ID: 233901
Sample Name:
BriggsLawFirm.zip
Cookbook: default.jbs
Time: 16:46:54
Date: 28/05/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

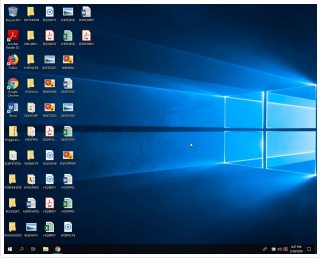
Analysis Report BriggsLawFirm.zip

Overview

General Information

Sample Name:	BriggsLawFirm.zip
MD5:	8e28538307d25e..
SHA1:	b33f3558b16a929.
SHA256:	b78a26b587a8ce..

Most interesting Screenshot:



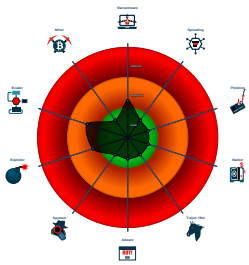
Detection

Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Contains long sleeps (>= 3 min)
- Creates a process in suspended mod…
- Detected potential crypto function
- Found inlined nop instructions (likely …
- May sleep (evasive loops) to hinder d…

Classification



Startup

- **System is w10x64**
- unarchiver.exe (PID: 1716 cmdline: 'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\Desktop\BriggsLawFirm.zip' MD5: 8B435F8731563566F3F49203BA277865)
  - 7za.exe (PID: 3496 cmdline: 'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\u0kti52c.lu3' 'C:\Users\user\Desktop\BriggsLawFirm.zip' MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
    - conhost.exe (PID: 620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

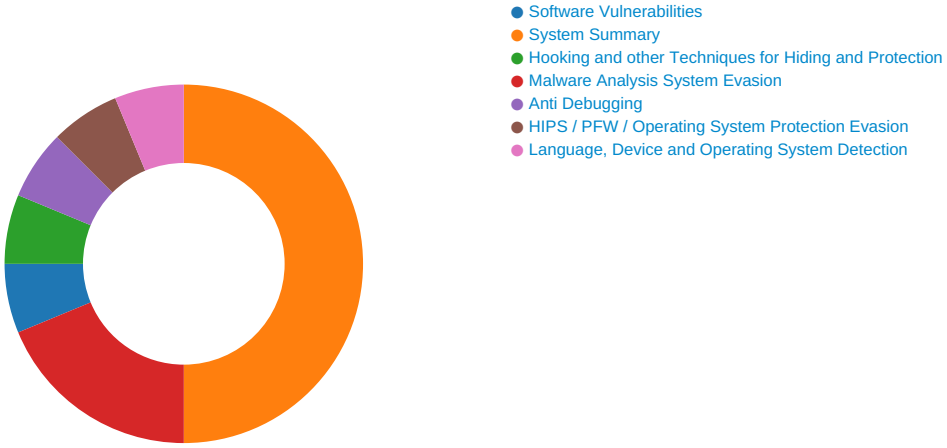
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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 Remote Management	Winlogon Helper DLL	Process Injection 1 1	Disabling Security Tools 1	Credential Dumping	Virtualization/Sandbox Evasion 2	Application Deployment Software	Data from Local System	Data Encrypted 1	Standard Cryptographic Protocol 1	Eavesdrop Insecure Network Communica
Replication Through Removable Media	Service Execution	Port Monitors	Accessibility Features	Virtualization/Sandbox Evasion 2	Network Sniffing	System Information Discovery 3	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Fallback Channels	Exploit SS7 Redirect Ph Calls/SMS
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Process Injection 1 1	Input Capture	Query Registry	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Custom Cryptographic Protocol	Exploit SS7 Track Devic Location
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Obfuscated Files or Information 1	Credentials in Files	System Network Configuration Discovery	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

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:	29.0.0 Ocean Jasper
Analysis ID:	233901
Start date:	28.05.2020
Start time:	16:46:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BriggsLawFirm.zip
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	4
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:	CLEAN
Classification:	clean2.winZIP@4/2@0/0
EGA Information:	• Successful, ratio: 100%
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: .zip • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe

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:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	388
Entropy (8bit):	5.208369949735452
Encrypted:	false
MD5:	56A68D966B645BCFA01ECFAE7839AB82
SHA1:	4AC8F5A5A047B1D532B71DC84628C9A84A27E6F8
SHA-256:	1E088A7F3182E336A6267D8220CDFF18D4A87BAA72E920B71CA51032FA184F9B
SHA-512:	0774911E5703069C689662D2DD67BE6D8ABE1CD75B3ACCDC09CF61F04E0B9FBB14544CADE56A229CFF967E103C98FCB99CDA4794A80310CFE82CA8AF62086A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\d72bdddce94cd6438f15999de0b0afb6\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\49235fda2a08f24faad85fb3459473ea\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\10e08475dc461c7289efd159e9f0e339\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Temp\2y10w0sp.qqv\unarchiver.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	1632
Entropy (8bit):	5.1283459875299915
Encrypted:	false
MD5:	9A9AC5A9416FC1DE931300E50F2D77C0
SHA1:	76A9D969C563E7DF4E22AA9AF38F82A67D052E64
SHA-256:	36F7CA46CC809F8D7C5837DBDC96A10B79F3B74914472DDF85A8FAC64FA1DFDD
SHA-512:	74557D0A275085BDB2C8F0FEB1E1349302017FA6676DFE9D48D242D34E9EAD65E5BF48EB3B47136A8211474E6860DBDA9763BF463D44178852345F0E0E674113
Malicious:	false
Reputation:	low
Preview:	05/28/2020 4:47 PM: Unpack: C:\Users\user\Desktop\BriggsLawFirm.zip..05/28/2020 4:47 PM: Tmp dir: C:\Users\user\AppData\Local\Temp\u0kti52c.lu3..05/28/2020 4:47 PM: Received from standard out: ..05/28/2020 4:47 PM: Received from standard out: 7-Zip 18.05 (x86) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30..05/28/2020 4:47 PM: Received from standard out: ..05/28/2020 4:47 PM: Received from standard out: Scanning the drive for archives:..05/28/2020 4:47 PM: Received from standard out: 1 file, 62662 bytes (62 KiB)..05/28/2020 4:47 PM: Received from standard out: ..05/28/2020 4:47 PM: Received from standard out: Extracting archive: C:\Users\user\Desktop\BriggsLawFirm.zip..05/28/2020 4:47 PM: Received from standard out: --..05/28/2020 4:47 PM: Received from standard out: Path = C:\Users\user\Desktop\BriggsLawFirm.zip..05/28/2020 4:47 PM: Received from standard out: Type = zip..05/28/2020 4:47 PM: Received from standard out: Physical Size = 62662..05/28/2020 4:47 PM: Received from s

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.996913512324501
TrID:	• ZIP compressed archive (8000/1) 100.00%
File name:	BriggsLawFirm.zip
File size:	62662
MD5:	8e28538307d25e1f2f307eb4f3e745a8
SHA1:	b33f3558b16a9296205c0e59d3bce839be9282ef
SHA256:	b78a26b587a8cebf6b5e83e4d69cc661332cc791aaaeb1 ded1893d72a899c3f
SHA512:	3a5317cfceb8cd527f39fbe38204e1c5947fd6c33475889 106a6b00cff6d0540393d0a3189c2ae2aea4a636e49e75f 77b9f141c2699e03f9c5e61ccfb73d5666
SSDEEP:	1536:EAH3mdkO9/Z5LWmi/3t/Be7W5mEQd+7pNZhYo b4pm:wdkOFLWBLXBp5iobl
File Content Preview:	PK.....R..P....8....!.....rule-05.20.doc.. .s.....1.....|.....N. P.4...4.Q)..W..'...n3m.....6.#....?.}.\...>...!..f'.....U...O7.{ Fj.g... u.....,.i.....;M'.....B^...w...|...#c.t._.....h...[bA.....Q.. g...~..... ..F..E.....J..@....k.A.....u..

File Icon

	
Icon Hash:	00828e8e8686b000

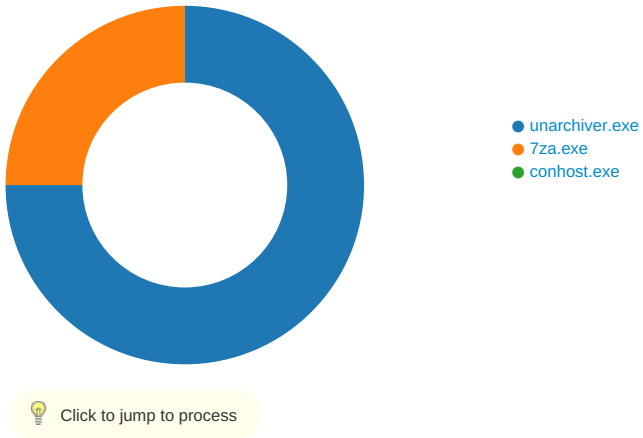
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: unarchiver.exe PID: 1716 Parent PID: 3248

General

Start time:	16:47:20
Start date:	28/05/2020
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\Desktop\BriggsLawFirm.zip'
Imagebase:	0x740000
File size:	10240 bytes
MD5 hash:	8B435F8731563566F3F49203BA277865
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7225608C	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7225608C	unknown
C:\Users\user\AppData\Local\Temp\2y10w0sp.qqv	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	CDA4B1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\2y10w0sp.qqv\unarchiver.log	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	CDA5AB	CreateFileW
C:\Users\user\AppData\Local\Temp\u0kti52c.lu3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	CDA4B1	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2y10w0sp.qqv\unarchiver.log	unknown	70	30 35 2f 32 38 2f 32 30 32 30 20 34 3a 34 37 20 50 4d 3a 20 55 6e 70 61 63 6b 3a 20 43 3a 5c 55 73 65 72 73 5c 47 75 63 63 69 5c 44 65 73 6b 74 6f 70 5c 42 72 69 67 67 73 4c 61 77 46 69 72 6d 2e 7a 69 70 0d 0a	05/28/2020 4:47 PM: Unpack: C:\Users\user\Desktop\BriggsLawFirm.zip..	success or wait	1	CDA8EF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2y10w0sp.qqv\unarchiver.log	unknown	77	30 35 2f 32 38 2f 32 30 32 30 20 34 3a 34 37 20 50 4d 3a 20 54 6d 70 20 64 69 72 3a 20 43 3a 5c 55 73 65 72 73 5c 47 75 63 63 69 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 75 30 6b 74 69 35 32 63 2e 6c 75 33 0d 0a	05/28/2020 4:47 PM: Tmp dir: C :\Users\user\AppData\Local\Temp\u0kti52c.lu3..	success or wait	1	CDA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\2y10w0sp.qqv\unarchiver.log	unknown	50	30 35 2f 32 38 2f 32 30 32 30 20 34 3a 34 37 20 50 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 6f 75 74 3a 20 0d 0a	05/28/2020 4:47 PM: Received from standard out: ..	success or wait	18	CDA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\2y10w0sp.qqv\unarchiver.log	unknown	90	30 35 2f 32 38 2f 32 30 32 30 20 34 3a 34 37 20 50 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 65 72 72 6f 72 3a 20 45 52 52 4f 52 3a 20 57 72 6f 6e 67 20 70 61 73 73 77 6f 72 64 20 3a 20 72 75 6c 65 2d 30 35 2e 32 30 2e 64 6f 63 0d 0a	05/28/2020 4:47 PM: Received from standard error: ERROR: Wrong password : rule-05.20.doc..	success or wait	1	CDA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\2y10w0sp.qqv\unarchiver.log	unknown	31	30 35 2f 32 38 2f 32 30 32 30 20 34 3a 34 37 20 50 4d 3a 20 47 65 74 20 66 69 6c 65 73 0d 0a	05/28/2020 4:47 PM: Get files..	success or wait	1	CDA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\2y10w0sp.qqv\unarchiver.log	unknown	37	30 35 2f 32 38 2f 32 30 32 30 20 34 3a 34 37 20 50 4d 3a 20 4e 62 72 20 6f 66 20 66 69 6c 65 73 3a 20 31 0d 0a	05/28/2020 4:47 PM: Nbr of files: 1..	success or wait	1	CDA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\2y10w0sp.qqv\unarchiver.log	unknown	98	30 35 2f 32 38 2f 32 30 32 30 20 34 3a 34 37 20 50 4d 3a 20 46 69 6c 65 20 69 73 20 65 6d 70 74 79 3a 20 43 3a 5c 55 73 65 72 73 5c 47 75 63 63 69 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 75 30 6b 74 69 35 32 63 2e 6c 75 33 5c 72 75 6c 65 2d 30 35 2e 32 30 2e 64 6f 63 0d 0a	05/28/2020 4:47 PM: File is empty: C:\Users\user\AppData\Local\Temp\u0kti52c.lu3\rule-05.20.doc..	success or wait	1	CDA8EF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	unknown	388	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 64 37 32 62 64 64 64 63 65 39 34 63 64 36 34 33 38 66 31 35 39 39 39 64 65 30 62 30 61 66 62 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 34 39 32 33 35 66 64 61 32 61 30 38 66 32 34 66 61 61 64 38 35 66 62 33 34 35 39 34 37 33 65 61 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\d72bddce94cd6438f15999de0b0afb6\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\49235fda2a08f24faad85fb3459473ea\System.Drawing.ni.dll",0..3,"	success or wait	1	7252A806	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722854EC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722854EC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4106	success or wait	1	722854EC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722886E0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722886E0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4106	success or wait	1	722886E0	ReadFile
unknown	unknown	1024	success or wait	2	CDA8EF	ReadFile
unknown	unknown	1024	pipe broken	2	CDA8EF	ReadFile

Analysis Process: 7za.exe PID: 3496 Parent PID: 1716

General

Start time:	16:47:21
Start date:	28/05/2020
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\u0kti52c.lu3' 'C:\Users\user\Desktop\BriggsLawFirm.zip'
Imagebase:	0x1020000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\u0kti52c.lu3\rule-05.20.doc	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10263B0	CreateFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BriggsLawFirm.zip	unknown	1024	success or wait	1	102686E	ReadFile
C:\Users\user\Desktop\BriggsLawFirm.zip	unknown	62662	success or wait	1	102686E	ReadFile
C:\Users\user\Desktop\BriggsLawFirm.zip	unknown	4	success or wait	1	102686E	ReadFile
C:\Users\user\Desktop\BriggsLawFirm.zip	unknown	26	success or wait	1	102686E	ReadFile
C:\Users\user\Desktop\BriggsLawFirm.zip	unknown	14	success or wait	1	102686E	ReadFile
C:\Users\user\Desktop\BriggsLawFirm.zip	unknown	12	success or wait	1	102686E	ReadFile

Analysis Process: conhost.exe PID: 620 Parent PID: 3496

General

Start time:	16:47:21
Start date:	28/05/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c77e0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis