ID: 553254
Sample Name: IMG-000284794.exe
Cookbook: default.jbs
Time: 15:06:26
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report IMG-000284794.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Data Directories 15
Sections 15
Resources 15
Imports 15
Version Infos 15
Network Behavior 15
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: IMG-000284794.exe PID: 964 Parent PID: 3560 15
General 15
File Activities 15
File Created 16
File Written 16
File Read 16
Analysis Process: conhost.exe PID: 4908 Parent PID: 964 16
General 16
Analysis Process: aspnet_regbrowsers.exe PID: 6112 Parent PID: 964 16
General 16
Analysis Process: WerFault.exe PID: 5516 Parent PID: 6112 17

General 17
File Activities 17
File Created 17
File Deleted 17
File Written 17
Registry Activities 17
Key Created 18
Key Value Created 18
Disassembly 18
Code Analysis 18

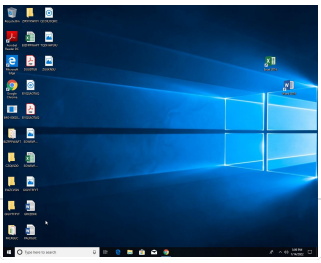
Windows Analysis Report IMG-000284794.exe

Overview

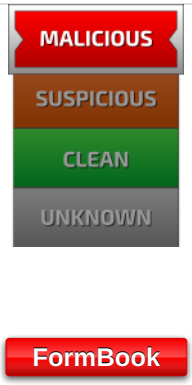
General Information

Sample Name:	IMG-000284794.exe
Analysis ID:	553254
MD5:	abd28466f7cb80d.
SHA1:	fb2911028f32b2b..
SHA256:	5686f840b9b2834.
Tags:	exe xloader
Infos:	

Most interesting Screenshot:



Detection



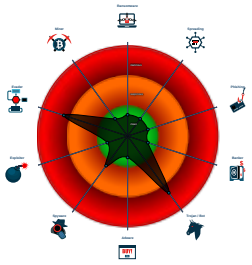
FormBook

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Writes to foreign memory regions
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- AV process strings found (often use…
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- IMG-000284794.exe (PID: 964 cmdline: "C:\Users\user\Desktop\IMG-000284794.exe" MD5: ABD28466F7CB80D6DA36FED9F3E6BEF4)
  - conhost.exe (PID: 4908 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - aspnet_regbrowsers.exe (PID: 6112 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe MD5: B490A24A9328FD89155F075FA26C0DEC)
    - WerFault.exe (PID: 5516 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6112 -s 176 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.129qihu.com/c6si/"
  ],
  "decoy": [
    "tristateinc.construction",
    "americanscaregroundstexas.com",
    "kanimisoshiru.com",
    "wihling.com",
    "fishcheekstosa.com",
    "parentsfuid.com",
    "greenstandmarket.com",
    "fc8fla8kzq.com",
    "gametwist-83.club",
    "jobsncvs.com",
    "directrealtysells.com",
    "avida2015.com",
    "conceptasite.net",
    "arkaneattire.com",
    "indev-mobility.info",
    "2160centurypark412.com",
    "valefloor.com",
    "septembership.com",
    "stackflix.com",
    "jimc0sales.net",
    "socialviralup.com",
    "lastra41.com",
    "juliaepaulovaocasar.com",
    "jurisagora.com",
    "drawandgrow.online",
    "rebekahlouise.com",
    "herport-fr.com",
    "iphone13.webcam",
    "appz-one.net",
    "inpost-pl.net",
    "promocion360fitness.com",
    "global-forbes.biz",
    "diamondtrade.net",
    "albertcantos.com",
    "gtgits.com",
    "travel-ai.online",
    "busipe6.com",
    "mualikesubvn.com",
    "niftyhandy.com",
    "docprops.com",
    "lido88.bet",
    "baywoodphotography.com",
    "cargosouq.info",
    "newsnowlive.online",
    "floridafishingoverboard.com",
    "missnikissalsa.net",
    "walletvalidate.space",
    "kissimmeeinternationalcup.com",
    "charterhome.school",
    "gurujupiter.com",
    "entertainmentwitchy.com",
    "jokeaou.com",
    "sugarmountainfirearms.com",
    "iss-sa.com",
    "smittyssierra.com",
    "freedomoff.com",
    "giftoin.com",
    "realitystararmwrestling.com",
    "salsalunch-equallyage.com",
    "ladouba.com",
    "thepropertygoat.com",
    "bestofmerrick.guide",
    "4the.top",
    "regioinversiones.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000000.361422282.0000000000600000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000000.361422282.0000000000600000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000010.00000000.361422282.0000000000600000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000010.00000002.391762498.0000000000601000.00000020.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000010.00000002.391762498.0000000000601000.00000020.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x136a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x137a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1391f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x83aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1240c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19c3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.0.aspnet_regbrowsers.exe.600000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
16.0.aspnet_regbrowsers.exe.600000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
16.0.aspnet_regbrowsers.exe.600000.2.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cc9:$sqlite3step: 68 34 1C 7B E1 • 0x15ddc:$sqlite3step: 68 34 1C 7B E1 • 0x15cf8:$sqlite3text: 68 38 2A 90 C5 • 0x15e1d:$sqlite3text: 68 38 2A 90 C5 • 0x15d0b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e33:$sqlite3blob: 68 53 D8 7F 8C
16.0.aspnet_regbrowsers.exe.600000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
16.0.aspnet_regbrowsers.exe.600000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected FormBook

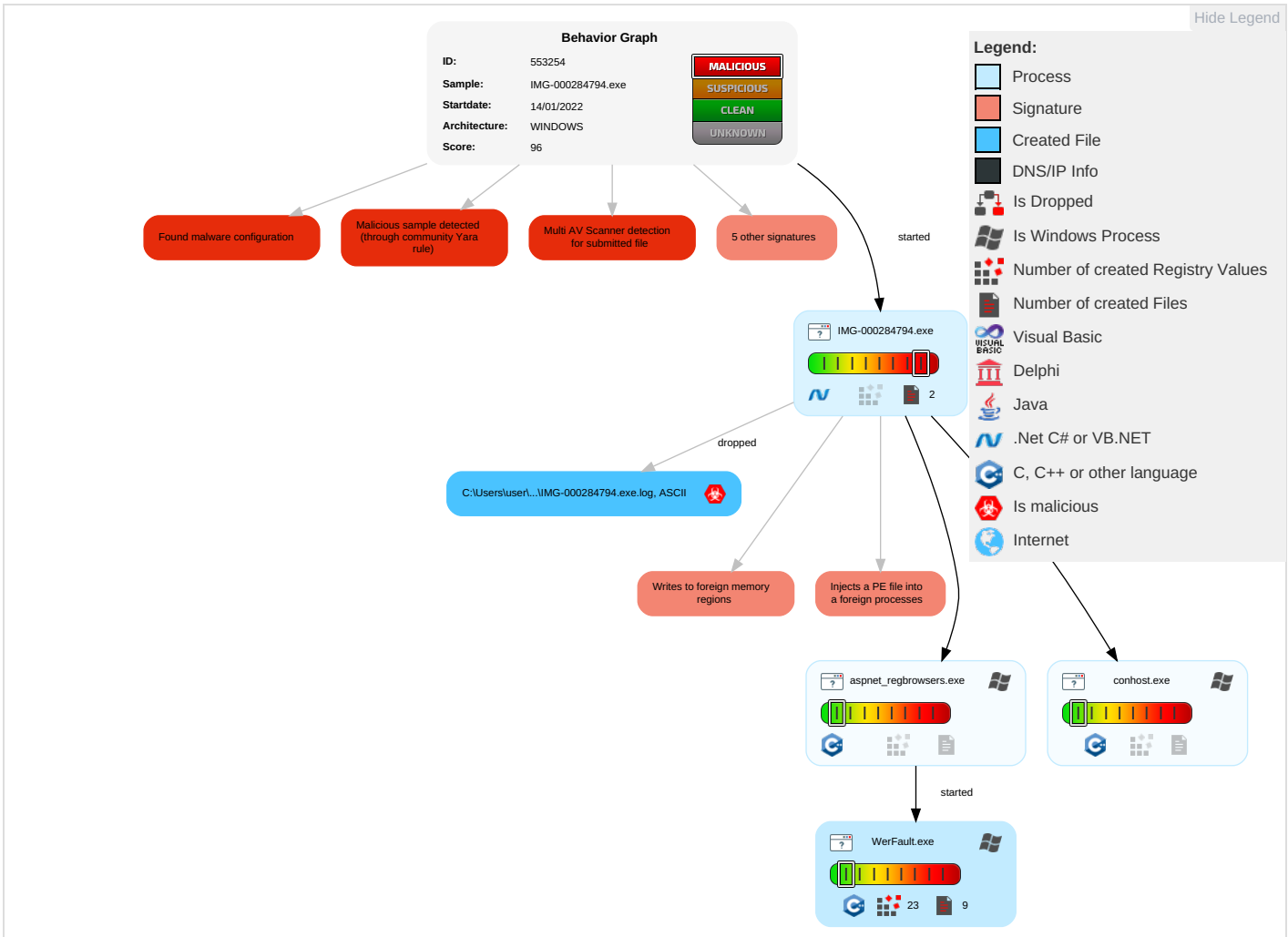
Remote Access Functionality:

Yara detected FormBook

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 2 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Application Layer Protocol 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	System Information Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 2 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

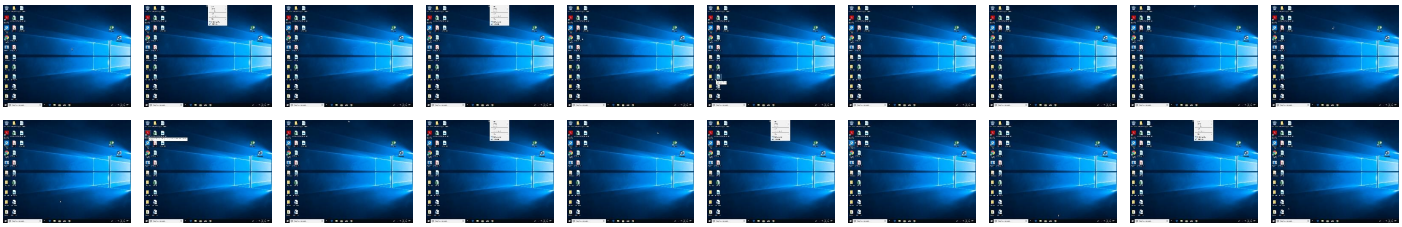
Behavior Graph



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
IMG-000284794.exe	35%	Virustotal		Browse
IMG-000284794.exe	11%	Metadefender		Browse
IMG-000284794.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.0.aspnet_regbrowsers.exe.600000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.0.aspnet_regbrowsers.exe.600000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.0.aspnet_regbrowsers.exe.600000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.0.aspnet_regbrowsers.exe.600000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.0.aspnet_regbrowsers.exe.600000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.2.aspnet_regbrowsers.exe.600000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.129qihu.com/c6si/	0%	Virustotal		Browse
www.129qihu.com/c6si/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.129qihu.com/c6si/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553254
Start date:	14.01.2022
Start time:	15:06:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IMG-000284794.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
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:	mal96.troj.evad.winEXE@5/7@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:08:33	API Interceptor	1x 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\ReportQueue\AppCrash_aspnet_regbrowse_f95c31a2fdc9c125db8ce65728fe31536eece7ae_029cb4bf_1487ecfd\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):	0.6509921914164435
Encrypted:	false
SSDEEP:	96:5XF4wjjVZ4qboI7Rm6tpXIQcQvc6QcEDMcw3DSUN+HbHsZAXGng5FMTPSkvPkpX5:ZtjjVXHBUZMXojl/u7skS274ltER
MD5:	5EFCD7407CCB68F5E1600CA700B71B7B
SHA1:	9E23AF958536F4686D7E2E7137AADFEA33808E72
SHA-256:	08067088893A6E1F716B87FFED7D5F8678293802C5B5C36602BAD2AD0B584CAE

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_aspnet_regbrowse_f95c31a2fdc9c125db8ce65728fe31536eece7ae_029cb4bf_1487ecfd\Report.wer	
SHA-512:	E8AB39C39E29B7E057AE2DAC6B668823A9748CCF5DDF5E114C85D5BF4868C8367A1108EC0C1273E0A079F8E41DB11B559DDF7254166FA923EDE608A2FF230C1
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.=.1.3.2.8.6.6.7.5.3.0.4.1.5.7.5.9.1.4.....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.=.1.3.2.8.6.6.7.5.3.1.2.1.1.0.7.2.0.2.....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.=.e.8.3.9.3.b.9.7.-.a.6.c.9.-.4.d.2.4.-.b.b.d.5.-.a.9.a.d.a.7.0.5.c.b.9.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.=.9.d.7.2.7.e.2.e.-.b.c.b.3.-.4.e.4.6.-.b.c.e.6.-.d.9.8.f.8.0.d.7.8.c.a.7.....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.=.a.s.p.n.e.t._.r.e.g.b.r.o.w.s.e.r.s...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.a.s.p.n.e.t._.r.e.g.b.r.o.w.s.e.r.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.e.0.-.0.0.0.1.-.0.0.1.6.-.3.d.1.3.-.d.1.9.e.9.b.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.l.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.f.6.2.e.c.c.c.d.c.d.8.b.8.9.1.7.7.a.6.a.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER52C0.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 23:08:24 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	18530
Entropy (8bit):	2.065770230992707
Encrypted:	false
SSDEEP:	96:5T8E8//48ihXZi7wG+4Nq52fnlruzqPpUlWInWIHOIx0+TL:qf48ihXZOG52fnlC2pUx0
MD5:	976AB1615F5656EF1055D4657F8E0A4D
SHA1:	3BF1FBE0A826781DB73CCE8691859300D7A6A192
SHA-256:	182DFD5996EF301F00E42D7F6EECE00542CD533F7E6469F4D74884A13E0CCB85
SHA-512:	04C9FD520A6D3225FB0A559BBD75F938DB451025A17BEA89C4B4CAEE236FE86C47355D1219DCDA053CA09C575630F58EE2AB9EBB21E56CD301320286568ADFD
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....h..a.....4.....<.....D.....T.....8.....T.....h....@.....U.....B.....t.....GenuineIntelW.....T.....c..a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER56D8.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):	3.6918681097319936
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiof686Yx46V/gmfnScCprm89bq6rsfyum:RrlsNiA686Y+6V/gmfnSLq6wfS
MD5:	41619F79F56F0C337AB8AC0BF82C97B0
SHA1:	F364E1838497D9579435AFA7B3DBE2A654BB766F
SHA-256:	534FD25188DDD54DBDFB47C1E2455949DCF00ECEBB760142343D5B6AA7E4BC10
SHA-512:	0FC0B4A1FED28C11E7DE8E95C28EE6DC25FC883C0175B04C0941F5545CE12D567613C956EB1F1ECD3348E07FD75811EDC53DB5A3C3E03FE67DBC3875729F464
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.>.6.1.1.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AC1.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4827
Entropy (8bit):	4.488511864546086
Encrypted:	false
SSDEEP:	48:cvIwSD8zsHJgtWI9d5WSC8Bds8fm8M4J3NjMFwZ+q8vfNjKIZDX0d:uITfp6ISN9J3BhKfBKIVX0d
MD5:	98A255139FE144A352AAB322A336A659
SHA1:	8EE696116C940258519C8E79B0054266776B32C8
SHA-256:	ABAEA5F01D9AAE87CB7B4B472DA35D2B6A4F8D2FA51334E3E6FD12F74C7E4845

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AC1.tmp.xml	
SHA-512:	7A12D3C5F8061593D71E390341D9261621C8BAEFBFF387197BF3E52081A2DB6F7E54BFBB9C8A93C4AFA0BFB43D19A50B6558BD2E27A572F4D61B46DAF7F5BA7 1
Malicious:	false
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="1342579" />.. <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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IMG-000284794.exe.log	
Process:	C:\Users\user\Desktop\IMG-000284794.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.348034597186669
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21t92n4M9XKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2f84qXKDE4KhK3VZ9pKhk
MD5:	2BB2F12BA5748B56A733B09151565321
SHA1:	3D3EC51320B4BD72C20E5472FBA4675B5BD7E550
SHA-256:	4114743647967ADE8811D6824ABC4C9ABD4EF0177A0082BACEBFC70C53EE3B16
SHA-512:	84B7D2949FC3E4900A2F74E63C314CC331528BC3010F7867462B8C78AC530075F01C6B7576AE0ACAD909DA200AC28F8BD312F77E0013A73E1D81918CD513DE3
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

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):	4.265899431057205
Encrypted:	false
SSDEEP:	12288:d5n+5OEen+S6rGx2pTp4xCqie6kZSGf3Peg+Qkpr98fuTTLY//DhLbEt:nn+5OEen+S6rGx2Msf7t
MD5:	6DE45ECD67182A11CEBC37E1CA1949C7
SHA1:	9438D2EB075E20FDE0989078476933DBCD36D2CD
SHA-256:	A5F2C6D80C50CF7558D993C7B5E73370ACB7729CBF0AB09946229A8AF5584022
SHA-512:	75D425E646133670FEA1013FF3663772998387437B47DA0541D9980081001FE0CC4F396D155FAD3A28493B0057233303E4C39A2C16D659BB8955345CA06D8AC3
Malicious:	false
Reputation:	low
Preview:	regfQ...Q...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.0..... ....!..... .....

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):	3.8443472902958162
Encrypted:	false
SSDEEP:	384:H4p5tZrdvdX95bQp8fXQnxOf2oTPmxwp+5GjZmG3BDTTez5N5FneHe//:Y3XrrX9uplgf2oyxwpiWmG3pTe9N5de+
MD5:	4137D35BA1E9CECBDDADC65887522682
SHA1:	A15E11804FB79DCA2F6578269E8853E22E4D3AFF
SHA-256:	6E930F69803F0CD00BC5997FFCCDEB773FBB661B9A0E3822E1B0B57BA782F4D4
SHA-512:	C3DE9587C3E8CAF2573F0A982029A7427F05CFA08F1B7EC21AFBE93372FE59B1B73C7EDE3D39E803D69D62D1CD31088EB65E05C1EC6C0A7C7EA8D6258661A8 3B
Malicious:	false
Reputation:	low

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Preview:	regfP...P...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.0..... .....'...HvLE.^.....P.....pV.]..p@bS..... ..hbin.....p.\.,.....nk,..0..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..0..... .....P..... .....Z.....Root.....lf.....Root....nk ..0.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	2.8202817542758174
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	IMG-000284794.exe
File size:	1211392
MD5:	abd28466f7cb80d6da36fed9f3e6bef4
SHA1:	fb2911028f32b2b3c07004a21e84773e3efd1519
SHA256:	5686f840b9b2834952367cd9c37ec4c8385bcc90348dd3a92e488c0faebed85a
SHA512:	0c6aa40cc0797ae3e59bf863bce36c1bb4a96760aa2897b8b03706da83e24a9009fbda569a243c890c7013d4f6e1514e73349757b16c0b318407019ad1e51586
SSDEEP:	6144:jfdz156S1GVaDMtNo7AudqtXwKc95TYY8DZW4aQgUDWEkbp+Y0X5uu8SN7FuuH57:j1NyEqJHEB20uZ6T+YLHEwsL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....E....."...0..r.....1... .....@.. ..... ` .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4031ca
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0xE045D3C7 [Sat Mar 26 10:49:43 2089 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1271d0	0x127200	False	0.373518404543	data	2.81710734526	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x12a000	0x5d4	0x600	False	0.432942708333	data	4.19198536242	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x12c000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: IMG-000284794.exe PID: 964 Parent PID: 3560

General

Start time:	15:07:21
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\IMG-000284794.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\IMG-000284794.exe"
Imagebase:	0x760000
File size:	1211392 bytes
MD5 hash:	ABD28466F7CB80D6DA36FED9F3E6BEF4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 4908 Parent PID: 964

General

Start time:	15:07:22
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: aspnet_regbrowsers.exe PID: 6112 Parent PID: 964

General

Start time:	15:08:19
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe
Imagebase:	0x220000
File size:	45160 bytes
MD5 hash:	B490A24A9328FD89155F075FA26C0DEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000000.361422282.0000000000600000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000000.361422282.0000000000600000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000000.361422282.0000000000600000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.391762498.0000000000601000.00000020.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.391762498.0000000000601000.00000020.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.391762498.0000000000601000.00000020.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000000.361776680.0000000000600000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000000.361776680.0000000000600000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000000.361776680.0000000000600000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000000.364298420.0000000000601000.00000020.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000000.364298420.0000000000601000.00000020.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000000.364298420.0000000000601000.00000020.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000000.363861751.0000000000601000.00000020.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000000.363861751.0000000000601000.00000020.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000000.363861751.0000000000601000.00000020.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Analysis Process: WerFault.exe PID: 5516 Parent PID: 6112

General

Start time:	15:08:22
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6112 -s 176
Imagebase:	0x1350000
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