Basic Dynamic Analysis Lab Solution and Guide TMPprovider038.dll

SHORT ANSWERS

Any interesting observations from basic static analysis?

The sample appears to be packed and/or obfuscated using a tool called VMProtect.

What do you observe this program doing through dynamic analysis?

The malware connects to fauxnet.mandiant.com and flossme.mandiant.com over port 80 using HTTP POST requests.

The malware copies itself to %TEMP%\TMProvider038.dll and sets itself for persistence at HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\TmProvider.

The malware also writes a GUID value to

"HKCU\Software\Microsoft\Internet Explorer\InternetRegistry\fertger".

The malware creates a file qln.dbx in the current user's Temp directory with an unknown constant "044"

List any potential host-based indicators of this malware.

The registry value HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\TmProvider

The registry value "HKCU\Software\Microsoft\Internet Explorer\InternetRegistry\fertger"

The copy location of %TEMP%\TMProvider038.dll

Creates a file qln.dbx in the user's Temp directory

List any potential network-based indicators of this malware.

fauxnet.mandiant.com:80 /wp08/wp-includes/dtcla.php

flossme.mandiant.com:80 /geo/productid.php

DETAILED ANALYSIS

Any interesting observations from basic static analysis?

Open the file in "*CFF Explorer*". There are suspicious anomalies that suggest packing. There are sections named .FLARE0 and .FLARE1. Five of the sections have "*Raw Size"* of 0 which suggests decoding/decompression at runtime.

Name	Virtual Size	Virtual Address	Raw Size
Byte[8]	Dword	Dword	Dword
.text	000136A7	00001000	0000000
.rdata	00007208	00015000	0000000
.data	00001330	0001D000	0000000
.gfids	000000A8	0001F000	0000000
.FLARE0	000C76CD	00020000	0000000
.FLARE1	001AA5B0	000E8000	001AA600
.reloc	000007F4	00293000	00000800
.rsrc	000001D5	00294000	00000200

Figure 1: Section headers indicate possible packing

Open the file in *PEiD* and *DIE* to investigate further. Both tools have multiple detection techniques. For *PEiD*, try the "*Hardcore Scan*". Unfortunately, no packer is detected with *PEiD*. *DIE* has additional rules you can select. Instead of using the "*Detect It Easy*" ruleset, try the "*Nauz File Detector*". When choosing this option, *DIE* successfully detects the *VMProtect* packer.

Scan Scrip	ts Log	ser/Desktop/Lab	syo1_basic Sta		meprovideroso.dii	
Type:	PE	Size: 17	50016	Entropy	FLC S H	
Export	Import	Resource	Overlay	.NET	PE	
EntryPoint:	001d87	/1d >		ImageBase:	1000000	
NumberOfSect	tions:	0008 >		SizeOfImage:	00295000	
Detect It Eas	şy					Options
Detect It Eas Nauz File De	Sy tector		Signatu	ires Info		Options About
Detect It Eas Nauz File De YARA	sy tector	u 70	Signatu	res Info > 31 ms	Scan	Options About Exit

VMProtect Software1 VMProtect Software CA

Dynamic analysis will be needed to analyze this obfuscated sample, since there is no tool available to easily deal with *VMProtect*.

What do you observe this program doing through dynamic analysis?

Prepare your dynamic analysis environment.

1. Open "*Process Monitor*" to capture Windows events during the malware execution. Stop capture and clear the output, then prepare filters. It is recommended to show *Operations* that include ProcessCreate, RegSetValue, WriteFile, and SetDispositionInformationFile. There are many approaches to filtering the events captured by "*Process Monitor*", so experiment with different workflows and use what works for you.

Process Monitor Display entries match Operation	Filter	SetDispositionInfor	mationFile 👻 then Include
Reset		,	Add Remove
Column	Relation	Value	Action
🔽 📀 Operation	is	Process Create	Include
🔽 📀 Operation	is	RegSetValue	Include
🔽 📀 Operation	is	WriteFile	Include
🔽 📀 Operation	is	Set Disposition Inf	Include
V Rocess N	is	Procmon.exe	Exclude
V 🐼 Process N	is	Procexp exe	Exclude
		ОК	Cancel Apply

Figure 3: Filter by Operation using "Process Monitor"

2. Open "Process Explorer" to observe running processes.

3. Open *FakeNet-NG* to simulate a network connection and capture network behavior. *FakeNet-NG* requires a connected network interface, so make sure you have a network interface set to "*Host Only*". This is configured by default within FLARE VM.

4. Open an Administrator Command Prompt and prepare to run the malware via the command line. This sample is a DLL so use the Windows utility rund1132.exe. Open "*CFF Explorer*" and examine the "*Export Directory*" so rund1132.exe can run an exported DLL function. The DLL has one export, RunD11Entry.

i 💫 📕 🔊	TMPprovider	38.dll							
	Member		Offs	Offset		Size		2	
File: TMPprovider038.dll	Characteristics		0003	6C90	Dwo	rd	00000	0000	
- E II Nt Headers	TimeDateStamp		0003	6C94	Dwo	rd	5A61	4BB6	
File Header	MajorVersion		0003	6C98	Wor	d	0000		
Data Directories [x]	MinorVersion		0003	6C9A	Wor	d	0000		
Section Headers [x] Front Directory	Name		0003	6C9C	Dword		0011E8CE		
- Control Directory	Base		0003	00036CA0 Dw		vord 0000		0001	
	NumberOfFunctions		00036CA4		Dword		0000001		
- Address Converter	NumberOfNam	es	00036CA8		Dword		0000001		
	AddressOfFunct	ions	0003	6CAC	Dwo	rd	0011	E8B8	
	Ordinal	Function F	RVA	Name Ord	inal	Name RVA		Name	
	N/A	00036CB8		00036CBC		00036CBE	-	00036CC2	
	(nFunctions)	Dword		Word	Dword		czAnci		
	00000001	00003180	0000			0011E8C2	RunDIIEntr		у

Figure 4: "Export Directory" shows a single export: RunDllEntry

Prepare the text to run the program on the command line, but do not run it until a VM snapshot has been taken.

Select Administrator: cmd.exe - Shortcut

C:\Users\user\Desktop\Labs\01_Basic Static and Dynamic>rundl132.exe TMPprovider038.dll, RunDllEntry_

Figure 5: Prepare to run the malware on the command line

5. Take a VM snapshot so the computer state can be restored after analysis is complete.

VM	Tabs Help 🛛 🗸	🕂 🖓 🚇	Ð		∠" ▼
() ©	Power Removable Devices Pause	> > Ctrl+Shift+P			
₽,	Send Ctrl+Alt+Del Grab Input	Ctrl+G		Taka Canada at	
чo	Capture Screen	Ctrl+Alt+PrtScn	49 (44	Revert to Snapshot: **CLEAN**	
B	Manage Reinstall VMware Tools	>	<u> </u>	Snapshot Manager 1 **CLEAN**	Ctrl+M 11/13/2020 10:26:53 AM
7	Settings	Ctrl+D			

Figure 6: Take a snapshot before running the malware

6. Turn on capturing within "Process Monitor" and press Enter on the Command Prompt to run the malware.

Analyze the captured data.

First wait a few seconds for the malware to execute. *FakeNet-NG* continually produces output, so it is advisable to close it shortly after malware behavior is captured, but before the output is filled with unrelated data. Click on the *FakeNet-NG* window and press CTRL-C to exit the program. You may need to press it twice. It is recommended to allow *FakeNet-NG* to complete the closing process and exit cleanly rather than forcing it closed – this way *FakeNet-NG* is more likely to restore changes it has made to Windows networking behavior.

Stop the capture in "Process Monitor".

FakeNet-NG output can be examined in the output window or by using the packet analysis tool *WireShark*. Sometimes Windows can produce a lot of network traffic and the output window can become filled – in those cases *WireShark* may be better. *FakeNet-NG* produces a packet capture file (.pcap) that contains traffic captured by *FakeNet-NG* (both before and after the packet is modified by *FakeNet-NG*). By default, the file is saved in the directory from which *FakeNet-NG* is run. FLARE VM may be configured to save the file in the directory C:\Users\user\Desktop\fakenet_logs if *FakeNet-NG* is run from the taskbar. *FakeNet-NG* is also configured to save a file for each HTTP request that is served by the application. Here is an example of what the directory listing can contain:



							×
C:\User	s\use	r\Desktop\fakenet_logs		✓ ✓ Search fall	kenet_logs		٩
Organize 🔻 🦳 O	Open	▼ Share with ▼ Print New folder			:==	•	0
🔆 Favorites	•	Name	Date modified	Туре	Size		
🧮 Desktop		http_20201023_170819.txt	10/23/2020 5:08 PM	Text Document	1 KB		
🐌 Downloads		http_20201023_170854.txt	10/23/2020 5:08 PM	Text Document	1 KB		
🗐 Recent Places	=	http_20201023_170923.txt	10/23/2020 5:09 PM	Text Document	1 KB		
J FLARE		http_20201023_171038.txt	10/23/2020 5:10 PM	Text Document	1 KB		
🐌 Utilities		http_20201023_171039.txt	10/23/2020 5:10 PM	Text Document	1 KB		
		http_20201023_171042.txt	10/23/2020 5:10 PM	Text Document	1 KB		
詞 Libraries		http_20201023_171046.txt	10/23/2020 5:10 PM	Text Document	1 KB		
Documents		http_20201023_171048.txt	10/23/2020 5:10 PM	Text Document	1 KB		
J Music		🔚 packets_20201023_170739.pcap	10/23/2020 5:10 PM	Wireshark capture	535 KB		
Pictures	-						
http_20201 Text Docum	1023 <u>.</u> nent	171038.txt Date modified: 10/23/2020 5:10 PM Size: 333 bytes	Date created: 10/2	3/2020 5:10 PM			

Figure 7: Fakenet-NG creates .txt files for captured HTTP requests

Try opening each of the .txt files to see if any HTTP traffic was captured. Most of them will likely be related to benign Windows activity, such as Online Certificate Status Protocol (OCSP) requests. These can be ignored as they are not generated by the malware.

iii http_20201023_171039.txt - Notepad		3
File Edit Format View Help		
POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/ocsp-request Accept: */* User-Agent: Microsoft-CryptoAPI/6.1 Content-Length: 83 Host: ocsp.digicert.com		*
0Q000M0K0I0 – +ぉ⊣⊣ 」qfþ¶;j£kÑ€H¿oGâ"•†ý–™」q–н⊾ё⊥gk¹ ≊X#Ì".ñÆeÒdŽ₁+дâ.»¦!чÖzêçf		Ŧ
	•	

Figure 8: Windows activity such as OCSP creates noise in Fakenet-NG output

FakeNet-NG should have captured HTTP traffic from the malware to flossme.mandiant.com.

http_20201023_171038.txt - Notepad		x
File Edit Format View Help		
POST /geo/productid.php?id=BE92941DA4Ac4Ac9BA38c6A4F3BBE1D7&v1=038&v2=261857261&q=5265882854508EFCF958F979E4 HTTP/1.1 User-Agent: Mozilla / 5.0 (Windows; U; Windows NT 6.1; en-US) ApplewebKit / 525.19 (KHTML, like Gecko) Chrome / 1.0.154.36 Safari / 52 Host: flossme.mandiant.com Content-Length: 0 Cache-Control: no-cache	25.19	4 III +
	ŀ	- _{ad}

Figure 9: HTTP POST request to C2 as captured by Fakenet-NG

If you are unable to observe HTTP requests this way, open the .pcap file in *WireShark*. *WireShark* is a powerful tool and there are many ways to approach traffic analysis. One way to examine HTTP traffic is to navigate to *File* – *"Export Objects"* – *HTTP*. Here you can see the malware requests grouped together, and you can click them to see the packets in the main window.

nideol.ir

📕 pa	ackets_2	2021021	9_0932	05.pcap														x
File	Edit	View	Go	Capture	Analyze	Sta	tistics	Telepl	nony	Wire	less	Tools	Help					
	Open				Ctrl+0		<u>۲</u>	₺ 📃		Ð,	Q. @	L 🔢						
	Open F	Recent				•										E	•	+
	Merge.							Destinatio	n			Protoco	Leng	jth	Info			
	Import	from H	lex Dui	mp				192.168	3.57.2	255		NBNS		96	Registrat	ion NB	F	
	Close				Ctrl+W			192.168	3.57.2	255		NBNS		96	Registrat	ion NB	F	
								192.168	3.57.2	255		NBNS		96	Registrat	ion NB	F	
	Save				Ctrl+S			192.168	3.57.2	255		NBNS		96	Registrat	ion NB	F	
	Save A	s			Ctrl+Shift+	S		192.168	5.5/.2	255		NBNS		96	Registrat	ion NB N	Ň	
	File Car							192.168	3.57.2	255		NBNS		78	Name quer	V NB TS	Δ	
	File Set					`		192.168	3.57.2	255		NBNS		78	Name quer	y NB IS	4	
	Export	Specifie	d Pacl	cets				127.255	5.255	. 255		NBNS		78	Name quer	v NB IS	4	-
	Export	Packet	Dissect	tions		۶.										4		
	Export	Packet	Bvtes		Ctrl+Shift+	x	96	bytes c	aptur	ed (768	bits)						-
	Export		File								_							=
	Export Export	TLC C	· · · · · ·				2.168	.57.130	, Dst	:: 19	2.16	8.57.25	5					
	Ехроп	TLS Ses	SION K	eys			, US	L POPL:	15/									Ŧ
	Export	Objects	;			•		DICOM	2	E٠	•`•q	•• ••••	· · 9 ·					
	Print				Ctrl+P		H	HTTP	0		9	·· ·L··	··)·					
						_	I	MF	6	CF.	FEGE	··· EGE	MEBF					
	Quit				Ctrl+Q		S	MB	∧ Ľ	AC	ACAC							
0050	00 0	20 00	01 00	0 04 93	e0 00 0	6 0	Т	FTP 🤇	2		• • • •		· · 9 ·					
							•	30										
0	💙 pa	ackets_2	02102:	19_093205	.pcap		\sim	Y		Pad	kets: :	2727 • Dis	played:	2727	7 (100.0%)	Profile: D	efault	

Wireshark · Export · HTTP object list										
Packet	Hostname	Content Type	Size	Filename						
1453	ctldl.windowsupdate.com	text/html	1410 bytes	disallowedcertstl.cab?f9f79f3e0b516276						
1492	fauxnet.mandiant.com	text/html	1410 bytes	dtcla.php?id=E47CDF6657B94EAAA04771ECD3CDE8DA&v1=	=					
493	fauxnet.mandiant.com	text/html	1410 bytes	dtcla.php?id=E47CDF6657B94EAAA04771ECD3CDE8DA&v1=	=					
1520	flossme.mandiant.com	text/html	1410 bytes	productid.php?id=E47CDF6657B94EAAA04771ECD3CDE8DA	a.					
1521	flossme.mandiant.com	text/html	1410 bytes	productid.php?id=E47CDF6657B94EAAA04771ECD3CDE8DA	ł.					
1554	crl.microsoft.com	application/pkix-crl	1410 bytes	microsoftrootcert.crl						

Figure 10: WireShark - export HTTP objects

Once you identify the HTTP packets, right click on one and choose *Follow – "TCP Stream"*. A text output of the requests is displayed.

No.	Time	Source	Destination	Protocol	Length Info					
+	1488 84.969000	192.168.57.130	192.168.57.130	TCP	57 80 → 3	1066 [PSH,	ACK]	Seq=1 Ack=343 W	lin=7680 Len=17 [T	CP segme.
	1489 84.969000	192.0.2.123	192.168.57.130	тср	57 80 → 3	1066 [PSH,	ACK]	Seq=1 Ack=343 W	lin=7680 Len=17 [T	CP segme.
 +	1490 84.969000	192.168.57.130	192.168.57.130	TCP	1500 80 → 3	1066 [PSH,	ACK]	Seq=18 Ack=343	Win=7680 Len=1460	[TCP_se.
	1491 84.969000	192.0.2.123	192.168.57.130	TCP	1500 80 → 3	1066 [PSH,	ACK]	Seq=18 Ack=343	Win=7680 Len=1460	[TCP_se.
-	1492 84.969000	192.168.57.130	192.168.57.130	· · · · · ·			· · · ·	xt/html)		
	1493 84.984000	192.0.2.123	192.168.57.130	Mark/Unm	ark Packet	Ctrl+M		xt/html)		
	1494 84.984000	192.168.57.130	192.168.57.130	Ignore/Uni	gnore Packet	Ctrl+D		Seq=1535 Ack=34	43 Win=7680 Len=0	
	1495 84.984000	192.0.2.123	192.168.57.130	Set/Unset T	ime Reference	Ctrl+T		Seq=1535 Ack=34	43 Win=7680 Len=0	
4				Time Chift		Ctol Shift	- I			•
				time shirt.	•	Ctri+Shirt+	'			
	Server: FakeNet/	1.3\r\n		Packet Con	nment	Ctrl+Alt+C				
	Date: Fri, 19 Fe	0 2021 14:33:34 GMI	,r \n	Edit Daraha	ad Manag					
	Content-Type: te	xt/ntml\r\n		Edit Resolve	ed Name					
	Content-Length:	1410\r\n		Apply as Fil	lter		- F			
		/1]		Deserve of Filter			.			
	[Time cince negu	/1] ost, 0.016000000.cos	onds 1	Prepare as i	Filter		·			
	[Poquest in from	est: 0.010000000 set	lonusj	Conversatio	on Filter		-			
	[Request In Iran	te: 1405	+ com/wn00/wn inc	Colorize Co	onversation		→	1 5 CD 2 CD 5 8 D 4 9 1 - 0 2 8 2 - 1 5 7001 6 6 1 9 - 5 2 6 5 8 9 2		
	Eile Data: 1410	bytes	re.com/wpob/wp-inc	SCTP			ъľ	LCCDSCDLODAdVI-0	56402-157651001ad	-52050020
⊳	Line-based text dat	a: text/html (37 lir	les)	5011			- C	TODO		
4	Eine basea eext aat	.u. cexe/itemi (5/ 11/		Follow			-	TCP Stream	Ctrl+Alt+Shift+1	-
				Conv			•	UDP Stream	Ctrl+Alt+Shift+U	
00	00 45 00 00 61 06	e5 40 00 80 06 00 0	0 c0 a8 39 82 E	сору				TLS Stream	Ctrl+Alt+Shift+S	
00	10 C0 88 39 82 00	50 04 2a 04 5a 30 a 00 00 00 3c 3f 63 3	6 d/ 9b e4 93	Protocol Pr	eferences		+	HTTD Stream	Ctrl+ Alt+ Shift+ H	
00	30 65 6d 61 69 6c	0a 3c 62 3e 46 61 6	b 65 4e 65 74 e	Decode Ar				ATTE Stedin	CULTAILTOURCET	
00	40 40 66 69 72 65	65 79 65 2e 63 6f 6	d 3c 2f 62 3e @	Decode As.				HTTP/2 Stream		
00	50 2e 0a 3c 2f 62	6f 64 79 3e 0a 3c 2	f 68 74 6d 6c .	Show Pack	et in New Windo	w		QUIC Stream		
00	60 3e		>				_			8

Wireshark · Follow TCP Stream (tcp.stream eq 49) · packets_20210219_093205.pcap
POST /wp08/wp-includes/dtcla.php?id=E47CDF6657B94EAAA004771ECD3CDE8DA&v1=038&v2=157091661&q=5265882854508EFCF958F979E4 HTTP/1.1
User-Agent: Mozilla / 5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit / 525.19 (KHTML, like Gecko) Chrome / 1.0.154.36 Safari / 525.19
Host: fauxnet.mandiant.com
Content-Length: 0
Cache-Control: no-cache
HTTP/1.0 200 OK
Server: FakeNet/1.3
Date: Fri, 19 Feb 2021 14:33:34 GMT
Content-Type: text/html
Content-Length: 1410

Figure 11: TCP stream displayed in WireShark

Observe that the malware makes two HTTP requests as follows:

POST /geo/productid.php?id=BE92941DA4AC4AC9BA38C6A4F3BBE1D7&v1=038&v2=261857261&q=5265882854508EFCF958F979E4 HTTP/1.1
User-Agent: Mozilla / 5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit / 525.19 (KHTML, like Gecko) Chrome / 1.0.154.36 Safari /
525.19
Host: flossme.mandiant.com
Content-Length: 0
Cache-Control: no-cache

POST /wp08/wp-includes/dtcla.php?id=BE92941DA4AC4AC9BA38C6A4F3BBE1D7&v1=038&v2=261857261&q=5265882854508EFCF958F979E4 HTTP/1.1
User-Agent: Mozilla / 5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit / 525.19 (KHTML, like Gecko) Chrome / 1.0.154.36 Safari /
525.19
Host: fauxnet.mandiant.com
Content-Length: 0
Cache-Control: no-cache

Now consider the "*Process Monitor*" output. Start by identifying the start of the process – you can ignore prior events. Although the malware file is named TMPprovider038.dll, the process of interest is rundll32.exe. rundll32.exe is responsible for loading the malicious DLL, which then runs within the context of the rundll32.exe process. Once you identify the start of the process, right click on it and choose "*Highlight 'rundll32.exe*".

3:58:0	dispython.exe	1260 🛃 WriteFile	C:\Users\u	ser\Desktop\fakenet_logs\packets_20201023_170739.pcap
3:58:0	rundll32	0010 88M - DI	- <u> </u>	er\AppData\Local\Temp\qln.dbx
3:58:0	nundli 32	Properties	Ctrl+P	er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Stack	Ctrl+K	er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	rundll32			er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Toggle Bookmark	Ctrl+B	er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	rundll32	Jump To	Ctrl+J	er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	rundll32	Carach Online		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	rundll32	Search Unline		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32			er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Include 'rundli32.exe'		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Exclude 'rundll32.exe'		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Little Kinke Income 1022 and		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Highlight rundli32.exe		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Copy 'rundll32.exe'		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32			er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Edit Filter 'rundll32.exe'		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32			er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Exclude Events Before		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Evolution Evolution Affra		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Exclude Events After		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Include		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Include		er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Exclude	•	er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32			er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli 32	Highlight	•	er\AppData\Local\Temp\TMPprovider038.dll
3:58:0	nundli32.exe		C. VOSers No	ser\AppData\Local\Temp\TMPprovider038.dll
2-50-0	Devedll 22 even	201C 🛄 Weto Ello	C:\Ulaam\u	aar\AapData\Laad\Zamp\TMParavidar029.dll

Figure 12: Highlight events produced by process named rundll32.exe•

Now the output is limited to the filtered events, and only the process of interest is highlighted.

				*	
3:58:0	nundli32.exe	2916 💀 WriteFile	C:\Users\user\AppData\Local\Temp\aln.dbx	SUCCESS	Offset: 0. Length: 3. Priority: Normal
3:58:0	Jundi 32 exe	2916 WriteFile	C:\leen\user\AppData\local\Temp\TMPprovider038.dl	SUCCESS	Offset: 0 Length: 65.536 Priority: Normal
3-58-0	nundli32 eve	2916 WriteFile	C \lears\ueer\ueer\ueer\ueer\ueer\ueer\ueer\ue	SUCCESS	Offset: 65 Sign Length: 65 Sig
2.59.0	Devodi 22 ono	2010 Weeple	C (Lase) (and C polar Lase) (Tame) (M Particle (22) dl	0000200	Offent: 10,000, Length: CE 520
3.50.0	Junui 32.exe	2010 0 Wa-Di-	C. Ausers user Applear action of the provide USA and the Control of the Control o	0000200	Offset 10 (072) being in 60,000
3:56:0	Inunali32.exe	2010 Witterlie	C:\usersuserveppuera\useruserveppuera\useruseruseruse.cii	SUCCESS	Offset: 136,600, Length: 65,536
3:58:0	rundli32.exe	2916 WriteHie	C:\Users\user\v\$ppData\Local\Temp\TMPproviderU38.dll	SUCCESS	Ottset: 262,144, Length: 65,536
3:58:0	rundli32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 327,680, Length: 65,536
3:58:0	lrundli32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 393,216, Length: 65,536
3:58:0	rundli32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 458,752, Length: 65,536
3:58:0	🕅 rundi 32.exe	2916 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dl	SUCCESS	Offset: 524,288, Length: 65,536
3:58:0	rundli32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 589.824, Length: 65.536
3:58:0	Trundl32.exe	2916 😽 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 655.360. Length: 65.536
3:58:0	Inundli32.exe	2916 KWriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 720.896, Length; 65.536
3.58.0	Daundli32 eve	2916 WriteBle	C/Users/user/AppData/Local/Temp/TMPppy/der038.dl	SUCCESS	Offset: 786.432 Length: 65.536
3-58-0	andl32 eve	2916 WeeFle	Cillear (ura) App Data) and Tamp TMPprovider038 dl	SUCCESS	Offent: 851 952 Length: 65 536
3-59-0	andi 32 ere	2916 Witte File	C \Lear \uer \uer \uer \uer \uer \uer \uer \ue	SUCCESS	Offset 917 504 Length 65 526
2.50.0	Deventil 22 even	2010 10400	C. (Jaka wat vyposta taka himpi nin protosta (20 al.	SUCCESS	Official OFFICIAL DESIGN
3.36.0	unui sz.exe	2310 Wittenie	C. Weers user oppoala (boat fremp rime provider 030 m	3000E33	Oriset, 303,040,570,80,030
3:58:0	undi 32.exe	2916 Store File	C:\Users\user\user\user\user\user\user\user\	SUCLESS	Offset: 1,048,576, Length: 55,535
3:58:0	rundi 32.exe	2916 Vinterile	C:/Users/user/AppData/Local/Temp/TMPproviderU38.dll	SUCCESS	Uffset: 1,114,112, Length: 65,536
3:58:0	lrundli32.exe	2916 KWriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 1,179,648, Length: 65,536
3:58:0	lrundli32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 1,245,184, Length: 65,536
3:58:0	Inundli32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 1,310,720, Length: 65,536
3:58:0	nundli32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 1,376,256, Length: 65,536
3:58:0	nundli32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 1,441,792, Length: 65,536
3:58:0	Inundl32.exe	2916 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dll	SUCCESS	Offset: 1.507.328, Length: 65.536
3-58-0	Jundi 32 exe	2916 WriteFile	C:\Users\user\AppData\Local\Temp\TMPprovider038.dl	SUCCESS	Offset: 1 572 864 Length: 65 536
3-58-0	andi32 eve	2916 WriteFile	C \lears\user\user\user\user\user\user\user\us	SUCCESS	Offset 1 638 400 Length 65 536
2-59-0	Daundi 22 owo	2016 Witte Fla	C (Lange) uned (applicate Lange) The period of Q2 dl	0000200	Offent: 1 702 926 Length: 46 090
2.59.0	Jandi 32.exe	2016 Pag SatValue	C. Coests Goest Oppoals (Coest (Temp) (Temp) (Coest) (Coust)	0000233	Contest: 17703/030 (2019) 149/000 Times and 22 C/Ulana (unar) Ann Data (Lana) Tama (TMPana) dar 029 dll. Pun Difference Times (2019) 149/000 dll. Pun Difference (2019) 149/0000 dll. Pun Difference (2019) 149/0
3.50.0	Junui 32.exe	2010 Progetvalue	Incol convale vincosit vincosit cone i vestori va fina da se	0000200	Type: NEC_52, being in: 140, base intributes c. tosets opposed storage the provide usauli, humble by Type: DEC_52, being introduced by the storage storage being storage by the storage b
3:58:0	Inunali32.exe	2016 Manager Value	HIGLU Software Wicrosoft Unternet Explorer Unternet Registry Vetger	SUCCESS	Type: REG_32, Length: 66, Data: 43633EATATEP40C2AE02E36CA52F233E
3:58:0	unali32.exe	2916 RegSet value	HKLM/SOFTWARE/Wow6432Node/Microsoft/Tracing/VundI32_HASAP132/EnableFile Tracing	SUCCESS	Type: REG_DWORD, Lengin: 4, Data: 0
3:58:0	rundli32.exe	2916 RegSetValue	HKLM/SOFTWARE/Wow6432Node/Microsoft/Tracing/rundl32_RASAPI32/EnableConsole Tracing	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3:58:0	nundli32.exe	2916 🚉 RegSet Value	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\FileTracingMask	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294901760
3:58:0	rundli32.exe	2916 🕰 RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\ConsoleTracingMask	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294901760
3:58:0	rundli32.exe	2916 🍂 RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundlI32_RASAPI32\MaxFileSize	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1048576
3:58:0	rundli32.exe	2916 KRegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\FileDirectory	SUCCESS	Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\tracing
3:58:0	Inundl32.exe	2916 🍂 RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundli32_RASMANCS\EnableFileTracing	SUCCESS	Type: REG_DWORD, Length; 4, Data; 0
3:58:0	Inundli 32.exe	2916 KReoSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundl32 RASMANCS\EnableConsoleTracing	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3.58.0	Daundli32 eve	2916 RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\nundl32_RASMANCS\FileTracingMask	SUCCESS	Type: REG_DWORD_Length: 4_Data; 4294901760
3-58-0	andi32 exe	2916 RegSetValue	HKI M\SOFTWARE\Wow6432Node\Microsoft\Tracing\nundl32_RASMANCS\Copsole_Tracing/Mask	SUCCESS	Type: BEG_DWORD_Length: 4_Data; 4294901760
3-58-0	Daundi 32 erre	2916 RegSetValue	HKI M\SOFTWARE\Wow6432Node\Microsoft\Tracing\nupdl32_RASMANCS\MaxFieSze	SUCCESS	Type: REG_DWORD_Length: 4_Data: 1048576
2-59-0	Davodi 22.000	2016 PagSetValue	LKI NO SOFTWARE Way 622Neds Microsoft Tracing and 22 DASMANCS File Directory	CHOCESS	Tues DEC EVPAND S7 Length 14 Date (winds)/traine
3.50.0	Deventil 22 even	2010 ResCallaba	TREE CONTRACT WATE WORKSTRONG INCOMENTATION IN THE REPORT OF STRUCTURE CONTRACT IN THE REPORT OF STRUCTURE AND A S	0000200	Type, NEC_DWORD_Leads A Date 0
3.56.0	fundi 32.exe	2010 M DesCalValue	HIGO Software Villorosoft Winnows (Current Version Vitemet, Settings Viroxy Enable	3000233	Type: REG_DWORD, Length: 4, Data: 0
3.58.0	Inunaii32.exe	2010 RegSetValue	Incluis Software vincrosoft vinndows vulnent version vintemet. Settings VLonnections SavedLegacySettings	SULLESS	Type: TEC4_DIMART, Length: boo, bata: 40 00 00 00 00 00 00 00 00 00 00 00 00
3:58:0	rundli32.exe	2916 MagSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet_Settings\ZoneMap\UNCAsintranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3:58:0	rundli32.exe	2916 KRegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
3:58:0	lrundli32.exe	2916 KRegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3:58:0	rundli32.exe	2916 KRegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
3:58:0	🔁 python.exe	1260 🛃 WriteFile	C:\Users\user\Desktop\Vakenet_logs\http_20201027_155806.bt	SUCCESS	Offset: 0, Length: 342, Priority: Normal
3:58:0	🔁 python.exe	1260 🛃 WriteFile	C:\Users\user\Desktop\fakenet_logs\packets_20201023_170739.pcap	SUCCESS	Offset: 331,776, Length: 4,096
3:58:0	rundli32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\H0XUCTQ0\dtcla11	ntm SUCCESS	Offset: 0, Length: 1,023, Priority: Normal
3:58:0	Trundli 32.exe	2916 WriteFile	C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\H0XUCTQ0\dtcla[1]	ntm SUCCESS	Offset: 1.023. Length: 387
3:58:0	ovthon.exe	1260 WriteFile	C:\Users\user\Desktop\fakenet_logs\http_20201027_155806.bt	SUCCESS	Offset: 0. Lenoth: 333. Priority: Normal
3.58.0	avthon exe	1260 WriteFile	C\Lisers\user\Desktop\fakenet_logs\packets_20201023_170739.pcap	SUCCESS	Offset: 335.872 Length: 4.096
3-58-0	andl32 exe	2916 WriteFile	C\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Context IE5\5\IC9EE1M\vanducti	(1) htm success	Offset: 0 Length 1023 Priority: Normal
2-59-0	Dandil 22 and	2016 Witte File	C\lear\use\AppDate\Local\Microsoft\Mindows\Temporary Internet Files\Context IE5\5\/C9EE1M\product	5000E55	Offsat: 1 023 Laost 297
3.30.0	initialities in the	2010 WALKELING	 C. Yoaka waa Advard Yorka Andra Advard Adv Advard Advard Adva Advard Advard Adva	success	viraet, i,vev, tenger, 307

Figure 13: Highlighted output makes malware activity easier to recognize

The first interesting event is a WriteFile operation to C:\Users\user\AppData\Local\Temp\qln.dbx. Double click on the event to view more details.

🗐 Event Propertie	'S	
Event Process	Stack	
Date:	10/26/2020 10:10:34.2042372 AM	
Thread:	884	
Class:	File System	
Operation:	WriteFile	
Result:	SUCCESS	
Path:	C: \Users \user \AppData \Local \Temp \qln.dbx	
Duration:	0.0000233	
	<u> </u>	
Length:	3	*
Priority:	Normal	

Figure 14: Event details for WriteFile operation

The length of the operation is only 3 bytes. Close this window, right click on the event, and choose "*Jump To....*" This takes you to the file location in "*File Explorer*".

			2					
Search Temp								
Organize 👻 📄 Open	Share with 🔻 New folder		Y					0
🔆 Favorites	Name	Date modified	Туре	Size				
🧮 Desktop	퉬 4CA43513-F817-4809-AB17-076588E14365	7/31/2020 3:11 PM	File folder					
🐌 Downloads	9D917D93-A8AE-4031-9A3C-6F0F722C5F	7/31/2020 3:08 PM	File folder					
🔛 Recent Places	🐌 ConEmu	10/23/2020 5:08 PM	File folder					
퉬 FLARE	preprocessor	7/31/2020 2:11 PM	File folder					
퉬 Utilities	Vmware-user	7/31/2020 1:51 PM	File folder					
	🕋 -1436953092.xml	10/16/2018 5:09 PM	XML Document	2,033 KB				
🧊 Libraries	FXSAPIDebugLogFile.txt	5/20/2020 12:32 AM	Text Document	0 KB				
Documents	📄 git_version.txt	10/23/2020 5:08 PM	Text Document	1 KB				
🁌 Music	😂 Procmonб4.exe	10/23/2020 5:06 PM	Application	1,150 KB				
Pictures	📄 qln.dbx	10/26/2020 10:10	DBX File	1 KB				
Videos	TMPprovider038.dll	5/28/2019 8:15 PM	Application extens	1,709 KB				
	🛃 user.bmp	7/31/2020 3:09 PM	Bitmap image	32 KB				
📜 Computer	💯 ZoomIt64.exe	8/16/2020 5:47 AM	Application	575 KB				
🗣 Network								

Figure 15: "File Explorer" displays dropped files

Open the file in "010 Editor" to view the contents. The text is 044.

🍛 010 Editor - C:\Users\user\AppData\Local\Temp\qln.dbx													
File	Edit	Search	View	Format	Scripts	Templa	ates	Debug	Tools	Win	dow	He	р
) ~ 🔁		0	þ 🖞	s، ا	b b	5	C	<u>,</u>	5	⇒	Ą	1 👌
Sta ∓	rtup Edit As:	qln.dbx Text∨	× Run Sci	ipt∨ S	Syntax 🗸								
	0	44					•						

Figure 16: Examine file contents with "010 Editor"

At this point there is not enough information to understand the purpose of this file, but it can be recorded as a hostbased indicator. Continue analyzing the "*Process Monitor*" output. Next there is a sequence of WriteFile operations to C:\Users\user\AppData\Local\Temp\TMPprovider038.dll. Right click and choose "*Jump To....*" to view the file. Often malware will copy itself into a common directory in order to blend in with Windows system files. C:\Users\user\AppData\Local\Temp\ is likely the Windows Environment Variable %TEMP%. Compare the hash of the new file to the original in order to confirm this theory.

C:\Users\user\Desktop\Labs\01_Basic Static and Dynamic> <mark>sigcheck -h TMPprovider038.dll</mark>							
Sigcheck v2.73 - File version and signature viewer							
Conuright (C) 2004-2019 Mark Russinguich							
Susinternals – www.susinternals.com							
C:\Users\user\Deskton\Labs\01 Basic Static and Dunamic\TMPnopuider038 d]]:							
levified: Insigned							
MD5 - 713111BF923A04567B9928C7598105FB8							
SH01 - 68461 FEB9F1 335678EC72999065E061 BE03CE554E							
1 E3101 - E1-070 70702 (1-3770) 707 70702 01 E700 7 E909 20 EF 20 20 20 20 20 20 20 20 20 20 20 20 20							
$\frac{1}{1}$							
THE STOLESZZYCHYZELGTONTYGYCTY2424							
C:\Users\user\Desktop\Labs\01_Basic_Static_and_Dunamic>sigcheck_h_C:\Users\user\AppData\Local\Temp\TMPprovider038.dll							
Sigcheck v2.73 - File version and signature viewer							
Copyright (C) 2004-2019 Mark Russinovich							
Sysinternals - www.sysinternals.com							
c:\users\user\appdata\local\temp\TMPprovider038.dll:							
Verified: Unsigned							
Link date: 8:36 PM 1/18/2018							
Publisher: n/a							
Company: n/a							
Description: n/a							
Product: n/a							
Prod version: n/a							
File version: n/a							
MachineType: 32-bit							
MD5: 713111BF1249A567B9928C75901A5FB8							
SHA1: 68461EFB9E133567BFC77990A5F061BE03CF554E							
PESHA1: EB469A7DFC0291457F39407790C982C4BBF1FCA7							
PE256: 82777261C3CAAE9F9676F90DC7F2A1F02B8AAFF0B2A58CA4D175445AA6D62F2A							
SHA256: 98744AFC621B0A96034E6A4970110E6114A8405AA6DE5DF4268B8A022DEA4C5C							
IMP: 346E55297EA79E1C1F6919C96F942424							

Figure 17: sigcheck is used to compare file hashes and verify dropped file is identical to original sample

Now that it has been confirmed, continue to analyze the "*Process Monitor*" output. The next interesting event is a RegSetValue operation with path HKCU\Software\Microsoft\Windows\CurrentVersion\Run\TmProvider.



Double click to see the details and observe that the data written to that registry value is "rundll32 C:\Users\user\AppData\Local\Temp\TMPprovider038.dll, RunDllEntry". The registry subkey HKCU\Software\Microsoft\Windows\CurrentVersion\Run is used to register programs to run automatically on system start. In this case rundll32 is used to launch the DLL export RunDllEntry, establishing persistence on the host. Note this as another host-based indicator.

2	Event Propertie	s 🗖 🗖	×
ſ	Event Process	Stack	
	Date:	10/27/2020 3:58:06.7164081 PM	
	Thread:	2528	
	Class:	Registry	
	Operation:	RegSetValue	
	Result:	SUCCESS	
	Path:	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\TmProvider	
	Duration:	0.0001343	
	Type: Length: Data:	REG_SZ 148 rundll32 C:\Users\user\AppData\Local\Temp\TMPprovider038.dll, RunDllEntry	

Figure 18: Persistence is achieved via registry

The next interesting event is another RegSetValue operation with value "HKCU\Software\Microsoft\Internet Explorer\InternetRegistry\fertger". Double click to see details and observe the data written is a hexadecimal string 49839EA1A1EF40C2AE02E9BCA52F259E. At this point there is insufficient data to understand the purpose of this behavior, however this registry key should be documented as a potential host-based indicator.

😂 Ev	vent Propertie	5	- • •
Ev	vent Process	Stack	
	Date:	10/27/2020 3:58:06.7167907 PM	
Т	Thread:	2528	
0	Class:	Registry	
0	Operation:	RegSetValue	
R	Result:	SUCCESS	
P	Path:	HKCU\Software\Microsoft\Internet Explorer\InternetRegistry\fertger	
	Ouration:	0.0000685	
	Type: Length: Data:	REG_SZ 66 49839EA 1A 1EF40C2AE02E9BCA52F259E	*

Figure 19: Unknown hexadecimal string written to fertger registry subkey



The remaining "*Process Monitor*" output is less relevant to our malware analysis tools. The RegSetValue operations to HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing and

"HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings" are common behavior related to the Windows internet API. The WriteFile operations to

"C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files" are related to caching web requests. These can all be ignored.

3:58:0	rundli32.exe	2916 KegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\vundli32_RASAPI32\EnableFile fracing	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3:58:0	rundl32.exe	2916 🍂 RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\EnableConsoleTracing	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3:58:0	rundl32.exe	2916 KRegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundl32_RASAP132\FileTracingMask	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294901760
3:58:0	rundl32.exe	2916 式 RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\ConsoleTracingMask	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294901760
3:58:0	rundl32.exe	2916 KRegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\MaxFileSize	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1048576
3:58:0	Inundl 32.exe	2916 KRegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\vundll32 RASAPI32\FileDirectory	SUCCESS	Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\tracing
3:58:0	Trundl 32.exe	2916 RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASMANCS\EnableFileTracing	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3:58:0	Inundl32.exe	2916 RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASMANCS\EnableConsoleTracing	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3:58:0	Trundl 32.exe	2916 RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\vundll32_RASMANCS\FileTracingMask	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294901760
3:58:0	Inundl 32.exe	2916 KRegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\vundll32_RASMANCS\ConsoleTracingMask	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294901760
3:58:0	Inundl 32.exe	2916 KRegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\vundll32_RASMANCS\MaxFileSize	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1048576
3:58:0	rundl 32.exe	2916 RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASMANCS\FileDirectory	SUCCESS	Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\tracing
3:58:0	Trundl32.exe	2916 RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3:58:0	Trundl 32.exe	2916 RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacvSettings	SUCCESS	Type: REG_BINARY, Length: 568, Data: 46 00 00 00 19 00 00 00 09 00 00 00 00 00 00 00 00
3:58:0	Inundl 32.exe	2916 KRegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3:58:0	rundl 32.exe	2916 KRegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
3:58:0	rundl 32.exe	2916 RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
3:58:0	Trundl 32.exe	2916 RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
3:58:0	python.exe	1260 WriteFile	C:\Users\user\Desktop\fakenet_logs\http_20201027_155806.bt	SUCCESS	Offset: 0. Length: 342. Priority: Normal
3:58:0	python.exe	1260 🔜 WriteFile	C:\Users\user\Desktop\fakenet_logs\packets_20201023_170739.pcap	SUCCESS	Offset: 331,776, Length: 4,096
3:58:0	rundl32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\H0XUCTQ0\dtcla[1].htm	SUCCESS	Offset: 0, Length: 1,023, Priority: Normal
3:58:0	Trundl 32.exe	2916 - WriteFile	C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\H0XUCTQ0\dtcla111.htm	SUCCESS	Offset: 1.023. Length: 387
3:58:0	python.exe	1260 WriteFile	C:\Users\user\Desktop\fakenet_logs\http_20201027_155806.bt	SUCCESS	Offset: 0, Length: 333, Priority: Normal
3:58:0	python.exe	1260 🔜 WriteFile	C:\Users\user\Desktop\fakenet_logs\packets_20201023_170739.pcap	SUCCESS	Offset: 335,872, Length: 4,096
3:58:0	rundl32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5VC9FE1M\productid[1].htm	SUCCESS	Offset: 0, Length: 1,023, Priority: Normal
3:58:0	rundl 32.exe	2916 🛃 WriteFile	C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5VC9FE1M\productid[1].htm	SUCCESS	Offset: 1,023, Length: 387

Figure 20: "Process Monitor" captures events related to caching web requests

List any potential host-based indicators of this malware.

Referring to the above analysis, the host-based indicators are:

The file C:\Users\user\AppData\Local\Temp\qln.dbx is created and populated with the string 044.

The malware is copied to C:\Users\user\AppData\Local\Temp\TMPprovider038.dll.

The registry value HKCU\Software\Microsoft\Windows\CurrentVersion\Run\TmProvider is set to "C:\Users\user\AppData\Local\Temp\TMPprovider038.dll, RunDllEntry"

The registry value "HKCU\Software\Microsoft\Internet Explorer\InternetRegistry\fertger" is set to "49839EA1A1EF40C2AE02E9BCA52F259E"

List any potential network-based indicators of this malware

Referring to the above analysis, the host-based indicators are:

Two variant HTTP POST requests are made.

- flossme.mandiant.com on port 80. The query string is /geo/productid.php?id=BE92941DA4AC4AC9BA38C6A4F3BBE1D7&v1=038&v2=261857261&q=52658828 54508EFCF958F979E4.
- 2. fauxnet.mandiant.com on port 80. The query string is /wp08/wpincludes/dtcla.php?id=BE92941DA4AC4AC9BA38C6A4F3BBE1D7&v1=038&v2=261857261&q=52658828 54508EFCF958F979E4.

The HTTP User-Agent: "Mozilla / 5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit / 525.19 (KHTML, like Gecko) Chrome / 1.0.154.36 Safari / 525.19"