j.a.v.a.w...e.x.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B9.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Dec 10 20:16:13 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	18362
Entropy (8bit):	2.343903676364738
Encrypted:	false
SSDEEP:	96:5y8iT8Q/VrODryOCxYyoi7kj9zCHubLBE/1Tk2flR2WntEWInWIX4I4ChWO9OY:niXVruryOCubOKzRLYlMWtBChWOoY
MD5:	EB0B539902398955A64EF6B0E07C3BAA
SHA1:	FD3BD62651A5166D74603F07C6AA1DFA680F510E
SHA-256:	2DD148793BA664BE56E3C5B2EB1DFC64796FF3E0E9B90556FCC844883F9ED593
SHA-512:	E42FE9230E408F4035816CBDE921509C712DBA0A0FC97F27FC6950EB2DB2856A3A1EE068F81EEC75E8F173DC046CEA018840785DF73C591724EAD058F4B5CA6
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....4..... ...<.....d.....T.....8.....T.....>.....\.....H.....U.....B.....GenuineIntelW.....T.....H.....a.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B79.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):	8356
Entropy (8bit):	3.698609452578638
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiAkD60bv6YFASUUogmfgKbS5Cpr489bR5sfhbm:RrlsNiH646YCSUUogmfhS0RSfA
MD5:	216914B0B00EC2009D396AAAA7FFB323
SHA1:	F5F1BCEA1FD05CCCDF9E88EF7FD2504F0F372DA5
SHA-256:	0B0C307B0EFCDFB64C1CBEF95D904E66410A97C58BA088543A7DFAFA4CD976BD
SHA-512:	F1D563E56EB0A92F7A5C7BEA0081F4D39243AF20F91581A0D1D450220E485426712175A1B76F81B3FCD88DE52FB5355FAC0893FE4C7BCB268B3ACE608B27337
Malicious:	false
Reputation:	low
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.>.6.9.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E68.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4654
Entropy (8bit):	4.469771708373248
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI9HKzoWSC8B5y/8fm8M4Jij2mFoi+q8mWcc9osUd:uITfqFNSNGkJNiq9osUd
MD5:	C5A829051FB453E06999223896F7EAE8
SHA1:	49FDB57106FB64C6D32550E577BEC8A7A21A7FA4
SHA-256:	F52D469D5312316C025D55E6C2150CBED4C1BEA42E85D8020635372BCC0E85F9
SHA-512:	C45D9D45DE5953F1FF5DFB45A81A9B37775A37ADE198E8A20A66A8CFCE7C7C87A993510A530911B3C4D0D5009CF6D89328B8EF21266E07F0391D00461601E36
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E68.tmp.xml	
Reputation:	low
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="1292006" />.. <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):	4.275800585591826
Encrypted:	false
SSDEEP:	12288:vvsTovxSsEMRpXQDqJzAeuJgpN1sSxkbTHJsuRdNo4s6fThgDuxSy:HsTovxSsEMRpXQ3E
MD5:	31FA34FBB33900F29147D20EF0DA77C0
SHA1:	E70D0DADA92800498655AFD85A7BE4E3A01964CE
SHA-256:	9BD63165253885AB98F8592689B127D2766FAA9E490A3ECB50E7086D1497A60D
SHA-512:	C52B3E0D58FD8E4656AB43DAF33B0121C8EA2B150ED6B098E38A7F1388DE15638C2F025F3F321D63A62814343A9B574B3BCAF9F6DAB17935A14E674214BF50F
Malicious:	false
Reputation:	low
Preview:	regfZ...Z...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..r..... .....v.....

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):	24576
Entropy (8bit):	4.0023138344330675
Encrypted:	false
SSDEEP:	384:wJYX5Rftx1OPJ4XxZFFnQ7k9PBqXeSeq5QMVyiy+/1l4Lk4iZd1DoXzn+a8deV:wYJRftx10J4XTFFQ7KBqXleq5QMVyiy1
MD5:	C21D8691ED58E0FEA9BCF34504847DA0
SHA1:	69B0F3CAE2893150E8C21FE86AACAA0867C8F9A5
SHA-256:	986ADE1932FF0E7C06D04589D3222CC247E5345EFDE167682F2188D1DA7272B7
SHA-512:	C67FB1DA7DA1B3ADC6EAD421986CC53B7C19E995254B42E3140DF04B72A9C2DCDBF5FD486E383F31F46AD37E4F18CABF2A1AEB7AF705EB95A8DA5183D6861DD0
Malicious:	false
Reputation:	low
Preview:	regfY...Y...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..r..... .....v.HvLE.^.....Y.....C)..F..I!.5..J.j.....0..... ..hbin.....p.\..,.....nk,...u..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...u..... ....Z.....Root.....lf.....Root....nk ...u.....}..... .....*.....DeviceCensus..... ..vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.916588118656297
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	1.2.javaw.exe.22e0000.2.exe
File size:	58880
MD5:	c47bfe4e43d258b87c6cece9de90c89f
SHA1:	eb2c417a29d2f08e37d63f3b75cdc61b42855e91
SHA256:	f4d742d82698f532e0215832cb484619a4e84547d8a1ca8dc8f2e9f791a6f27d

General

SHA512:	e5fe932fc3245c68f846450db94459d69f992009667e2d9cc6e0ac520723ba9da558698948d596d18512afdfa554ce61dddafa1d0941cc7f3ab94b066885f57b
SSDEEP:	768:kg9fMhjuf6B6vgjloxr9Elz2y9Vn/uS4POG1GY5GMxzdAjNxc:klhiCB6gjyBEs3h4WG1lUMld4Nxc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.z.h.z.h.z.h...i.z.h...i.z.h...h.z.h.z.h.z.h=..i.z.h=..h.z.h=..i.z.hRich.h.z.h.....PE..L.....ga.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x22e4a40
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x22e0000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	GUARD_CF, NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x616701A9 [Wed Oct 13 15:56:25 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8f5f	0x9000	False	0.487820095486	data	6.55103014538	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xa000	0x1740	0x1800	False	0.583821614583	data	5.73452393233	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc000	0x9ec	0x200	False	1.021484375	data	7.55445028361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.teslaX	0xd000	0x2e70	0x3000	False	0.223551432292	data	2.49418691917	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x10000	0x1e0	0x200	False	0.291015625	data	1.76481887066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x11000	0x5d0	0x600	False	0.303385416667	data	3.43918740047	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 1.2.javaw.exe.22e0000.2.exe PID: 6984 Parent PID: 3416

General

Start time:	12:16:08
Start date:	10/12/2021
Path:	C:\Users\user\Desktop\1.2.javaw.exe.22e0000.2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\1.2.javaw.exe.22e0000.2.exe"
Imagebase:	0x22e0000
File size:	58880 bytes
MD5 hash:	C47BFE4E43D258B87C6CECE9DE90C89F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 2060 Parent PID: 6984

General

Start time:	12:16:10
Start date:	10/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6984 -s 212
Imagebase:	0x890000
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 Created

Disassembly

Code Analysis