Incident Response Analysis

Group 3

Analysts names:

- Mohamed Elshaheedy AbdElhakim
- Ahmed Amged Ibrahim
- Mohamed Mostafa Mohamed
- Ahmed Mohamed Hamdy
- Ahmed Adel Abd El Hady
- Mustafa Atallah Ali

First Incident

On December 14, 2017, at 23:03 UTC, Chris Lyons' Windows computer showed signs of infection with Formbook malware, an information-stealing malware.

From:	Le Huong-accounts <LeHuong-accounts@gmail.com>
To:	chris.lyons@supercarcenterdetroit.com
Sent time:	14 Dec, 2017 6:14:14 PM
Attachments:	Proforma Invoice P101092292891 TT slip pdf.rar.zip

Dear all,

We've made balance payment for attached invoice on 14/12/2017.
Our below forwarder will contact your side for pickup arrangement:

EVO Logistics Pte Ltd
No 7, Airline Road, #05-08, Cargo Agent Building E, Singapore 819834.
PIC: lucy Tiew (Email: lucy@evvtlogistics.com.sg

There's no need to send the original Tax Invoice or Declaration Letter together with the goods.

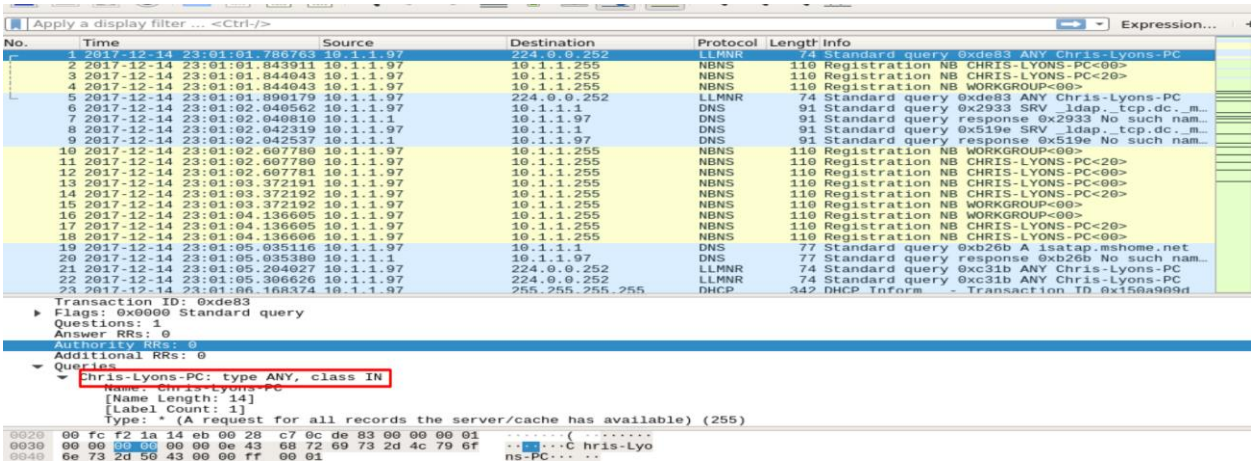
hank you,
uong Le

Infected host name: Chris-Lyons-PC

Infected host IP address: 10.1.1.97

Infected host MAC address: 00:22:15:D4:7A:E7

The establishment malicious Connection on Chris-lyons-PC



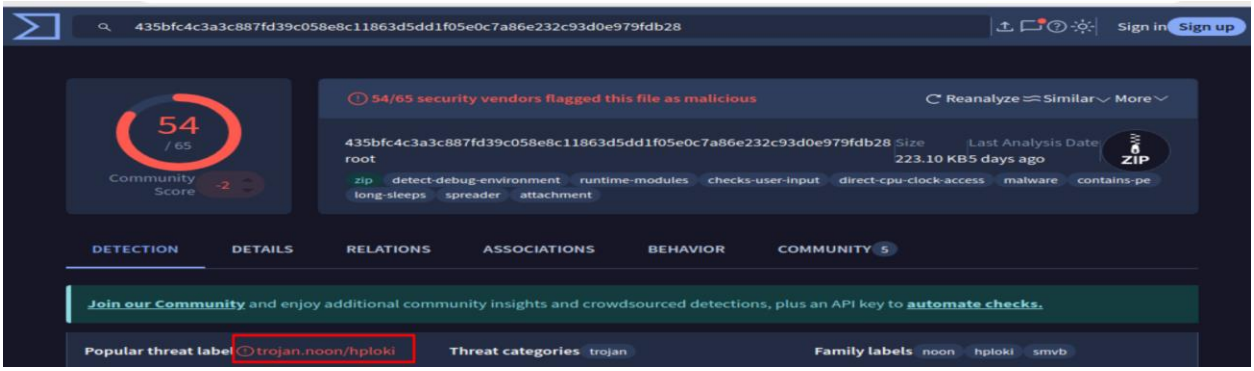
Malware activity was noted from the Email attachment

associated Malware

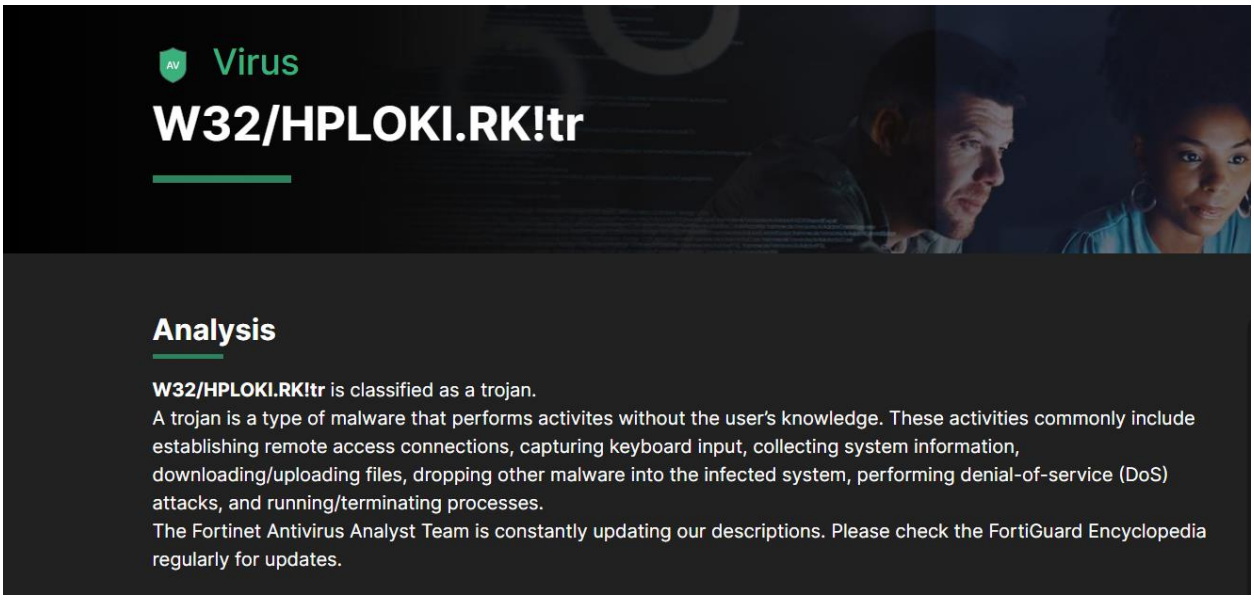
Malware sha265 hash :
435bfc4c3a3c887fd39c058e8c11863d5dd1f05e0c7a86e232c93d0e979fdb28

Malware file name: Proforma Invoice P101092292891 TT slip pdf.rar.zip (Comprised)

malware family: Trojan password Stealer



By searching in Threat Intelligence Websites we found The behavior of the Trojan

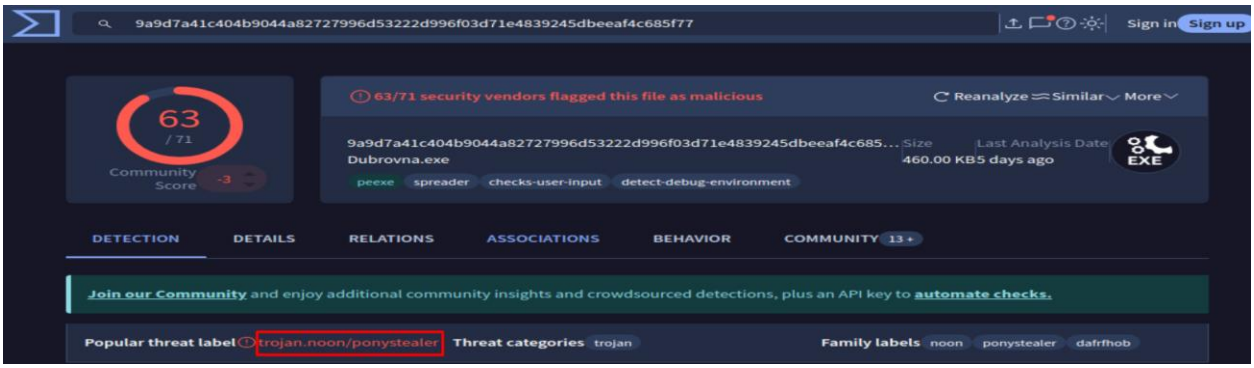


Malware sha265 hash :
9a9d7a41c404b9044a82727996d53222d996f03d71e4839245dbeeaf4c685f77

Malware file name: Proforma Invoice P101092292891 TT slip pdf.rar

malware name: Pony Stealer

malware family: Trojan password Stealer



My Little FormBook

By Paul Rascagneres

WEDNESDAY, JUNE 20, 2018 11:00

This blog post is authored by Warren Mercer and Paul Rascagneres.

Summary

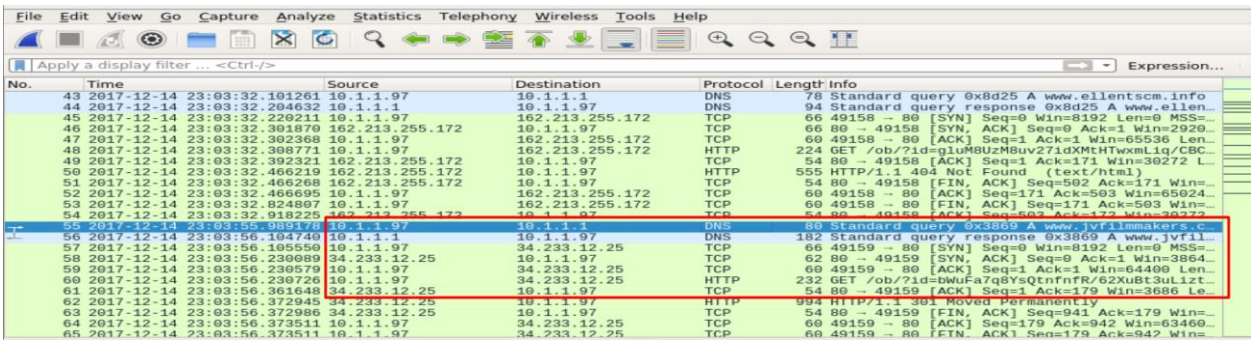
Cisco Talos has been tracking a new campaign involving the FormBook malware since May 2018 that utilizes four different malicious documents in a single phishing email. FormBook is an inexpensive stealer available as "malware as a service." This means an attacker can purchase a compiled piece of malware based on their desired parameters. This is commonplace with crimeware and stealer type malware such as FormBook. It is able to record keystrokes, steal passwords (stored locally and in web forms) and can take screenshots.

Some IoCs For the Data exfiltration Attack

Suspicious Ip address : 34.233.12.25 : 80

Suspicious Domain name : www.jvfilmmakers.com

The connection between the packets started with the Initial Packet Sent at 23:03:55 and the final 23:04:00 the requests started with DNS requests searching for the suspicious Domain www.jvfilmmakers.com



No.	Time	Source	Destination	Protocol	Length	Info
43	2017-12-14 23:03:32.101261	10.1.1.97	10.1.1.1	DNS	78	Standard query 0x8d25 A www.ellentscm.info
44	2017-12-14 23:03:32.204632	10.1.1.1	10.1.1.97	DNS	94	Standard query response 0x8d25 A www.ellen…
45	2017-12-14 23:03:32.220211	10.1.1.97	162.213.255.172	TCP	66	49158 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=…
46	2017-12-14 23:03:32.301870	162.213.255.172	10.1.1.97	TCP	66	80 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=2920…
47	2017-12-14 23:03:32.302368	10.1.1.97	162.213.255.172	TCP	60	49158 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len…
48	2017-12-14 23:03:32.308771	10.1.1.97	162.213.255.172	HTTP	224	GET /ob/?id=gluM8UzM8uv271dXMtHTwxmLlq/CBC…
49	2017-12-14 23:03:32.392321	162.213.255.172	10.1.1.97	TCP	54	80 → 49158 [ACK] Seq=1 Ack=171 Win=30272 L…
50	2017-12-14 23:03:32.466219	162.213.255.172	10.1.1.97	HTTP	555	HTTP/1.1 404 Not Found (text/html)
51	2017-12-14 23:03:32.466268	162.213.255.172	10.1.1.97	TCP	54	80 → 49158 [FIN, ACK] Seq=502 Ack=171 Win=…
52	2017-12-14 23:03:32.466695	10.1.1.97	162.213.255.172	TCP	60	49158 → 80 [ACK] Seq=171 Ack=503 Win=65024…
53	2017-12-14 23:03:32.824807	10.1.1.97	162.213.255.172	TCP	60	49158 → 80 [FIN, ACK] Seq=171 Ack=503 Win=…
54	2017-12-14 23:03:32.918225	162.213.255.172	10.1.1.97	TCP	54	80 → 49158 [ACK] Seq=503 Ack=172 Win=30272
55	2017-12-14 23:03:55.989178	10.1.1.97	10.1.1.1	DNS	80	Standard query 0x3869 A www.jvfilmmakers.c…
56	2017-12-14 23:03:56.104740	10.1.1.1	10.1.1.97	DNS	182	Standard query response 0x3869 A www.jvfil…
57	2017-12-14 23:03:56.105550	10.1.1.97	34.233.12.25	TCP	66	49159 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=…
58	2017-12-14 23:03:56.230089	34.233.12.25	10.1.1.97	TCP	62	80 → 49159 [SYN, ACK] Seq=0 Ack=1 Win=3864…
59	2017-12-14 23:03:56.230579	10.1.1.97	34.233.12.25	TCP	60	49159 → 80 [ACK] Seq=1 Ack=1 Win=64400 Len…
60	2017-12-14 23:03:56.230726	10.1.1.97	34.233.12.25	HTTP	232	GET /ob/?id=bWuFa7q8YsQtnfnfR/62XuBt3uLizt…
61	2017-12-14 23:03:56.361648	34.233.12.25	10.1.1.97	TCP	54	80 → 49159 [ACK] Seq=1 Ack=179 Win=3686 Le…
62	2017-12-14 23:03:56.372945	34.233.12.25	10.1.1.97	HTTP	994	HTTP/1.1 301 Moved Permanently
63	2017-12-14 23:03:56.372986	34.233.12.25	10.1.1.97	TCP	54	80 → 49159 [FIN, ACK] Seq=941 Ack=179 Win=…
64	2017-12-14 23:03:56.373511	10.1.1.97	34.233.12.25	TCP	60	49159 → 80 [ACK] Seq=179 Ack=942 Win=63460…
65	2017-12-14 23:03:56.373511	10.1.1.97	34.233.12.25	TCP	60	49159 → 80 [FIN, ACK] Seq=179 Ack=942 Win=

The DNS server responds with the public IP and the inflicted host establish a TCP connection with the Domain

```
    Source Port: 53
    Destination Port: 51816
    Length: 148
    Checksum: 0x2236 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]
▼ Domain Name System (response)
    Transaction ID: 0x3869
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ www.jvfilmmakers.com: type A, class IN
        Name: www.jvfilmmakers.com
        [Name Length: 20]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▼ Answers
    ▶ www.jvfilmmakers.com: type CNAME, class IN, cname www54.wixdns.net
    ▶ www54.wixdns.net: type CNAME, class IN, cname balancer.wixdns.net
    ▶ balancer.wixdns.net: type CNAME, class IN, cname dfn-tgt-us.wixprod.net
    ▶ dfn-tgt-us.wixprod.net: type A, class IN, addr 34.233.12.25
    [Request In: 55]
    [Time: 0.115562000 seconds]

0030  00 04 00 00 00 00 03 77  77 77 0c 6a 76 66 69 6c   ·····w ww·jvfil
0040  6d 6d 61 6b 65 72 73 03  63 6f 6d 00 00 01 00 01   mmakers· com····
0050  c0 0c 00 05 00 01 00 00  0e 10 00 12 05 77 77 77   ····· ·····www
0060  35 34 06 77 69 78 64 6e  73 03 6e 65 74 00 c0 32   54·wixdn s·net··2
```

Malware then start exfiltrating the Data and sending it to the domain through a post request

```
SRC: POST /ob/ HTTP/1.1
SRC: Host: www.jvfilmmakers.com
SRC: Connection: close
SRC: Content-Length: 455565
SRC: Cache-Control: no-cache
SRC: Origin: http://www.jvfilmmakers.com
SRC: User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
SRC: Content-Type: application/x-www-form-urlencoded
SRC: Accept: */*
SRC: Referer: http://www.jvfilmmakers.com/ob/
SRC: Accept-Language: en-US
SRC: Accept-Encoding: gzip, deflate
SRC:
SRC:
dat=bWuCYce8YsQtnfnfRzJAljo6p8bA6OQMtfFopKt5o2dQL2i5bIvB7aR9sPebqYP0AtmaLEeRr5Ek-h5
SDgGsSHlmy3yrCvI2uWvNydTWJjp9LQeM1sCpzvdHMUG9vZyxySOI6ZWXe9ERDZ_jXkTC5MHMcjb
vUGVtO56c3cIy9ENAvjkRp3vyehJ2li7RRhVueOzM7DB_V8dSw7StdyomFxIse960iuBN0sd9x5FyPThu
2DDHz99X_3NbZp0ZWVdQcWbaTgoXPm6E6MgnOp0I8TRyMDd0UnYrr6EYY2ArwyxOb-7LDrsLODtb
NQj0q7YrTv_WHacpHIrs-6CL7jPUX7fZ-qF2gPiynDia69n503u9HHuok4BPfI2Zsw3QPEg43_UnSou7yx
KZ9z9HVHHKmnURKNgbEFgyFeKEMdANzB-mVBsjOOnSmqQmYZJc9H40QBIIiA5WXI83uZTHuQdc
TOmB3_hv4bIaP5UTcIT85RiiksJRMcWoVqGGP4jk-7Xa7WvAxIrj_-QB4q-IfuNQSQqqgPLm6QjWVGAu
CcwGJFCTxGFuikp8PGV7OIDXRywriuMC34SVL1_IwqaWPEr3RLnWA13AF_EeXP96zNXIgsFBKELF
F9UOvJ4RgUih7kFgQVvg29XgeC3NjeMAaB2JdObpK7Tu2ghgZijL91N9-RhpBqDIzuWE2TDobhbe3i5W
oGGzV8OI_snTRBMWOGRywdo9jvNp3EmmPgVeGp6YhTuZ7CUgIZJsG-IFnr6KzsgFKH34R-npb_YB9
sH_EWGDHWkW5iWE0t1v-YEmOmxdxrWdsVJiuxSuwHAzuvAtIzJrRbXrqNX4KBcHv9NRcRLUYWCL
xo4njsvBD2IUEU20gm9OuS7F0deWkeWIF-mvQX
SRC:
zEiD4jp8it-PwBAr5pZqS1JivbIC1BO7W-qetm6vWzfig3rypb8nJuX_x-6bJMUGd0VPk-0I7PC9u52sTdgG
heWBQUx4n7wen4Y3Ecs2Kr9OZ9C6okwHeGMEly3c5uVvyxnOXWHStFSIamIyQuY-0U_4AsME3OzK
```

Search | Abort | Close

Debug Messages

To summarize The host cris download a password stealer attachment from the Spear phishing mail and the malware start exfiltrating the data of the host to remote server with the ip 34.233.12.25

Second Incident (First Alert)

On Friday, December 15, 2017 at 00:39 UTC, a Windows computer used by Darnell Castillo infected with TeamViewer-based malware. The infection came from a malicious email with an attachment, with the malware being disguised as an advertisement for a Black Friday sale.

File: 2017-12-14-malicious-email-2134-UTC.eml 55661 bytes

Woosters Almost Sold Out! Black Friday Prices + Free Shipping For A Few More Hours!

From:	Black Friday Shopping Voucher <admin367847@airmail.cc>
To:	darnell@castillomotorsports.com
Sent time:	14 Dec, 2017 9:34:24 PM
Attachments:	Black Friday.zip

Details:

Infected host name: Darnell-PC

Infected host IP address: 10.1.1.213

Infected host MAC address: 00087C39DA12

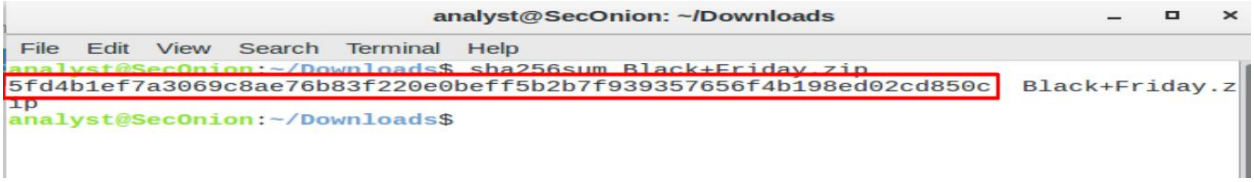
Malware activity was noted from the Email attachment

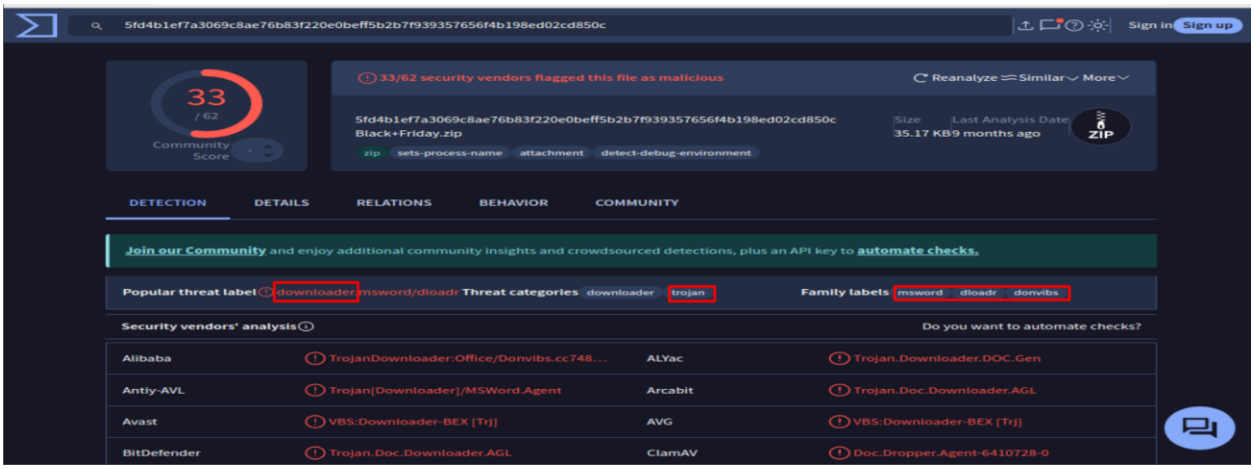
associated Malware

Malware sha265 hash : 5fd4b1ef7a3069c8ae76b83f220e0beff5b2b7f939357656f4b198ed02cd850c

Malware file name: Black Friday.zip (Comprised)

malware family: Trojan-Downloader.VBS.Donvibs



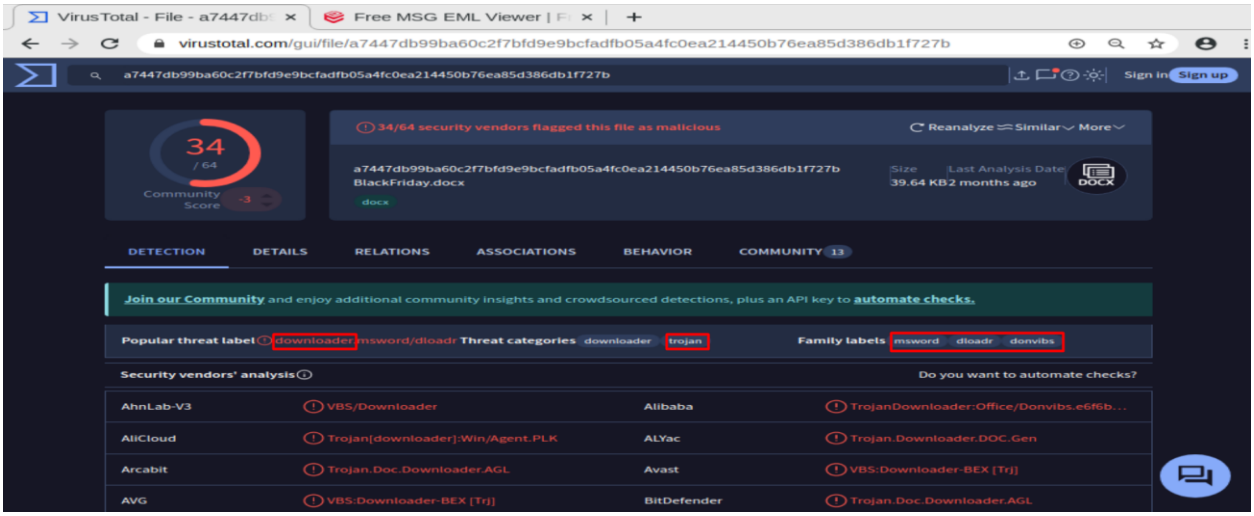


Malware sha265 hash :
a7447db99ba60c2f7bfd9e9bcfadfb05a4fc0ea214450b76ea85d386db1f727b

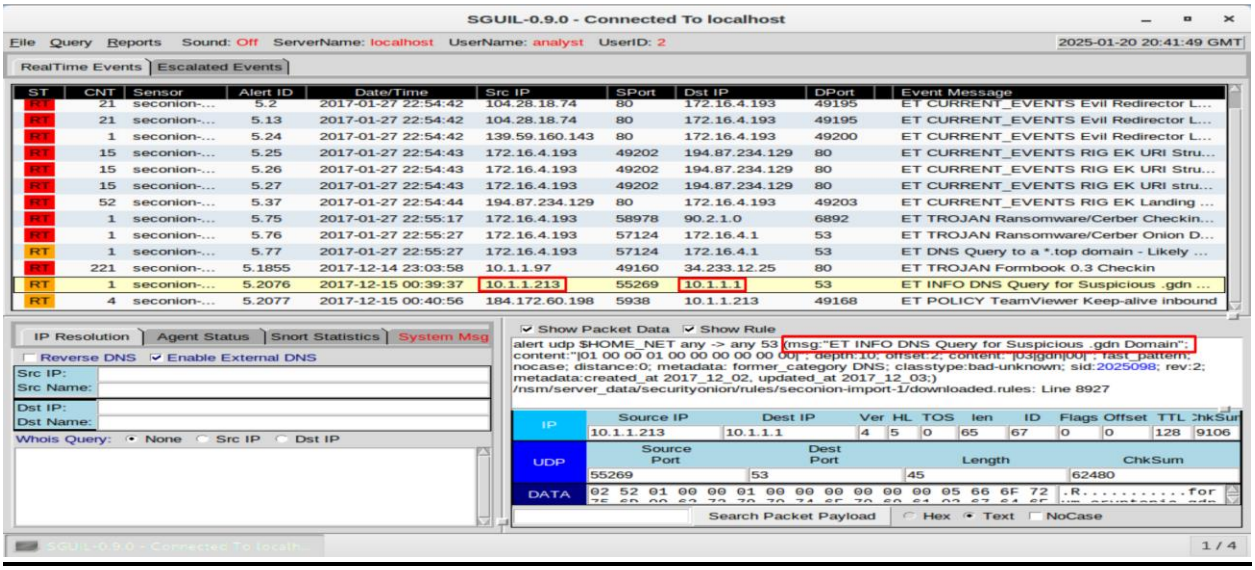
Malware file name: Black Friday.docx

malware name: Trojan-Downloader.VBS.Donvibs

malware family: msword dloadr donvibs

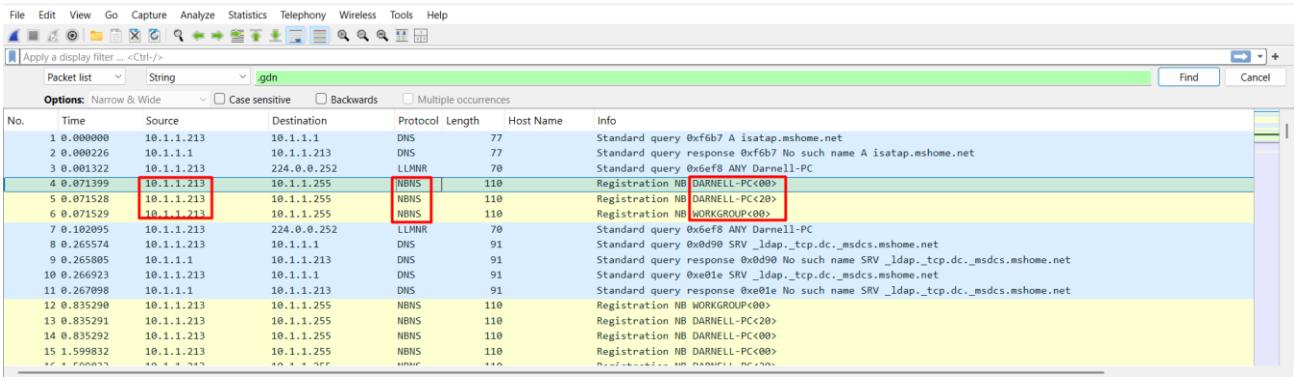


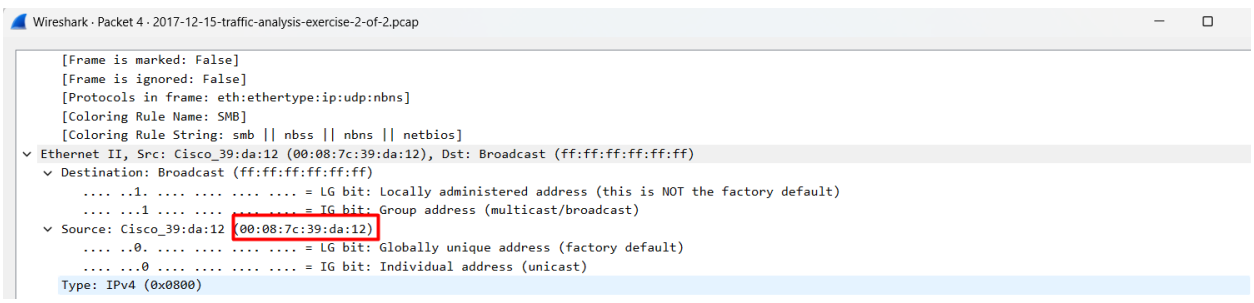
The alert in The SGUIL



Now we just need to confirm by a quick review of the pcap file, and obtain the host information from the traffic by wireshark

in the first few frames on the NetBIOS Name Service (NBNS) and DNS info. From there, we can correlate the host name, IP address, and MAC address.





Behaviour:

DNS query resolved the domain name into an IP address. and the host initiates the communication with the target server.

The client initiates a TCP connection with the server and a TLS handshake begins with the client sending a Client Hello to negotiate encryption protocols.Then The server responds with a Server Hello, its certificate, and key exchange details. Both parties finalize the handshake by securely exchanging keys and establishing an encrypted session.

2017-12-15-traffic-analysis-exercise-2-of-2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Packet list | String | .gdn | Find | Cancel

Options: Narrow & Wide | Case sensitive | Backwards | Multiple occurrences

No.	Time	Source	Destination	Protocol	Length	Host Name	Info
46	275.403227	10.1.1.213	10.1.1.1	DNS	79		Standard query 0x0252 A forum.cryptopia.gdn
47	275.404127	10.1.1.213	255.255.255.255	DHCP	342	Darnell-PC	DHCP Inform - Transaction ID 0xff6257c4
48	275.468282	10.1.1.1	10.1.1.213	DNS	514		Standard query response 0x0252 A forum.cryptopia.gdn A 185.92.222.9 NS i.root-servers.net NS j.root-servers.net
49	275.477028	10.1.1.213	185.92.222.9	TCP	66		49158 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
50	275.680765	185.92.222.9	10.1.1.213	TCP	66		443 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1288 SACK_PERM WS=128
51	275.681335	10.1.1.213	185.92.222.9	TCP	60		49158 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
52	275.690077	10.1.1.213	185.92.222.9	TLSv1.2	215		Client Hello (SNI=forum.cryptopia.gdn)
53	275.897909	185.92.222.9	10.1.1.213	TCP	54		443 → 49158 [ACK] Seq=1 Ack=162 Win=30336 Len=0
54	275.900447	185.92.222.9	10.1.1.213	TLSv1.2	1342		Server Hello
55	275.900736	185.92.222.9	10.1.1.213	TCP	1342		443 → 49158 [ACK] Seq=1289 Ack=162 Win=30336 Len=1288 [TCP PDU reassembled in 56]
56	275.900812	185.92.222.9	10.1.1.213	TLSv1.2	408		Certificate, Server Key Exchange, Server Hello Done
57	275.900995	10.1.1.213	185.92.222.9	TCP	60		49158 → 443 [ACK] Seq=162 Ack=1289 Win=65536 Len=0
58	275.901212	10.1.1.213	185.92.222.9	TCP	60		49158 → 443 [ACK] Seq=162 Ack=2931 Win=65536 Len=0
59	275.930999	10.1.1.213	185.92.222.9	TLSv1.2	220		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
60	276.138891	185.92.222.9	10.1.1.213	TLSv1.2	145		Change Cipher Spec, Encrypted Handshake Message

```
> Frame 46: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
v Ethernet II, Src: Cisco_39:da:12 (00:08:7c:39:da:12), Dst: HewlettPacka_bd:a1:2c (84:34:97:bd:a1:2c)
  > Destination: HewlettPacka_bd:a1:2c (84:34:97:bd:a1:2c)
  > Source: Cisco_39:da:12 (00:08:7c:39:da:12)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 10.1.1.213, Dst: 10.1.1.1
v User Datagram Protocol, Src Port: 55269, Dst Port: 53
    Source Port: 55269
    Destination Port: 53
    Length: 45
    Checksum: 0xf410 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 10]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (37 bytes)
v Domain Name System (query)
```

```
0000  84 34 97 bd a1 2c 00 08  7c 39 da 12 08 00 45 00   ·4···,·· |9····E·
0010  00 41 00 43 00 00 80 11  23 92 0a 01 01 d5 0a 01   ·A·C···· #·····
0020  01 01 d7 e5 00 35 00 2d  f4 10 02 52 01 00 00 01   ·····5·- ···R····
0030  00 00 00 00 00 00 05 66  6f 72 75 6d 09 63 72 79   ·******· f orum·cry
0040  70 74 6f 70 69 61 03 67  64 6e 00 00 01 00 01      ptopia·g dn·····
```

Ready to load or capture | Packets: 2982 | Profile: Default

Apply a display filter ... <Ctrl-/>

Packet list | String | .gdn | Find | Cancel

Options: Narrow & Wide | Case sensitive | Backwards | Multiple occurrences

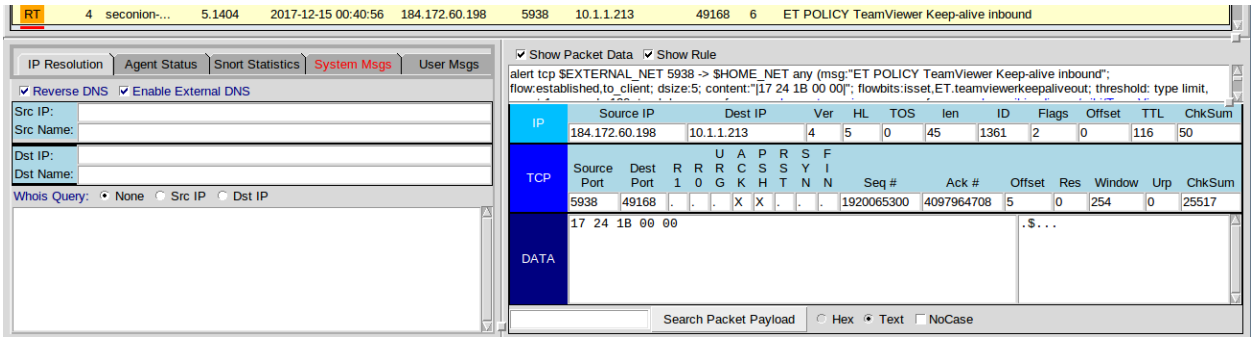
No.	Time	Source	Destination	Protocol	Length	Host Name	Info
48	275.468282	10.1.1.1	10.1.1.213	DNS	514		Standard query response 0x0252 A forum.cryptopia.gdn A 185.92.222.9 NS i.root-servers.net NS j.root-servers.n
49	275.477028	10.1.1.213	185.92.222.9	TCP	66		49158 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
50	275.680765	185.92.222.9	10.1.1.213	TCP	66		443 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1288 SACK_PERM WS=128
51	275.681335	10.1.1.213	185.92.222.9	TCP	60		49158 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
52	275.690077	10.1.1.213	185.92.222.9	TLSv1.2	215		Client Hello (SNI=forum.cryptopia.gdn)
53	275.897909	185.92.222.9	10.1.1.213	TCP	54		443 → 49158 [ACK] Seq=1 Ack=162 Win=30336 Len=0
54	275.900447	185.92.222.9	10.1.1.213	TLSv1.2	1342		Server Hello
55	275.900736	185.92.222.9	10.1.1.213	TCP	1342		443 → 49158 [ACK] Seq=1289 Ack=162 Win=30336 Len=1288 [TCP PDU reassembled in 56]
56	275.900812	185.92.222.9	10.1.1.213	TLSv1.2	408		Certificate, Server Key Exchange, Server Hello Done
57	275.900995	10.1.1.213	185.92.222.9	TCP	60		49158 → 443 [ACK] Seq=162 Ack=1289 Win=65536 Len=0
58	275.901212	10.1.1.213	185.92.222.9	TCP	60		49158 → 443 [ACK] Seq=162 Ack=2931 Win=65536 Len=0
59	275.930999	10.1.1.213	185.92.222.9	TLSv1.2	220		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
60	276.138891	185.92.222.9	10.1.1.213	TLSv1.2	145		Change Cipher Spec, Encrypted Handshake Message
61	276.139417	10.1.1.213	185.92.222.9	TCP	60		49158 → 443 [ACK] Seq=328 Ack=3022 Win=65536 Len=0
62	276.164228	10.1.1.213	10.1.1.255	NBNS	92		Name query NB WPAD<00>

```
..........Z3....
..0co2`..> )c.0..r...Q.....*.<./.=.5...
`......*.#...$.        .
.0.2.j.8......E.............forum.cryptopia.gdn.
................
.............]...Y.........c.....`./<.6......*...6b/ ..8.%..7.4.=..y......2...&r6.....'.......................   ...        ..          ...
0..         0................W..9.)....W.0
.           *.H..
.....0J1.0  ..U....US1.0...U.
.
Let's Encrypt1#0!..U....Let's Encrypt Authority X30..
171213074404Z.
180313074404Z0.1.0...U....forum.cryptopia.gdn0..."0
.           *.H..
.........0..
.....$....>.0a..k0A&.....U0/..x.OG...-X...'.....ea-...\..?p|..............k(Y.;.T.v".#IV...*._..n'9....
Z..S......*..@`I.....#<g. ..:.....h..c..^..7|&%.gk.q".......;._.vu...L+$PJ3wW.VW.7..w.....t..]....*..Vq...B...M..9W;n.._.        -.J...X_.C
..
.A=]...<.+../.........0...0...U...........0...U.%..0...+.........*......0...U.......0.0...U........n..Y@=.    X .(>.0  .U.# .0   .1c.)....9..Ee.....0o..+.......c0a0...+.....0..*http://ocsp.int-x3.letsencrypt.org0/..+.....0..#http://cert.int-
x3.letsencrypt.org/0...U....0...forum.cryptopia.gdn0....U. ...0..0...g.....0....+..........0..0&.+........http://cps.letsencrypt.org0.....+.......0.....This Certificate may only be relied upon by Relying Parties and only in accordance with the Certificate
Policy found at https://letsencrypt.org/repository/0
.           *.H..
```

Second Incident (Second Alert)

TeamViewer Activity Analysis

I will review this alert



1. Observed Activity

- **TeamViewer Keep-alive Inbound Detected**:
  - Multiple instances of **TeamViewer Keep-alive** packets were identified in the network traffic. These packets are part of TeamViewer's standard protocol to maintain an active connection between the client and server.
  - The traffic originated from the external IP address `184.172.60.198` and was directed to the internal IP `10.1.1.213`.
  - The keep-alive packets were detected on **port 5938**, the default port used by TeamViewer for remote connections.

2. Context and Significance

- **Legitimate Use**:
  - TeamViewer is a widely trusted remote access tool, and keep-alive packets are a normal part of its operation to ensure the connection remains active.
  - If TeamViewer is authorized and used for legitimate purposes (e.g., remote support, IT administration), this activity is expected and not inherently malicious.
- **Potential Abuse**:
  - TeamViewer can be exploited by attackers for unauthorized remote access, data exfiltration, or lateral movement within a network.
  - The repeated keep-alive packets could indicate an active remote session, which should be verified to ensure it is authorized.

3. Security Concerns

- **Unauthorized Access**:
  - If TeamViewer is not authorized in the environment, the presence of keep-alive packets from `184.172.60.198` to `10.1.1.213` could indicate unauthorized remote access.
- **Data Exfiltration**:
  - Attackers could use TeamViewer to exfiltrate sensitive data or deploy additional malware.
- **Persistence**:
  - TeamViewer can be configured to start automatically, providing attackers with persistent access to the compromised system.

4. Recommendations

- **Verify Authorization**:
  - Confirm whether TeamViewer is authorized for use in the environment. If not, investigate the source of the traffic and take appropriate action.
- **Monitor TeamViewer Usage**:
  - Regularly monitor TeamViewer activity to ensure it is used only by authorized personnel and for legitimate purposes.
- **Restrict Access**:
  - Use firewalls or network access controls to restrict TeamViewer traffic to authorized IPs and ports.
- **Review Logs**:
  - Check TeamViewer logs to identify the users and devices involved in the remote sessions.
- **Consider Alternatives**:
  - If TeamViewer is not required, consider disabling or uninstalling it to reduce the attack surface.

5. Conclusion

The observed **TeamViewer Keep-alive Inbound** traffic from `184.172.60.198` to `10.1.1.213` is consistent with normal operation of the software. However, given the potential for abuse, it is critical to verify that this activity is authorized and to implement controls to prevent unauthorized use. Regular monitoring and logging of TeamViewer activity are recommended to ensure the security of the network.
