MALWARE ANALYSIS: TRICKBOT

Report Type: Incident	Report Date: 2020-01-06
Report Owner: Grant S.	Data Classification: Unclassified
Incident Severity: Low	Incident Risk: Low

EXECUTIVE SUMMARY

One of our observant colleagues in Human Resources submitted a ticket for potential phishing email on December 16th, 2019. We verified the email was specially crafted for this organization and the link within is malicious. Based on PAI and OSINT, the detected malware appears to belong to the TickBot family. Once these files are executed by the victim, a decoy pop-up is displayed to reduce suspicion of any malicious behavior. Regardless of whether or not the user hits "OK" or closes the pop-up window, the file will still proceed with the download and installation of the Trickbot payload.

All Indicators of Compromise (IOCs) should be blocked immediately. We determined the scope of effect to exactly three end devices on the intranet and began triage actions to contain and eradicate the threat. These hosts will be re-imaged once we are satisfied that scoping is complete. The impacted users must reset their passwords and the Detection Team will review + monitor their access to sensitive sites for suspicious activity.

THE MALWARE

Trickbot is a well-known, modular credential stealer first discovered in 2016. It has been thought to be a descendent of another well-known credential stealer called Dyreza, or Dyre, due to similarities in functionalities and codebase. Due to its modularity, operators of Trickbot are able to gain access to different functions and capabilities by retrieving additional modules from the command and control (C2) servers. These include capabilities such as a worming function (i.e. copying itself to other devices), email inbox parser, and network reconnaissance.

We identified a Trickbot distribution campaign delivered via phishing emails with subject lines using topics around payroll or annual bonuses shown below.

> "Re: <Company Name> annual bonus document is ready"

Generally, Trickbot and similar tools have been largely associated with using malspam with malicious document attachments as the delivery mechanism of choice by their operators likely due to ease-of-use, relatively low resource cost, and high success rates. In this campaign, instead of solely relying on email attachments, the adversaries included links to what appeared to be a legitimate Google Docs document which itself contained links to malicious files hosted on Google Drive. To further obfuscate the malicious activity, the adversaries leveraged a legitimate Email Delivery Service (EDS) called SendGrid to distribute the initial emails, and also hide the Google Drive links in the documents behind a SendGrid URL. Once the user is fully redirected to the file hosted on Google Drive, an executable file is downloaded. This executable is a downloader tool designed to retrieve a Trickbot payload. Similar behavior was observed in August 2019 by Cofense. [1]

"TrickBot is a Trojan spyware program that has mainly been used for targeting banking sites in United States, Canada, UK, Germany, Australia, Austria, Ireland, London, Switzerland, and Scotland. TrickBot first emerged in

[1] https://unit42.paloaltonetworks.com/trickbot-campaign-uses-fake-payroll-emails-to-conduct-phishing-attacks/

the wild in September 2016 and appears to be a successor to Dyre. TrickBot is developed in the C++ programming language. [1] [2] [3]*"*

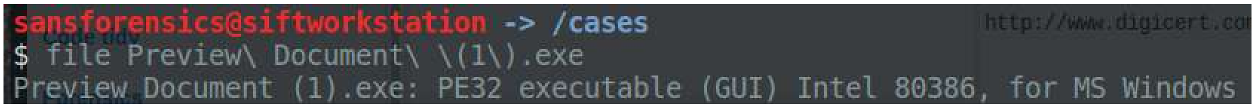
https://attack.mitre.org/software/S0266/

THE ANALYSIS

First Impressions:

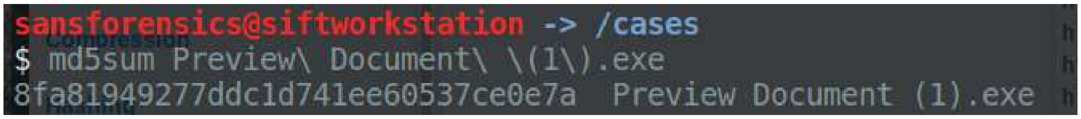
The downloader file in this case is named <Preview Document (1).exe> which defies conventional naming schemes. Combine this with the phishing email and we have good reason not to run this file without caution.

I ran the $file command in my SIFT Workstation to get a better idea of the actual file type:

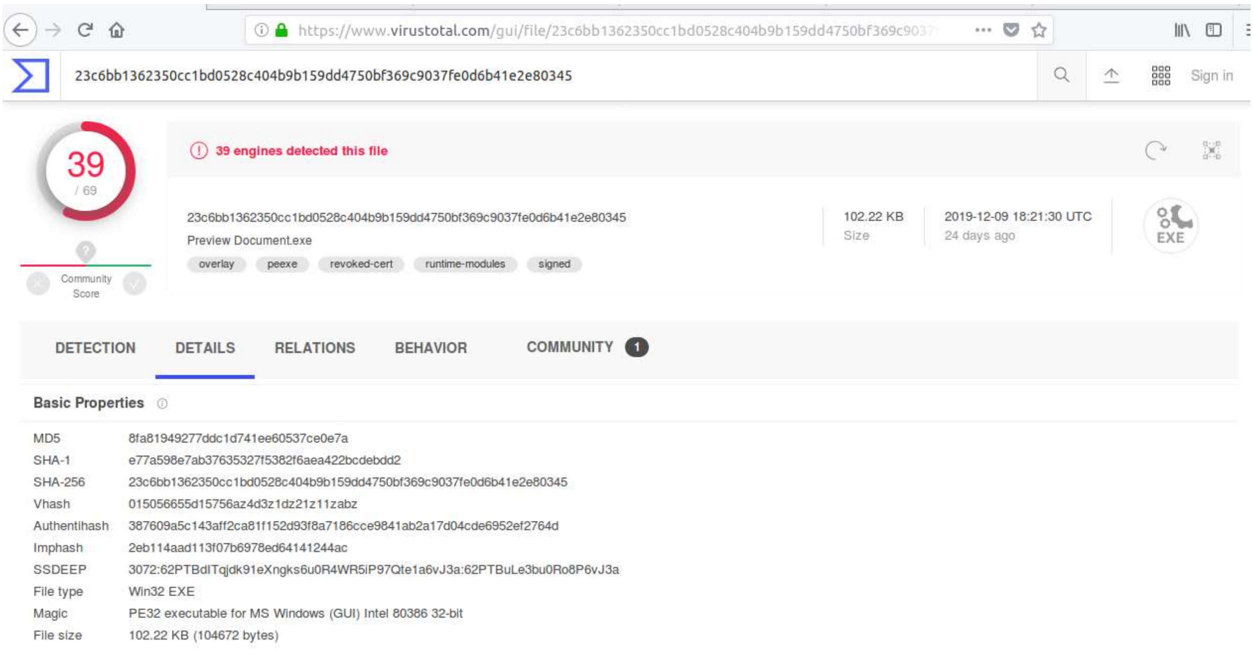


```
sansforensics@siftworkstation -> /cases
$ file Preview\ Document\ \(1\).exe
Preview Document (1).exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

I generated a hash of the file for searching in Virus Total:



```
sansforensics@siftworkstation -> /cases
$ md5sum Preview\ Document\ \(1\).exe
8fa81949277ddc1d741ee60537ce0e7a  Preview Document (1).exe
```



https://www.virustotal.com/gui/file/23c6bb1362350cc1bd0528c404b9b159dd4750bf369c9037
23c6bb1362350cc1bd0528c404b9b159dd4750bf369c9037fe0d6b41e2e80345
Sign in
39
/ 69
Community Score

39 engines detected this file

23c6bb1362350cc1bd0528c404b9b159dd4750bf369c9037fe0d6b41e2e80345
Preview Document.exe

overlay
peexe
revoked-cert
runtime-modules
signed

102.22 KB
Size

2019-12-09 18:21:30 UTC
24 days ago

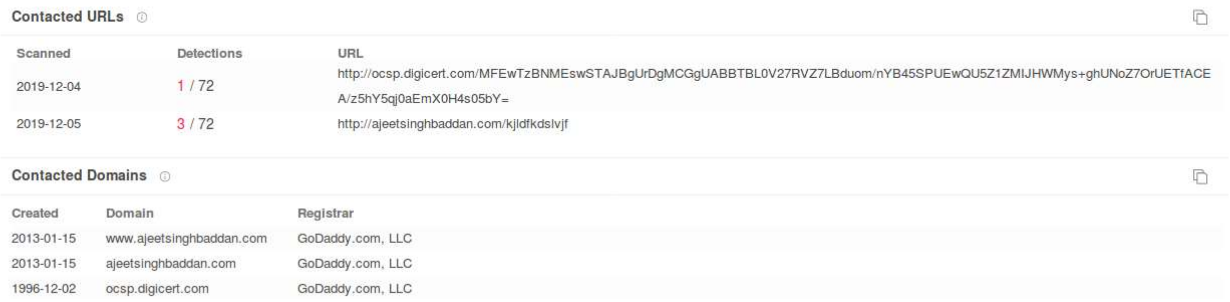
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 1

Basic Properties

MD5	8fa81949277ddc1d741ee60537ce0e7a
SHA-1	e77a598e7ab37635327f5382f6aea422bcdebdd2
SHA-256	23c6bb1362350cc1bd0528c404b9b159dd4750bf369c9037fe0d6b41e2e80345
Vhash	015056655d15756az4d3z1dz21z11zabz
Authentihash	387609a5c143aff2ca81f152d93f8a7186cce9841ab2a17d04cde6952ef2764d
Imphash	2eb114aad113f07b6978ed64141244ac
SSDEEP	3072:62PTBdITqjdk91eXngks6u0R4WR5iP97Qte1a6vJ3a:62PTBuLe3bu0Ro8P6vJ3a
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	102.22 KB (104672 bytes)

The downloader was signed but the signature is not verified.

The second contacted URL below turns out to be the actual payload:



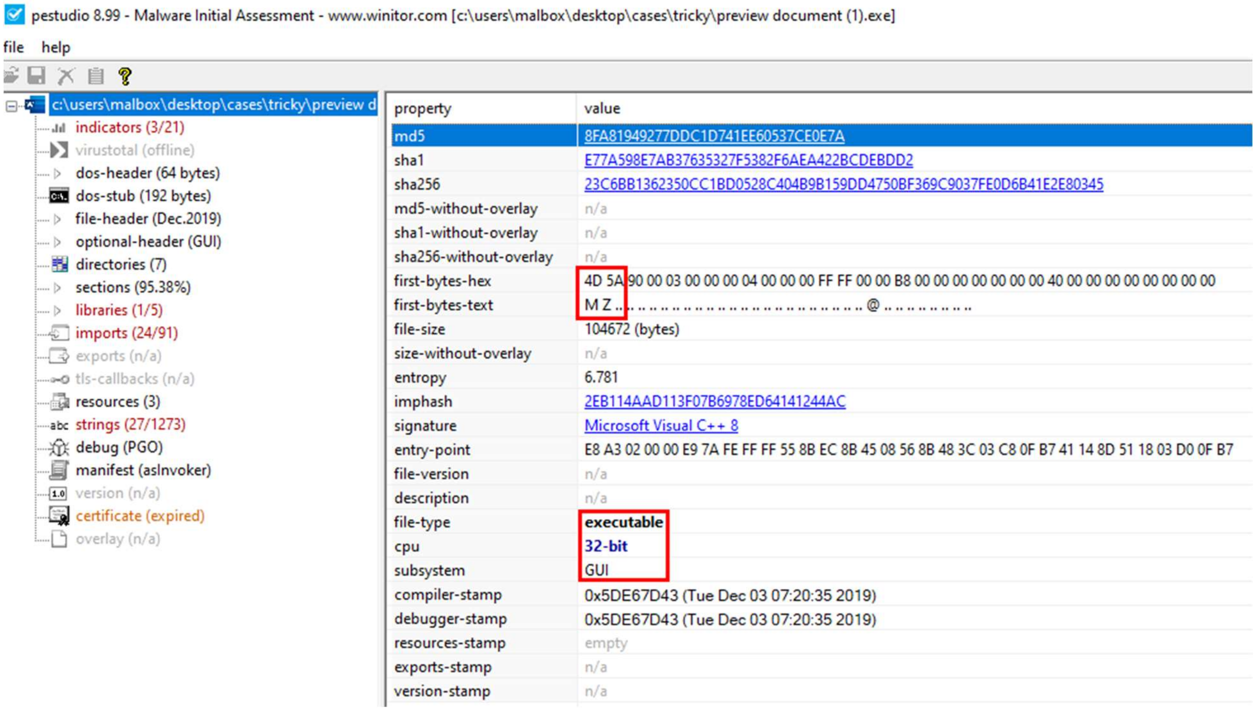
Contacted URLs

Scanned	Detections	URL
2019-12-04	1 / 72	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom/nYB45SPUEwQU5Z1ZMIJHWMys+ghUNoZ7OrUETfACEA/z5hY5qj0aEmX0H4s05bY=
2019-12-05	3 / 72	http://ajeetsinghbaddan.com/kjldfkdslvjf

Contacted Domains

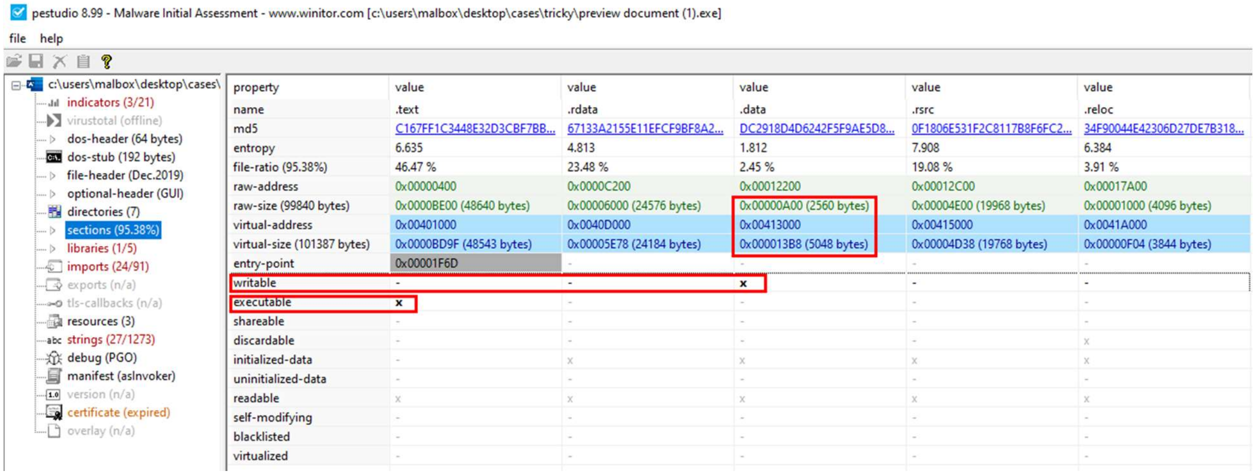
Created	Domain	Registrar
2013-01-15	www.ajeetsinghbaddan.com	GoDaddy.com, LLC
2013-01-15	ajeetsinghbaddan.com	GoDaddy.com, LLC
1996-12-02	ocsp.digicert.com	GoDaddy.com, LLC

Opened with pestudio to learn more about the design:



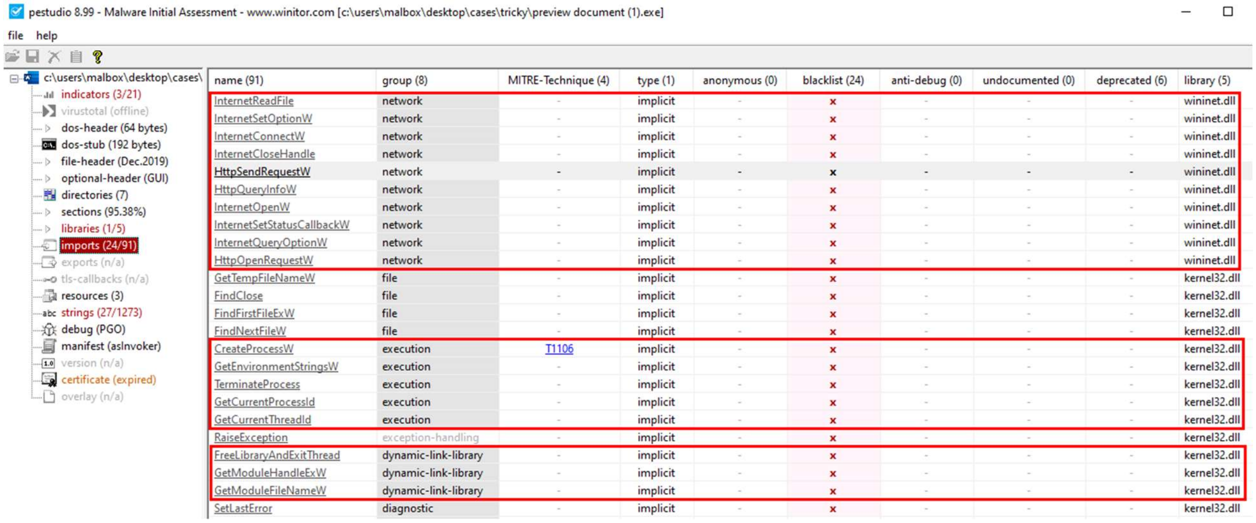
property	value
md5	8FA81949277DDC1D741EE60537CE0E7A
sha1	E77A598E7AB37635327F5382F6AEA422BCDEBDD2
sha256	23C6BB1362350CC1BD0528C404B9B159DD4750BF369C9037FE0D6B41E2E80345
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	104672 (bytes)
size-without-overlay	n/a
entropy	6.781
imphash	2EB114AAD113F07B6978ED64141244AC
signature	Microsoft Visual C++ 8
entry-point	E8 A3 02 00 00 E9 7A FE FF FF 55 8B EC 8B 45 08 56 8B 48 3C 03 C8 0F B7 41 14 8D 51 18 03 D0 0F B7
file-version	n/a
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x5DE67D43 (Tue Dec 03 07:20:35 2019)
debugger-stamp	0x5DE67D43 (Tue Dec 03 07:20:35 2019)
resources-stamp	empty
exports-stamp	n/a
version-stamp	n/a

The .data section sizes do not match, presumably to facilitate writing data:



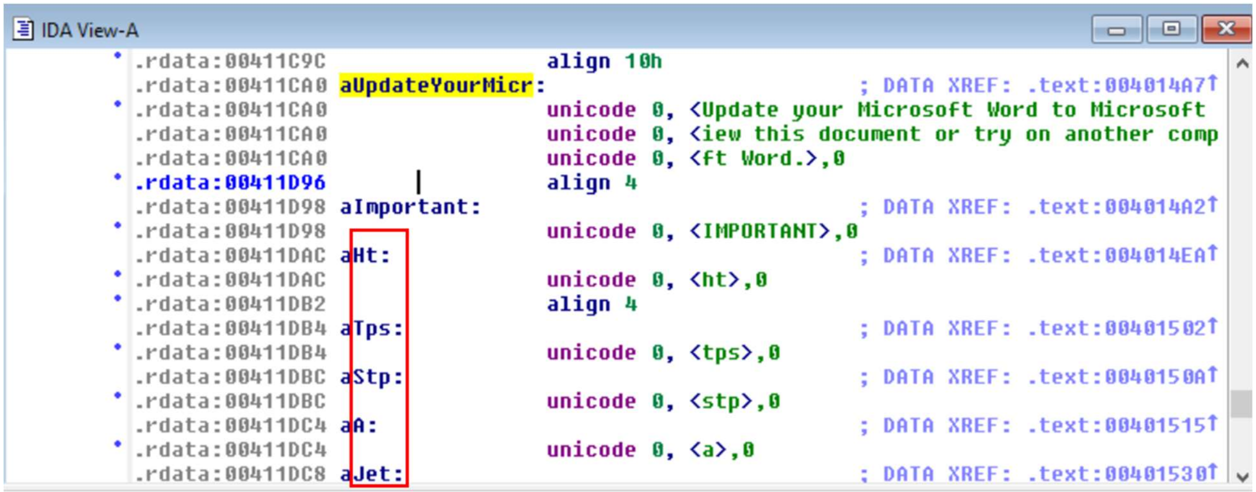
property	value	value	value	value	value
name	.text	.rdata	.data	.rsrc	.reloc
md5	C167FF1C3448E32D3CBF7BB...	67133A2155E11EFCF9BF8A2...	DC2918D4D6242F5F9AE5D8...	0F1806E531F2C8117B8F6FC2...	34F90044E42306D27DE7B318...
entropy	6.635	4.813	1.812	7.908	6.384
file-ratio (95.38%)	46.47 %	23.48 %	2.45 %	19.08 %	3.91 %
raw-address	0x00000400	0x0000C200	0x00012200	0x00012C00	0x00017A00
raw-size (99840 bytes)	0x0000BE00 (48640 bytes)	0x00006000 (24576 bytes)	0x00000A00 (2560 bytes)	0x00004E00 (19968 bytes)	0x00001000 (4096 bytes)
virtual-address	0x00401000	0x0040D000	0x00413000	0x00415000	0x0041A000
virtual-size (101387 bytes)	0x0000BD9F (48543 bytes)	0x00005E78 (24184 bytes)	0x000013B8 (5048 bytes)	0x00004D38 (19768 bytes)	0x00000F04 (3844 bytes)
entry-point	0x00001F6D	-	-	-	-
writable	-	-	x	-	-
executable	x	-	-	-	-
shareable	-	-	-	-	-
discardable	-	-	-	-	x
initialized-data	-	x	x	x	x
uninitialized-data	-	-	-	-	-
readable	x	x	x	x	x
self-modifying	-	-	-	-	-
blacklisted	-	-	-	-	-
virtualized	-	-	-	-	-

Possible browser hooking?

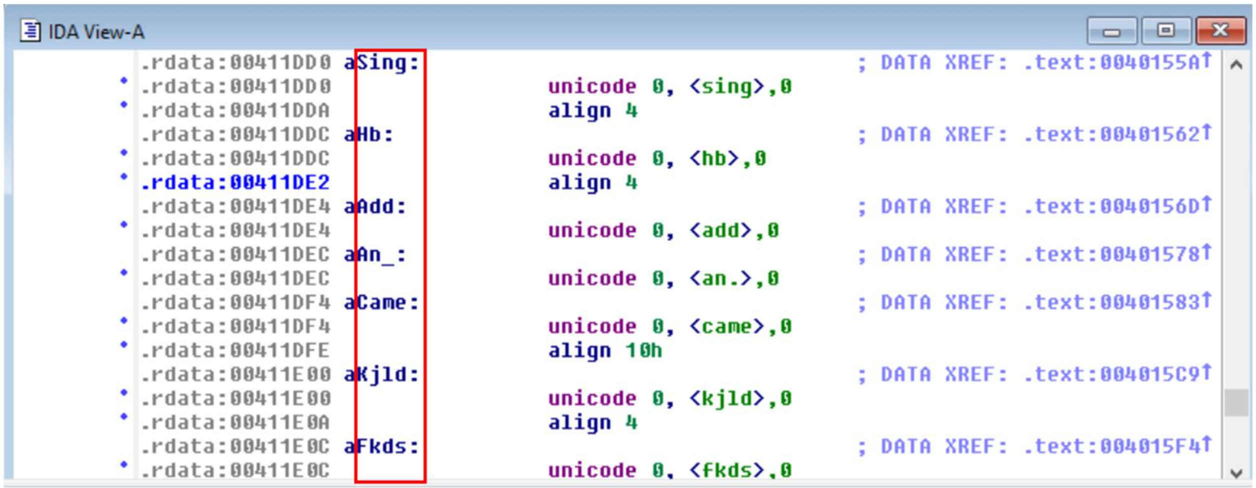


name (91)	group (8)	MITRE-Technique (4)	type (1)	anonymous (0)	blacklist (24)	anti-debug (0)	undocumented (0)	deprecated (6)	library (5)
InternetReadFile	network	-	implicit	-	x	-	-	-	wininet.dll
InternetSetOptionW	network	-	implicit	-	x	-	-	-	wininet.dll
InternetConnectW	network	-	implicit	-	x	-	-	-	wininet.dll
InternetCloseHandle	network	-	implicit	-	x	-	-	-	wininet.dll
HttpSendRequestW	network	-	implicit	-	x	-	-	-	wininet.dll
HttpQueryInfoW	network	-	implicit	-	x	-	-	-	wininet.dll
InternetOpenW	network	-	implicit	-	x	-	-	-	wininet.dll
InternetSetStatusCallbackW	network	-	implicit	-	x	-	-	-	wininet.dll
InternetQueryOptionW	network	-	implicit	-	x	-	-	-	wininet.dll
HttpOpenRequestW	network	-	implicit	-	x	-	-	-	wininet.dll
GetTempFileNameW	file	-	implicit	-	x	-	-	-	kernel32.dll
FindClose	file	-	implicit	-	x	-	-	-	kernel32.dll
FindFirstFileExW	file	-	implicit	-	x	-	-	-	kernel32.dll
FindNextFileW	file	-	implicit	-	x	-	-	-	kernel32.dll
CreateProcessW	execution	T1106	implicit	-	x	-	-	-	kernel32.dll
GetEnvironmentStringsW	execution	-	implicit	-	x	-	-	-	kernel32.dll
TerminateProcess	execution	-	implicit	-	x	-	-	-	kernel32.dll
GetCurrentProcessId	execution	-	implicit	-	x	-	-	-	kernel32.dll
GetCurrentThreadId	execution	-	implicit	-	x	-	-	-	kernel32.dll
RaiseException	exception-handling	-	implicit	-	x	-	-	-	kernel32.dll
FreeLibraryAndExitThread	dynamic-link-library	-	implicit	-	x	-	-	-	kernel32.dll
GetModuleHandleExW	dynamic-link-library	-	implicit	-	x	-	-	-	kernel32.dll
GetModuleFileNameW	dynamic-link-library	-	implicit	-	x	-	-	-	kernel32.dll
SetLastError	diagnostic	-	implicit	-	x	-	-	-	kernel32.dll

The payload address appears segmented to avoid detection:

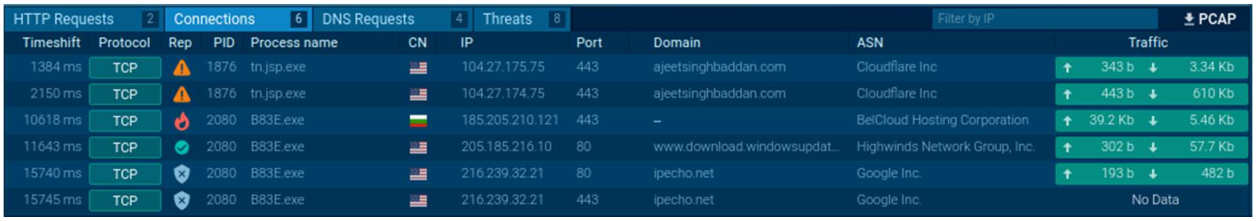


```
 .rdata:00411C9C                    align 10h
 .rdata:00411CA0 aUpdateYourMicr:                       ; DATA XREF: .text:004014A7↑
 .rdata:00411CA0                    unicode 0, <Update your Microsoft Word to Microsoft
 .rdata:00411CA0                    unicode 0, <iew this document or try on another comp
 .rdata:00411CA0                    unicode 0, <ft Word.>,0
 .rdata:00411D96                    align 4
 .rdata:00411D98 aImportant:                            ; DATA XREF: .text:004014A2↑
 .rdata:00411D98                    unicode 0, <IMPORTANT>,0
 .rdata:00411DAC aHt:                                   ; DATA XREF: .text:004014EA↑
 .rdata:00411DAC                    unicode 0, <ht>,0
 .rdata:00411DB2                    align 4
 .rdata:00411DB4 aTps:                                  ; DATA XREF: .text:00401502↑
 .rdata:00411DB4                    unicode 0, <tps>,0
 .rdata:00411DBC aStp:                                  ; DATA XREF: .text:0040150A↑
 .rdata:00411DBC                    unicode 0, <stp>,0
 .rdata:00411DC4 aA:                                    ; DATA XREF: .text:00401515↑
 .rdata:00411DC4                    unicode 0, <a>,0
 .rdata:00411DC8 aJet:                                  ; DATA XREF: .text:00401530↑
```



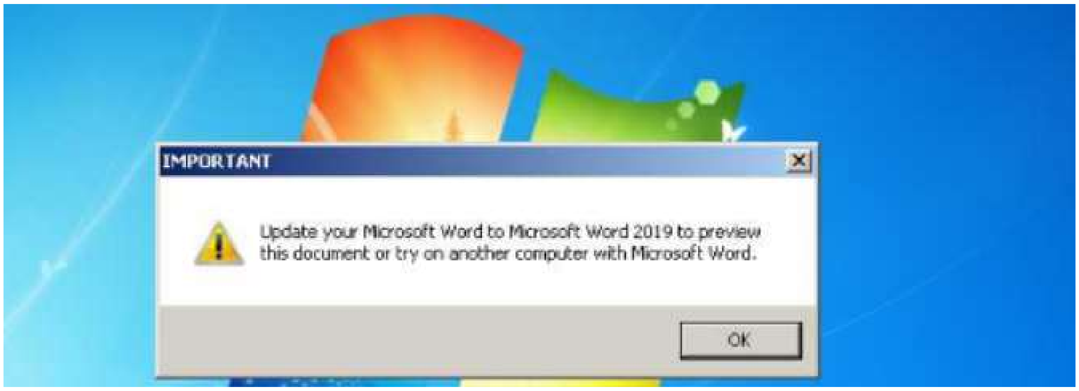
```
 .rdata:00411DD0 aSing:                                 ; DATA XREF: .text:0040155A↑
 .rdata:00411DD0                    unicode 0, <sing>,0
 .rdata:00411DDA                    align 4
 .rdata:00411DDC aHb:                                   ; DATA XREF: .text:00401562↑
 .rdata:00411DDC                    unicode 0, <hb>,0
 .rdata:00411DE2                    align 4
 .rdata:00411DE4 aAdd:                                  ; DATA XREF: .text:0040156D↑
 .rdata:00411DE4                    unicode 0, <add>,0
 .rdata:00411DEC aAn_:                                  ; DATA XREF: .text:00401578↑
 .rdata:00411DEC                    unicode 0, <an.>,0
 .rdata:00411DF4 aCame:                                 ; DATA XREF: .text:00401583↑
 .rdata:00411DF4                    unicode 0, <came>,0
 .rdata:00411DFE                    align 10h
 .rdata:00411E00 aKjld:                                 ; DATA XREF: .text:004015C9↑
 .rdata:00411E00                    unicode 0, <kjld>,0
 .rdata:00411E0A                    align 4
 .rdata:00411E0C aFkds:                                 ; DATA XREF: .text:004015F4↑
 .rdata:00411E0C                    unicode 0, <fkds>,0
```

Looking at behavior on a Windows 7 machine in Any.Run by a previous analysis for the same MD5 hash, we see downloading a second executable B83E.exe:



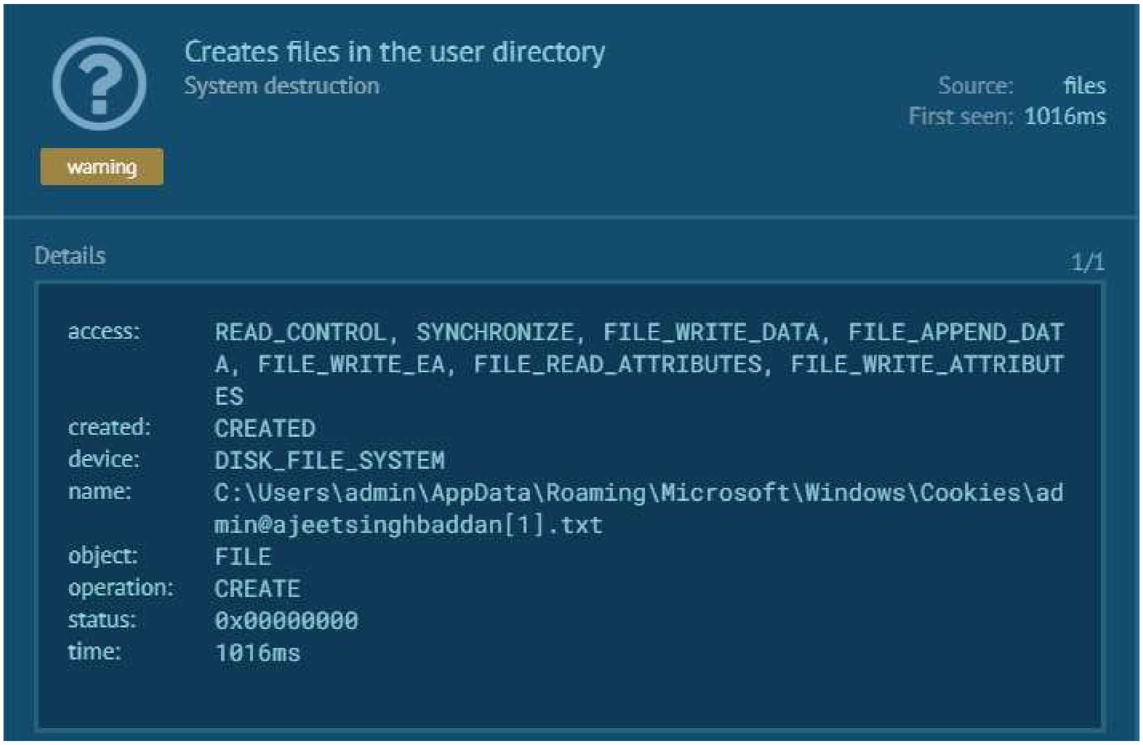
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
1384 ms	TCP	⚠	1876	tn.jsp.exe	🇺🇸	104.27.175.75	443	ajeetsinghbaddan.com	Cloudflare Inc	↑ 343 b ↓ 3.34 Kb
2150 ms	TCP	⚠	1876	tn.jsp.exe	🇺🇸	104.27.174.75	443	ajeetsinghbaddan.com	Cloudflare Inc	↑ 443 b ↓ 610 Kb
10618 ms	TCP	🔥	2080	B83E.exe	🇧🇬	185.205.210.121	443	–	BelCloud Hosting Corporation	↑ 39.2 Kb ↓ 5.46 Kb
11643 ms	TCP	✓	2080	B83E.exe	🇺🇸	205.185.216.10	80	www.download.windowsupdat...	Highwinds Network Group, Inc.	↑ 302 b ↓ 57.7 Kb
15740 ms	TCP	🛡	2080	B83E.exe	🇺🇸	216.239.32.21	80	ipecho.net	Google Inc.	↑ 193 b ↓ 482 b
15745 ms	TCP	🛡	2080	B83E.exe	🇺🇸	216.239.32.21	443	ipecho.net	Google Inc.	No Data

Again, the pop-up box is a distraction from the background processes launched by double-clicking the icon:



IMPORTANT

Update your Microsoft Word to Microsoft Word 2019 to preview this document or try on another computer with Microsoft Word.



Creates files in the user directory

System destruction

Source: files

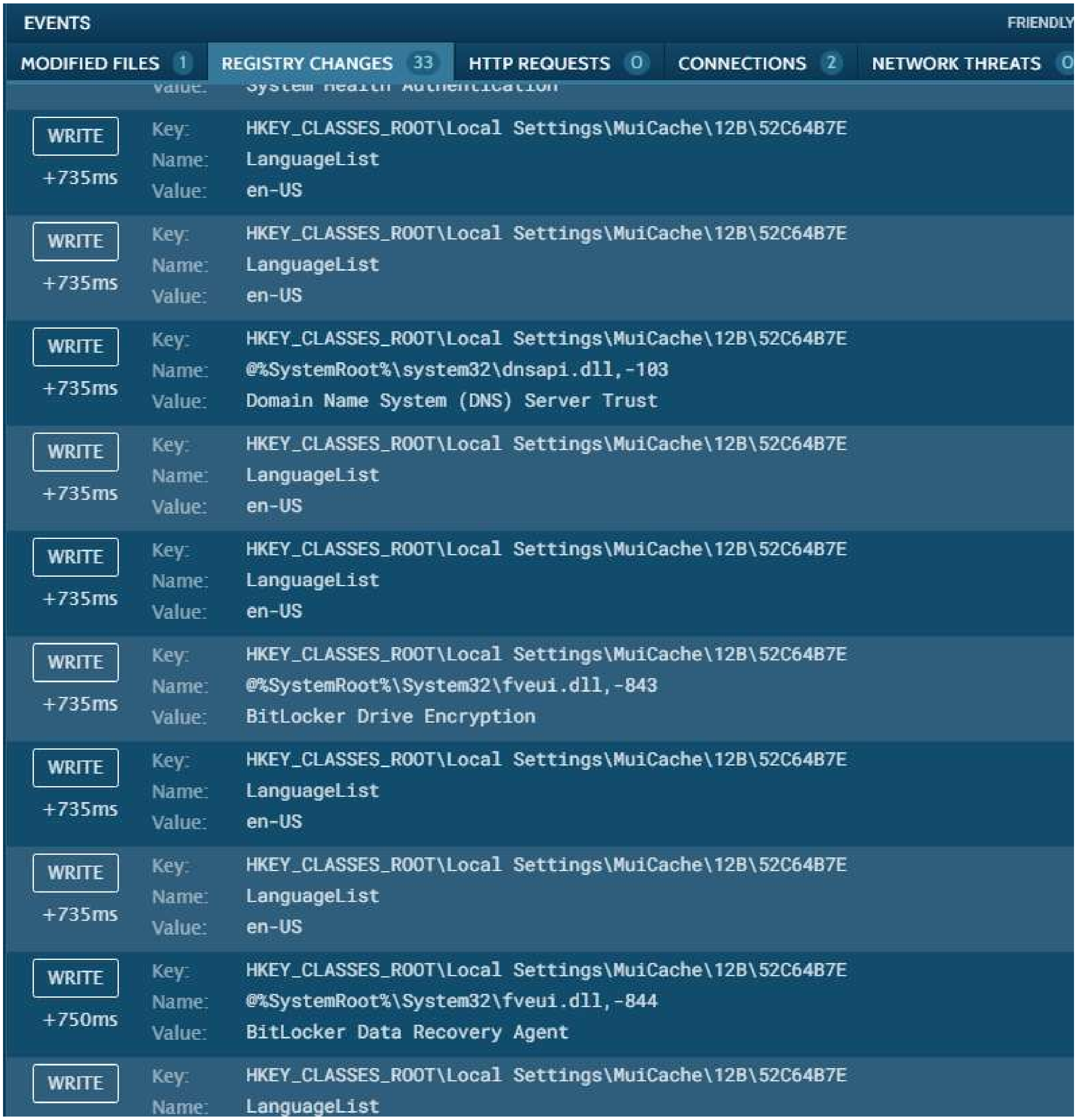
First seen: 1016ms

Details

1/1

```
access:     READ_CONTROL, SYNCHRONIZE, FILE_WRITE_DATA, FILE_APPEND_DAT
            A, FILE_WRITE_EA, FILE_READ_ATTRIBUTES, FILE_WRITE_ATTRIBUT
            ES
created:    CREATED
device:     DISK_FILE_SYSTEM
name:       C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\ad
            min@ajeetsinghbaddan[1].txt
object:     FILE
operation:  CREATE
status:     0x00000000
time:       1016ms
```

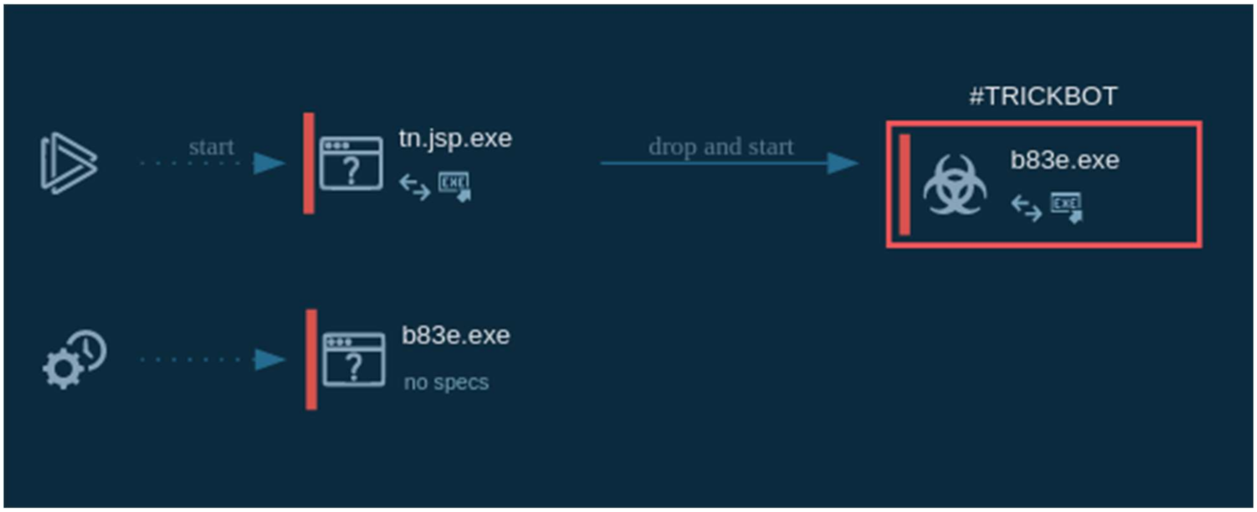
One set of registry changes seems to be performing a geo-locating function to determine the appropriate user interaction, perhaps even to call a payload more tailored for the environment:



```
         Value:  System Health Authentication
WRITE    Key:    HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E
         Name:   LanguageList
+735ms   Value:  en-US
WRITE    Key:    HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E
         Name:   LanguageList
+735ms   Value:  en-US
WRITE    Key:    HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E
         Name:   @%SystemRoot%\system32\dnsapi.dll,-103
+735ms   Value:  Domain Name System (DNS) Server Trust
WRITE    Key:    HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E
         Name:   LanguageList
+735ms   Value:  en-US
WRITE    Key:    HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E
         Name:   LanguageList
+735ms   Value:  en-US
WRITE    Key:    HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E
         Name:   @%SystemRoot%\System32\fveui.dll,-843
+735ms   Value:  BitLocker Drive Encryption
WRITE    Key:    HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E
         Name:   LanguageList
+735ms   Value:  en-US
WRITE    Key:    HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E
         Name:   LanguageList
+735ms   Value:  en-US
WRITE    Key:    HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E
         Name:   @%SystemRoot%\System32\fveui.dll,-844
+750ms   Value:  BitLocker Data Recovery Agent
WRITE    Key:    HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E
         Name:   LanguageList
```

THE PROCESS

According to Any.Run:



IOC SUMMARY

According to Any.Run:

Main object- "tn.jsp"

url hxxp://r20[.]rs6[.]net/tn.jsp?f=001Axp-rb1OUvD-HBDzYsE-
E44pINseNSuhttYlsDXbtvO22wIVLkCmHi3a-FSOAeE7LfkEnvgev5-
fbmNFlPO9tFBSP6TyQuve_ZHiXvOiymhOBBS7N_1Oao43whBrwZkLy5LdAWO8mkx2pJnC3cPq4zGom2uAEISh_zz-
ibKsglRTD1yKyXJWQ9C2lRg1N5u9S1gKQBx5cytv1vXZDOT9FN6wMzYejfHXeWJcorYcv3yKRW_-
47GxylYQZnoPHv4irVutz0-
Cwrfpf3L1vE2bf8D5HDHl3JYZSDIlMwYvIblvr4U6DLTT8J_Vmry8aM1e7PanzIzrjhDK7pud988dzWalNoMPm4HtyPgiqz
XuNea4Y9bZXzOaPbgtW8e3PXij&c=q2lrX5epVPMdjA15ck7PCyB67TEThDDawGl31SbU2WrT7nUvGW0ndw==&ch=
O0hclAUZ7bi81XMhCRO39WoMfD5ltid62SO_ksvJw9KV9shCoI_hcg==

sha256	23c6bb1362350cc1bd0528c404b9b159dd4750bf369c9037fe0d6b41e2e80345
sha1	e77a598e7ab37635327f5382f6aea422bcdebdd2
md5	8fa81949277ddc1d741ee60537ce0e7a

Dropped executable file

sha256 C:\Users\admin\AppData\Local\Temp\B83E.exe
ba46c4a7c5a10f375abef6148d8ece3ac1903041fdfeaa48221fdc033760319e

DNS requests

domain	www.ajeetsinghbaddan.com
domain	ajeetsinghbaddan.com
domain	ipecho.net

Connections

ip	104.27.175.75
ip	185.205.210.121
ip	104.27.174.75

HTTP/HTTPS requests

url	http://ipecho.net/plain

FINAL THOUGHTS

The next steps would involve a deeper behavioral analysis by detonation in a sand net where only a second virtual machine is routed with InetSim serving as the gateway and recorder. I would expect to find evidence of credential theft in an HTTP POST request to the Command and Control (C2) server over port(s) 443, 447, 448 or 449 using the TLS certificate found with pestudio for encryption.

CONTAINMENT ACTIONS/RECOMMENDATIONS

1. Isolate the host
2. Locate and remediate the initial attack vector (phishing email) and search+purge all related emails
3. Finalize the scope, beginning with the IOCs above
4. Set blocks and add/tune alerts based on IOCs
5. Collect host image for evidence and continued analysis
6. Re-image host with clean OS and reset user passwords
7. Final review of logs per user and host for the last 90 days to detect suspicious activity outbound, inbound or lateral.