NTI-CyberOps

SO-Investigation Report

Introduction

This report involves the investigation of two pcap files and two emails, through the report we will cover the investigation process, tools, and key findings.

Tools Used

1. Security Onion

   We are running Security Onion, using Oracle virtual box for facilitating the investigation process and to make use of all the tools brought with Security Onion.
2. https://www.encryptomatic.com/viewer/

   We have used this website to help view the emails and download their attachments.
3. Virus Total, Cisco Talos, hybrid-analysis.com.

   We have used the tools above for malware file(s) analysis.
4. SGUIL

   We have used SGUIL, to view any alerts that may help us and facilitate the investigation process.
5. Wireshark

   We have used Wireshark for packet analysis and host identification.
6. Kibana

   We have used Kibana to help us with filtering and further investigation.

First Case Investigation

Overview of Victim(s) Information

Start and End Time of The Malicious Activity

The start date of the malicious activity is:
December 14th 2017, 23:03:58 PM.

The last malicious activity was recorded on:
December 14th 2017, 23:14:47 PM.

Victim Email

chris.lyons@supercarcenterdetroit.com

Victim PC Host Name

Chris-Lyons-PC

Victim PC MAC Address

00:22:15:d4:9a:e7

Victim PC IP Address

10.1.1.97

Types of Noted Malicious Activities

Phishing, Malware Installation, and Data Exfiltration.

Indicators of Malicious Activity

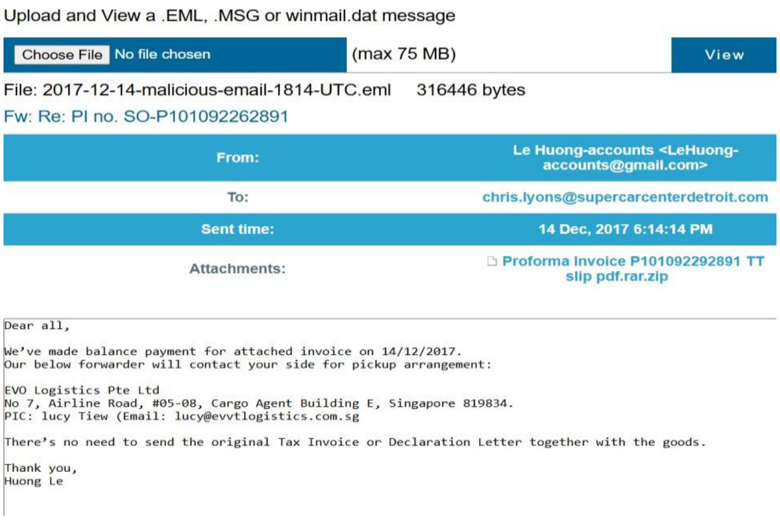
- Installed malware on the victim’s PC.
- Huge post requests to a large number of websites.

Summary

On December 14th, 2017, a phishing email was sent to chris.lyons@supercarcenterdetroit.com containing a malicious attachment, "Proforma Invoice P101092292891 TT slip pdf.rar.zip." Upon opening the attachment, a Formbook malware was installed on the victim’s PC (Chris-Lyons-PC, IP: 10.1.1.97, MAC: 00:22:15:d4:9a:e7). This malware initiated data exfiltration by sending large encoded POST requests to multiple domains.

Email Investigation

We started by uploading the mail to www.encryptomatic.com/viewer/, we can identify this mail as a phishing mail, for further investigation and confirmation let’s view the downloaded attachment “Proforma Invoice P101092292891 TT slip pdf.rar.zip”.



Upload and View a .EML, .MSG or winmail.dat message

File: 2017-12-14-malicious-email-1814-UTC.eml 316446 bytes

Fw: Re: PI no. SO-P101092262891

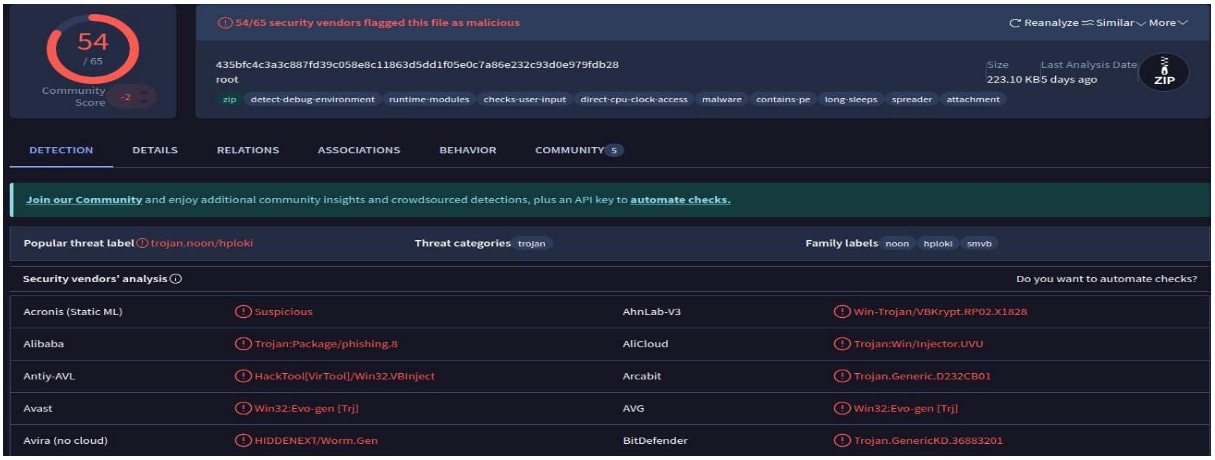
From:	Le Huong-accounts <LeHuong-accounts@gmail.com>
To:	chris.lyons@supercarcenterdetroit.com
Sent time:	14 Dec, 2017 6:14:14 PM
Attachments:	Proforma Invoice P101092292891 TT slip pdf.rar.zip

```
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.

Thank you,
Huong Le
```

Email Attachment Analysis

Uploading to Virus Total

We can easily see that the attachment “Proforma Invoice P101092292891 TT slip pdf.rar.zip” is malicious.



54/65 security vendors flagged this file as malicious

435bfc4c3a3c887fd39c058e8c11863d5dd1f05e0c7a86e232c93d0e979fdb28
root

zip detect-debug-environment runtime-modules checks-user-input direct-cpu-clock-access malware contains-pe long-sleeps spreader attachment

Size 223.10 KB

Last Analysis Date 5 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.noon/hploki

Threat categories trojan

Family labels noon hploki smvb

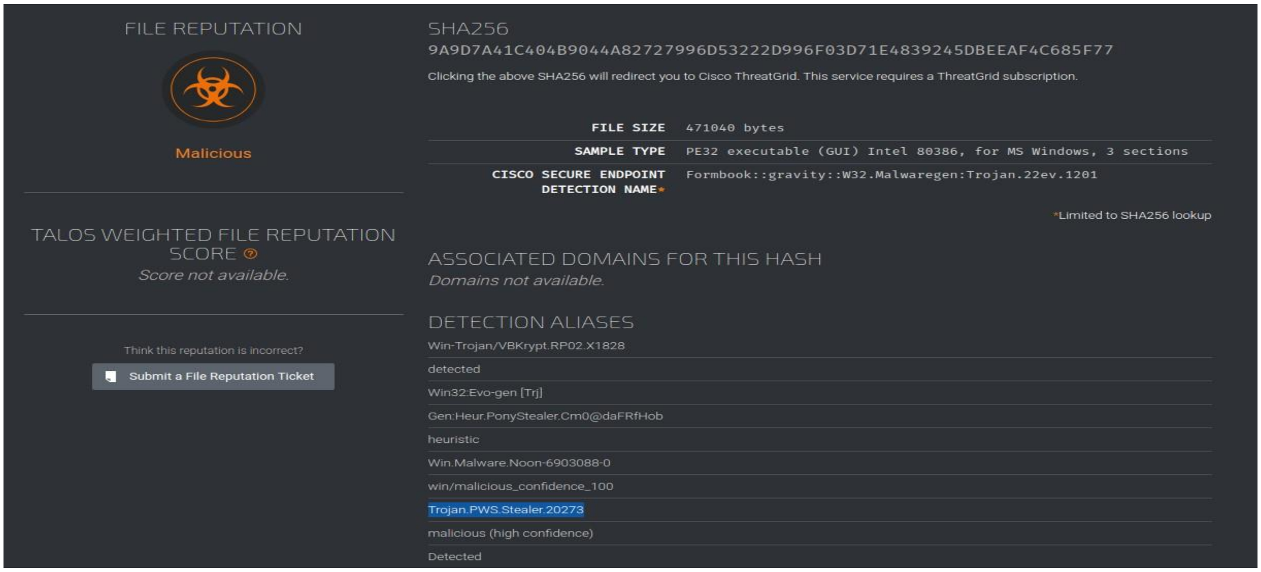
Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Win-Trojan/VBKrypt.RP02.X1828
Alibaba	Trojan:Package/phishing.8	AliCloud	Trojan:Win/Injector.UVU
Antiy-AVL	HackTool[VirTool]/Win32.VBInject	Arcabit	Trojan.Generic.D232CB01
Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
Avira (no cloud)	HIDDENEXT/Worm.Gen	BitDefender	Trojan.GenericKD.36883201

Uploading to Cisco Talos

Trojan.PWS.Stealer.20273 is an interesting finding since it aligns with the IDS Alert of SGUIL.



FILE REPUTATION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE

Score not available.

Think this reputation is incorrect?

Submit a File Reputation Ticket

SHA256
9A9D7A41C404B9044A82727996D53222D996F03D71E4839245DBEEAF4C685F77

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE	471040 bytes
SAMPLE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows, 3 sections
CISCO SECURE ENDPOINT DETECTION NAME*	Formbook::gravity::W32.Malwaregen:Trojan.22ev.1201

*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

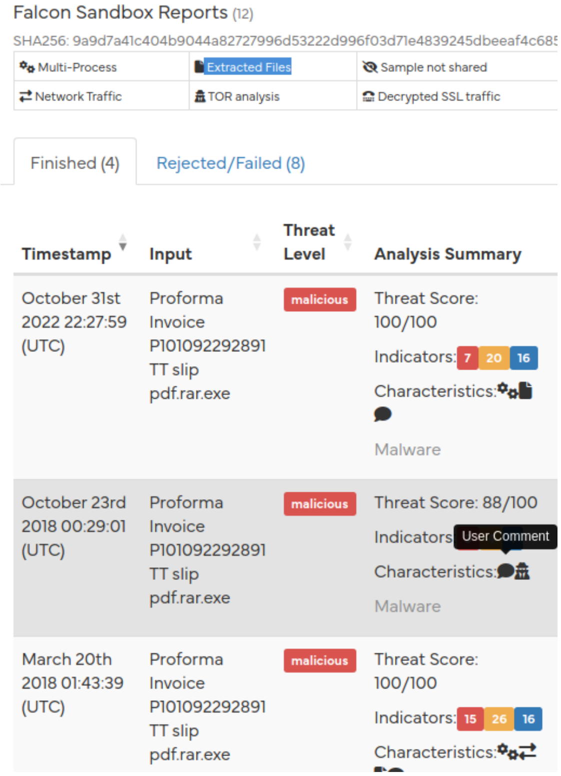
Domains not available.

DETECTION ALIASES

Win-Trojan/VBKrypt.RP02.X1828
detected
Win32:Evo-gen [Trj]
Gen:Heur.PonyStealer.Cm0@daFRfHob
heuristic
Win.Malware.Noon-6903088-0
win/malicious_confidence_100
Trojan.PWS.Stealer.20273
malicious (high confidence)
Detected

Uploading to hybrid-analysis.com

We can see that the malware was tagged for extracted files.



Falcon Sandbox Reports (12)

SHA256: 9a9d7a41c404b9044a82727996d53222d996f03d71e4839245dbeeaf4c685

Multi-Process	Extracted Files	Sample not shared
Network Traffic	TOR analysis	Decrypted SSL traffic

Finished (4) Rejected/Failed (8)

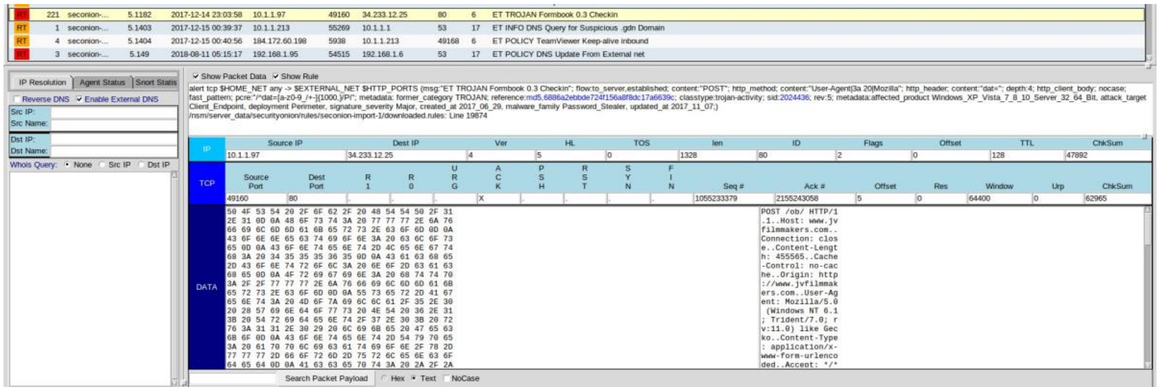
Timestamp	Input	Threat Level	Analysis Summary
October 31st 2022 22:27:59 (UTC)	Proforma Invoice P101092292891 TT slip pdf.rar.exe	malicious	Threat Score: 100/100 Indicators: 7 20 16 Characteristics: Malware
October 23rd 2018 00:29:01 (UTC)	Proforma Invoice P101092292891 TT slip pdf.rar.exe	malicious	Threat Score: 88/100 Indicators User Comment Characteristics: Malware
March 20th 2018 01:43:39 (UTC)	Proforma Invoice P101092292891 TT slip pdf.rar.exe	malicious	Threat Score: 100/100 Indicators: 15 26 16 Characteristics:

Overview of The Mail Attachment

The user seems to have installed a malicious attachment "Proforma Invoice P101092292891 TT slip pdf.rar.zip" with the sha256sum:"435bfc4c3a3c887fd39c058e8c11863d5dd1f05e0c7a86e232c93d0e979fdb28", That seems to be a formbook malware used to steal the users credentials.

Investigating Using SGUIL

We can find one associated alert, with the formbook malware at the ip "10.1.1.97" and the event message "ET Trojan Formbook 0.3 Checkin", which upon viewing the transcript seems to be a large encoded post request for the domain "34.233.12.255" which might be a possible data exfiltration, and we can also identify the malware family "password stealer" from the rule.



```
RT  221  seconion-...  5.1182  2017-12-14 23:03:58  10.1.1.97       49160  34.233.12.25  80     6   ET TROJAN Formbook 0.3 Checkin
RT    1  seconion-...  5.1403  2017-12-15 00:39:37  10.1.1.213      55269  10.1.1.1      53     17  ET INFO DNS Query for Suspicious .gdn Domain
RT    4  seconion-...  5.1404  2017-12-15 00:40:56  184.172.60.198  5938   10.1.1.213    49168  6   ET POLICY TeamViewer Keep-alive inbound
RT    3  seconion-...  5.149   2018-08-11 05:15:17  192.168.1.95    54515  192.168.1.6   53     17  ET POLICY DNS Update From External net
```

☐ Reverse DNS ☑ Enable External DNS

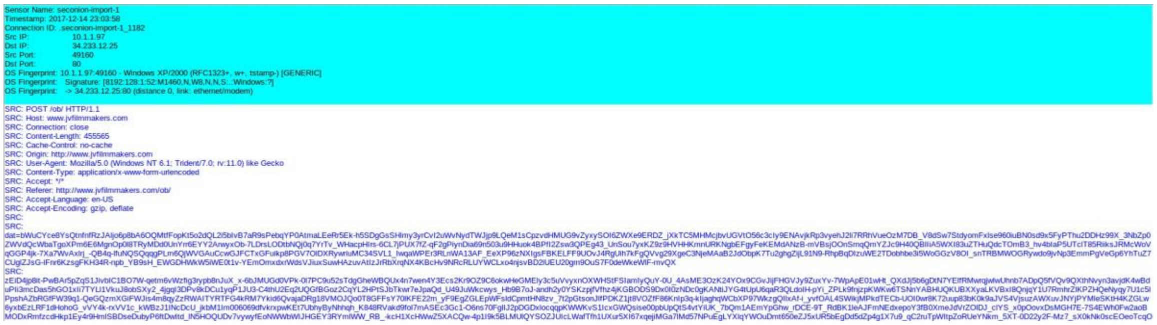
Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Formbook 0.3 Checkin"; flow:to_server,established; content:"POST"; http_method; content:"User-Agent|3a 20|Mozilla"; http_header; content:"dat="; depth:4; http_client_body; nocase;
fast_pattern; pcre:"/^dat=[a-z0-9_/+-]{1000,}/Pi"; metadata: former_category TROJAN; reference:md5,6886a2ebbde724f156a8f8dc17a6639c; classtype:trojan-activity; sid:2024436; rev:5; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target
Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_06_29, malware_family Password_Stealer, updated_at 2017_11_07;)
/nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 19874
```

```
IP    Source IP   Dest IP       Ver  HL  TOS  len   ID  Flags  Offset  TTL  ChkSum
      10.1.1.97   34.233.12.25  4    5   0    1328  80  2      0       128  47892

TCP   Source  Dest  R  R  U  A  P  R  S  F  Seq #       Ack #       Offset  Res  Window  Urp  ChkSum
      Port    Port  1  0  R  C  S  S  Y  I
                          G  K  H  T  N  N
      49160   80    .  .  .  X  .  .  .  .  1055233379  2155243058  5       0    64400   0    62965

DATA
50 4F 53 54 20 2F 6F 62 2F 20 48 54 54 50 2F 31
2E 31 0D 0A 48 6F 73 74 3A 20 77 77 77 2E 6A 76
66 69 6C 6D 6D 61 6B 65 72 73 2E 63 6F 6D 0D 0A
43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73
65 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74
68 3A 20 34 35 35 35 36 35 0D 0A 43 61 63 68 65
2D 43 6F 6E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 63
68 65 0D 0A 4F 72 69 67 69 6E 3A 20 68 74 74 70
3A 2F 2F 77 77 77 2E 6A 76 66 69 6C 6D 6D 61 6B
65 72 73 2E 63 6F 6D 0D 0A 55 73 65 72 2D 41 67
65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30
20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31
3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72
76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 65 63
6B 6F 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65
3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D
77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E 63 6F
64 65 64 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A

POST /ob/ HTTP/1
.1..Host: www.jv
filmmakers.com..
Connection: clos
e..Content-Lengt
h: 455565..Cache
-Control: no-cac
he..Origin: http
://www.jvfilmmak
ers.com..User-Ag
ent: Mozilla/5.0
 (Windows NT 6.1
; Trident/7.0; r
v:11.0) like Gec
ko..Content-Type
: application/x-
www-form-urlenco
ded..Accept: */*
```

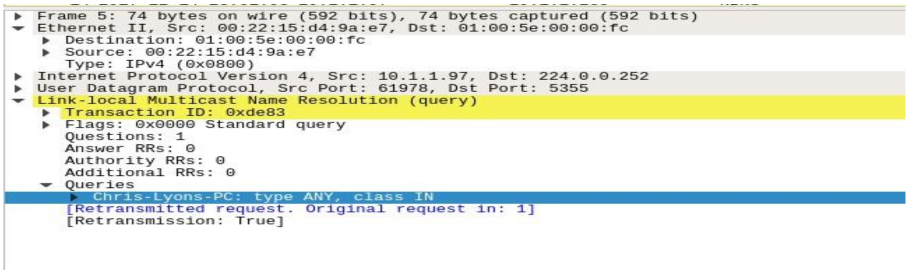
○ Hex ● Text ☐ NoCase



```
Sensor Name: seconion-import-1
Timestamp: 2017-12-14 23:03:58
Connection ID: .seconion-import-1_1182
Src IP:          10.1.1.97
Dst IP:          34.233.12.25
Src Port:        49160
Dst Port:        80
OS Fingerprint: 10.1.1.97:49160 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S::Windows:?]
OS Fingerprint:   -> 34.233.12.25:80 (distance 0, link: ethernet/modem)

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=bWuCYce8YsQtnfnfRzJAljo6p8bA6OQMtfFopKt5o2dQL2i5blvB7aR9sPebqYP0AtmaLEeRr5Ek-h5SDgGsSHlmy3yrCvI2uWvNydTWJjp9LQeM1sCpzvdHMUG9vZyxySOI6ZWXe9ERDZ_jXkTC5MHMcjbvUGVtO56c3cIy9ENAvjkRp3vyehJ2li7RRhVueOzM7DB_V8dSw7StdyomFxIse960iuBN0sd9x5FyPThu2DDHz99X_3NbZp0
ZWVdQcWbaTgoXPm6E6MgnOp0l8TRyMDd0UnYrr6EYY2AnwyxOb-7LDrsLODtbNQj0q7YrTv_WHacpHlrs-6CL7jPUX7fZ-qF2gPiynDia69n503u9HHuok4BPfI2Zsw3QPEg43_UnSou7yxKZ9z9HVHHKmnURKNgbEFgyFeKEMdANzB-mVBsjOOnSmqQmYZJc9H40QBIliA5WXI83uZTHuQdcTOmB3_hv4blaP5UTcIT85RiiksJRMcWoV
qGGP4jk-7Xa7WvAxlrj_-QB4q-lfuNQSQqqgPLm6QjWVGAuCcwGJFCTxGFulkp8PGV7OlDXRywrluMC345VL1_lwqaWPEr3RLnWA13AF_EeXP96zNXIgsFBKELFF9UOvJ4RgUih7kFgQVvg29XgeC3NjeMAaB2JdObpK7Tu2ghgZijL91N9-RhpBqDIzuWE2TDobhbe3i5WoGGzV8OI_snTRBMWOGRywdo9jvNp3EmmPgVeGp6YhTuZ7
CUglZJsG-lFnr6KzsgFKH34R-npb_YB9sH_EWGDHWkW5iWE0t1v-YEmOmxdxrWdsVJiuxSuwHAzuvAtIzJrRbXrqNX4KBcHv9NRcRLUYWCLxo4njsvBD2lUEU20gm9OuS7F0deWkeWIF-mvQX
SRC:
zEID4jp8it-PwBAr5pZqS1JivbIC1BO7W-qetm6vWzfig3rypb8nJuX_x-6bJMUGd0VPk-0I7PC9u52sTdgGheWBQUx4n7wen4Y3Ecs2Kr9OZ9C6okwHeGMEly3c5uVvyxnOXWHStFSIamIyQuY-0U_4AsME3OzK24YOx9CGvJijFHGVJy9ZuxYv-7WpApE01wHt_QXdJj5b6gDtN7YEIfRMwrqjwlwUhnb7ADpQ5fVQv9QXthNvyn3avjdK4wBd
uPli3mcDas5hGO1xli7TYLl1VkuJ8obSXy2_4jgql3DPv8kDCu1yqP1JU3-C4thU2Eq2UQGfBGoz2CqYL2HPtSJbTkwr7eJpaQd_U49JuWkcwys_Hb9B7oJ-andh2y0YSKzpjfVfhz4jKGBODS9Dx0t0zNDc0gKANtiJYG4tUpU6qaR3QLdolH-pYi_ZPLk9fnjzpKWKw6TSNnYABHUQKUBXXyaLKVBxI8QnjqY1U7RmhrZIKPZHQeNyqy7U1c5I
PpshAZbRGfFW39q1-QeGQzmXGiFWJis4m8qyZzRWAITYRTFG4kRM7Ykid6QvajaDRg18VMOJQo0T8GFFsY70lKFE22m_yF9EgZGLEpWFsldCpmtHN8zv_7t2pGtsonJlfPDKZ1jt8VOZfF86Knlp3q-kljaghqWCbXP97WkzgQllxAf-i_yvfOAL4SWikjMPkdTECb-UOI0wr8K72uup83bK0k9aJVS4VjsuzAWXuvJNYjPYMleSKtH4KZGLw
6yxbEzLRF1dHohoG_vVY4k-rxVV1c_kWBzJ1INcDcU_jkbM1lm006069dfvkrxpwKEt7UbhyByNhhqh_K848RVakd9foI7mASEc3Gc1-O6ns70FglJ2pDGDxlocqqpKWWKvS1IcxGWQsise00pbUpQtS4vtYiUK_7bQm1AEmYpGhw_rDCE-9T_RdBK1IeAJFmNEdxepoY3fB0XmeJdVrZOIDJ_cIYS_x0pOovxDsMGH7E-7S4EWh0Fw2aoB
MODxRmfzcdHkp1Ey4r9HmISBDseDubyP6ftDwltd_IN5HOQUDv7vywyfEoNWWbWIJHGEY3RYmIWW_RB_-kcH1XcHWwZ5XACQw-4p1l9k5BLMUIQYSOZJUlcLWafTfh1UXur5XI67xqejiMGa7lMd57NPuEgLYXlqYWOuDmt650eZJ5xUR5bEgDd5dZp4g1X7u9_qC2ruTpWltpZoRUeYNkm_5XT-0D22y2F-Mz7_sX0kNk0scEOeoTcqO
```

Identifying The Host Using Wireshark

We have investigated the associated pcap file “import1.pcap”, to extract the host information associated with the ip address “10.1.1.97”, host-pc-name: “Chris-Lyons-PC”, host-MAC-address: “00:22:15:d4:9a:e7”.

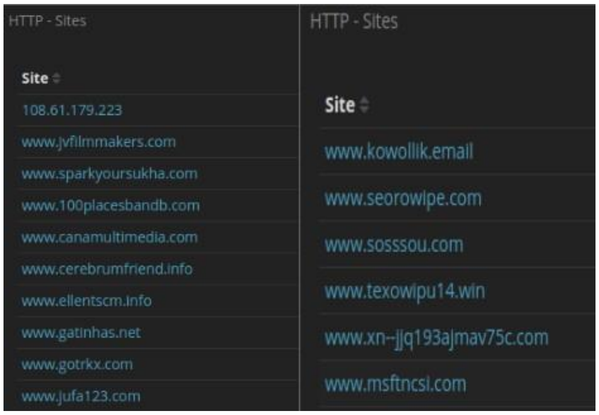


```
▶ Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▼ Ethernet II, Src: 00:22:15:d4:9a:e7, Dst: 01:00:5e:00:00:fc
    ▶ Destination: 01:00:5e:00:00:fc
    ▶ Source: 00:22:15:d4:9a:e7
      Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.1.1.97, Dst: 224.0.0.252
▶ User Datagram Protocol, Src Port: 61978, Dst Port: 5355
▼ Link-local Multicast Name Resolution (query)
    ▶ Transaction ID: 0xde83
    ▶ Flags: 0x0000 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    ▼ Queries
        ▶ Chris-Lyons-PC: type ANY, class IN
      [Retransmitted request. Original request in: 1]
      [Retransmission: True]
```

Further Investigation Using Kibana

We have found out multiple sites, with a huge number of post requests being sent to, which we suspect to be associated data exfiltration, however we failed to identify the motive behind sending the data to multiple domains.

Upon checking the sites on VirusTotal, we found none to be malicious however we still think they are associated with the data exfiltration process.

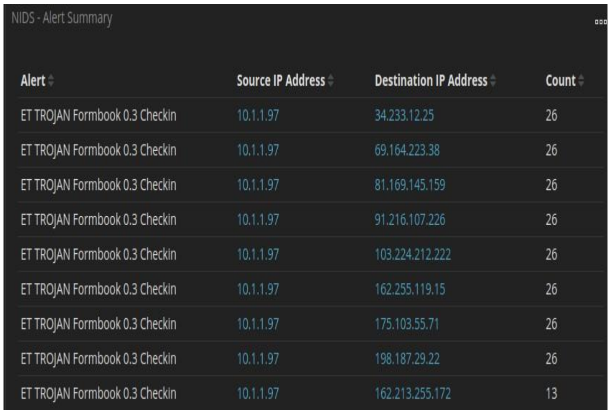


HTTP - Sites

Site
108.61.179.223
www.jvfilmmakers.com
www.sparkyoursukha.com
www.100placesbandb.com
www.canamultimedia.com
www.cerebrumfriend.info
www.ellentscm.info
www.gatinhas.net
www.gotrkx.com
www.jufa123.com

HTTP - Sites

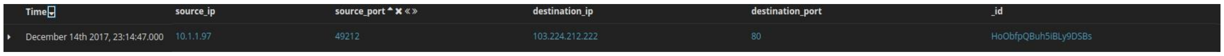
Site
www.kowollik.email
www.seorowipe.com
www.sosssou.com
www.texowipu14.win
www.xn--jjq193ajmav75c.com
www.msftncsi.com



NIDS - Alert Summary

Alert	Source IP Address	Destination IP Address	Count
ET TROJAN Formbook 0.3 Checkin	10.1.1.97	34.233.12.25	26
ET TROJAN Formbook 0.3 Checkin	10.1.1.97	69.164.223.38	26
ET TROJAN Formbook 0.3 Checkin	10.1.1.97	81.169.145.159	26
ET TROJAN Formbook 0.3 Checkin	10.1.1.97	91.216.107.226	26
ET TROJAN Formbook 0.3 Checkin	10.1.1.97	103.224.212.222	26
ET TROJAN Formbook 0.3 Checkin	10.1.1.97	162.255.119.15	26
ET TROJAN Formbook 0.3 Checkin	10.1.1.97	175.103.55.71	26
ET TROJAN Formbook 0.3 Checkin	10.1.1.97	198.187.29.22	26
ET TROJAN Formbook 0.3 Checkin	10.1.1.97	162.213.255.172	13

The last malicious data exfiltration activity was recorded on December 14th 2017, 22:14:47.



Time	source_ip	source_port	destination_ip	destination_port	_id
December 14th 2017, 23:14:47.000	10.1.1.97	49212	103.224.212.222	80	HoObfpQBuh5iBLy9DSBs

Second Case Investigation

Overview of Victim(s) Information

Start and End Time of The Malicious Activity

The start date of the malicious activity is:
14 Dec, 2017 00:39:37 PM.

The last malicious activity was recorded on:
15 Dec, 2017 00:49:28 PM.

Victim Email

darnell@castillomotorsports.com

Victim PC Host Name

Darnell-PC

Victim PC MAC Address

00:08:7c:39:da:12

Victim PC IP Address

10.1.1.213

Types of Noted Malicious Activities

Phishing, Malware Installation, and Suspicious Remote Access.

Indicators of Malicious Activity

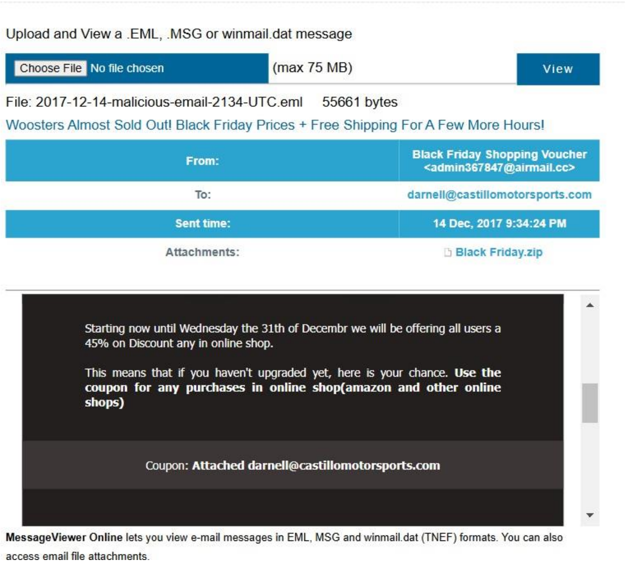
- An installed malware was identified on the victim’s PC.
- Visiting a suspicious website.
- Suspicious remote access.

Summary

On December 14th, 2017, a phishing email was sent to darnell@castillomotorsports.com containing a malicious attachment, "Black Friday.zip." Upon opening, a downloader Trojan (BlackFriday.docx,SHA256:a7447db99ba60c2f7bfd9e9bcfadfb05a4fc0ea214450b76ea85d38 6db1f727b) was executed on the victim's PC (Darnell-PC, IP: 10.1.1.213, MAC: 00:08:7c:39:da:12), The malware acted as a downloader to retrieve additional malicious content from forum.cryptopia.gdn, That then leads to downloading the malwares associated with TeamViewer.

Email Investigation

We started by uploading the mail to www.encryptomatic.com/viewer/, we can identify this mail as a phishing mail, for further investigation and confirmation let’s view the downloaded attachment.



Upload and View a .EML, .MSG or winmail.dat message

No file chosen (max 75 MB)

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

Starting now until Wednesday the 31th of Decembr we will be offering all users a 45% on Discount any in online shop.

This means that if you haven't upgraded yet, here is your chance. **Use the coupon for any purchases in online shop(amazon and other online shops)**

Coupon: **Attached darnell@castillomotorsports.com**

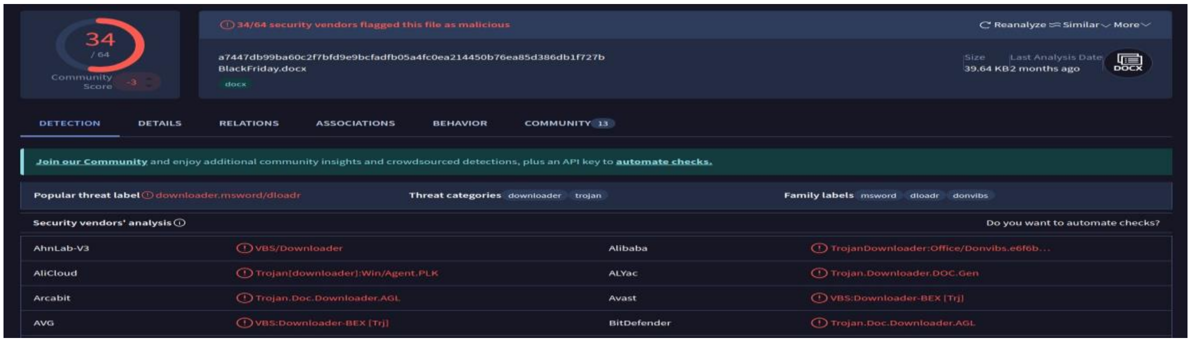
MessageViewer Online lets you view e-mail messages in EML, MSG and winmail.dat (TNEF) formats. You can also access email file attachments.

Email Attachment Analysis

Note: we have used both the attachment “Black Friday.zip” itself, and the hash using sha256sum “a7447db99ba60c2f7bfd9e9bcfadfb05a4fc0ea214450b76ea85d386db1f727b” of the attachment for the analysis.

Uploading to Virus Total

We can find that the malware was identified as downloader malware, which upon research is used for downloading more malwares.



34 / 64 Community Score -3

ⓘ 34/64 security vendors flagged this file as malicious

Reanalyze Similar More

a7447db99ba60c2f7bfd9e9bcfadfb05a4fc0ea214450b76ea85d386db1f727b
BlackFriday.docx
docx

Size 39.64 KB · Last Analysis Date 2 months ago · DOCX

DETECTION · DETAILS · RELATIONS · ASSOCIATIONS · BEHAVIOR · COMMUNITY 13

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

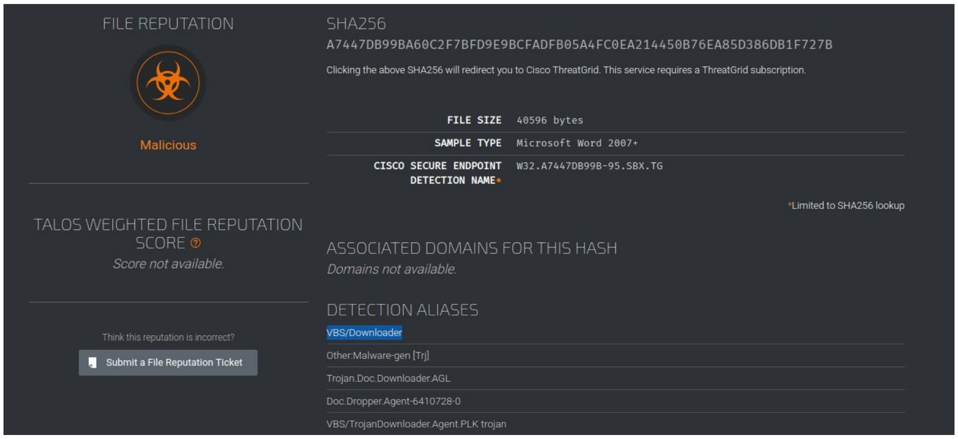
Popular threat label ⓘ downloader.msword/dloadr · Threat categories downloader trojan · Family labels msword dloadr donvibs

Security vendors' analysis ⓘ · Do you want to automate checks?

AhnLab-V3	ⓘ VBS/Downloader	Alibaba	ⓘ TrojanDownloader:Office/Donvibs.e6f6b...
AliCloud	ⓘ Trojan[downloader]:Win/Agent.PLK	ALYac	ⓘ Trojan.Downloader.DOC.Gen
Arcabit	ⓘ Trojan.Doc.Downloader.AGL	Avast	ⓘ VBS:Downloader-BEX [Trj]
AVG	ⓘ VBS:Downloader-BEX [Trj]	BitDefender	ⓘ Trojan.Doc.Downloader.AGL

Uploading to Cisco Talos

Again VBS/Downloader



FILE REPUTATION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE ?

Score not available.

Think this reputation is incorrect?

Submit a File Reputation Ticket

SHA256
A7447DB99BA60C2F7BFD9E9BCFADFB05A4FC0EA214450B76EA85D386DB1F727B

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE	40596 bytes
SAMPLE TYPE	Microsoft Word 2007+
CISCO SECURE ENDPOINT DETECTION NAME*	W32.A7447DB99B-95.SBX.TG

*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

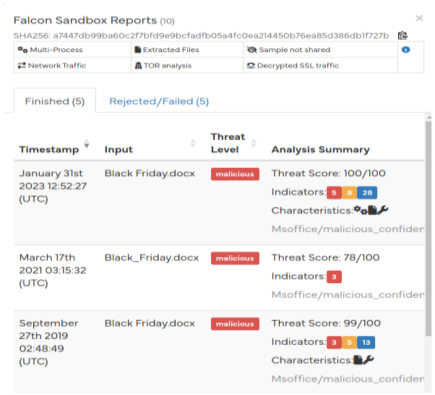
Domains not available.

DETECTION ALIASES

VBS/Downloader
Other:Malware-gen [Trj]
Trojan.Doc.Downloader.AGL
Doc.Dropper.Agent-6410728-0
VBS/TrojanDownloader.Agent.PLK trojan

Uploading to hybrid-analysis.com

Decrypted SSL Traffic, may be in association with “forum.cryptopia.gdn”.



Falcon Sandbox Reports (10)

SHA256: a7447db99ba60c2f7bfd9e9bcfadfb05a4fc0ea214450b76ea85d386db1f727b

Multi-Process	Extracted Files	Sample not shared
Network Traffic	TOR analysis	Decrypted SSL traffic

Finished (5) · Rejected/Failed (5)

Timestamp	Input	Threat Level	Analysis Summary
January 31st 2023 12:52:27 (UTC)	Black Friday.docx	malicious	Threat Score: 100/100 Indicators: 5 8 28 Characteristics: Msoffice/malicious_confiden
March 17th 2021 03:15:32 (UTC)	Black_Friday.docx	malicious	Threat Score: 78/100 Indicators: 3 Msoffice/malicious_confiden
September 27th 2019 02:48:49 (UTC)	Black Friday.docx	malicious	Threat Score: 99/100 Indicators: 3 5 13 Characteristics: Msoffice/malicious_confiden

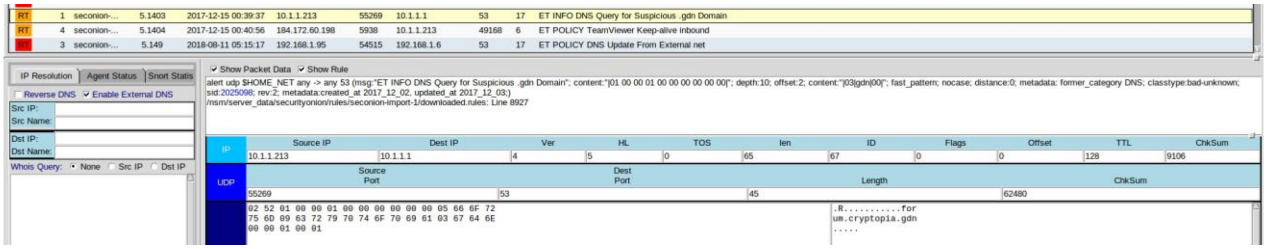
Overview of The Mail Attachment

The user seems to have installed a downloader trojan “Black Friday.docx” with the sha256sum: “a7447db99ba60c2f7bfd9e9bcfadfb05a4fc0ea214450b76ea85d386db1f727b”, upon a quick google search we can find that it’s used to download additional content, such as more malware, onto the infected computer.

Investigating Using SGUIL

We can find two associated alerts, with the IP address “10.1.1.213” belonging to Darnell.

The first event message is “ET INFO DNS Query for suspicious gdn Domain”.



```
RT   1  seconion-...  5.1403  2017-12-15 00:39:37  10.1.1.213      55269  10.1.1.1     53     17  ET INFO DNS Query for Suspicious .gdn Domain
RT   4  seconion-...  5.1404  2017-12-15 00:40:56  184.172.60.198  5938   10.1.1.213   49168  6   ET POLICY TeamViewer Keep-alive inbound
RT   3  seconion-...  5.149   2018-08-11 05:15:17  192.168.1.95    54515  192.168.1.6  53     17  ET POLICY DNS Update From External net
```

☐ Reverse DNS ☑ Enable External DNS

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert udp $HOME_NET any -> any 53 (msg:"ET INFO DNS Query for Suspicious .gdn Domain"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|03|gdn|00|"; fast_pattern; nocase; distance:0; metadata: former_category DNS; classtype:bad-unknown;
sid:2025098; rev:2; metadata:created_at 2017_12_02, updated_at 2017_12_03;)
/nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 8927
```

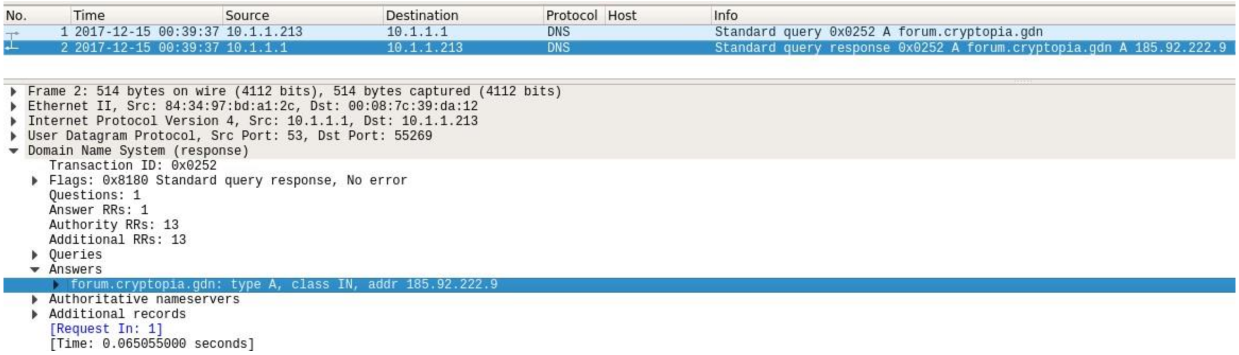
IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	10.1.1.213	10.1.1.1	4	5	0	65	67	0	0	128	9106

UDP	Source Port	Dest Port	Length	ChkSum
	55269	53	45	62480

```
02 52 01 00 00 01 00 00 00 00 00 00 05 66 6F 72    .R..........for
75 6D 09 63 72 79 70 74 6F 70 69 61 03 67 64 6E    um.cryptopia.gdn
00 00 01 00 01                                     .....
```

Wireshark Analysis

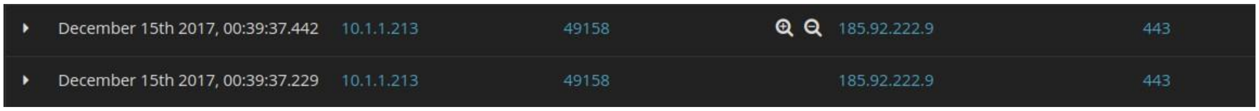
We can find that the user asked for the site “forum.cryptopia.gdn” which has the IP address “185.92.222.9”.



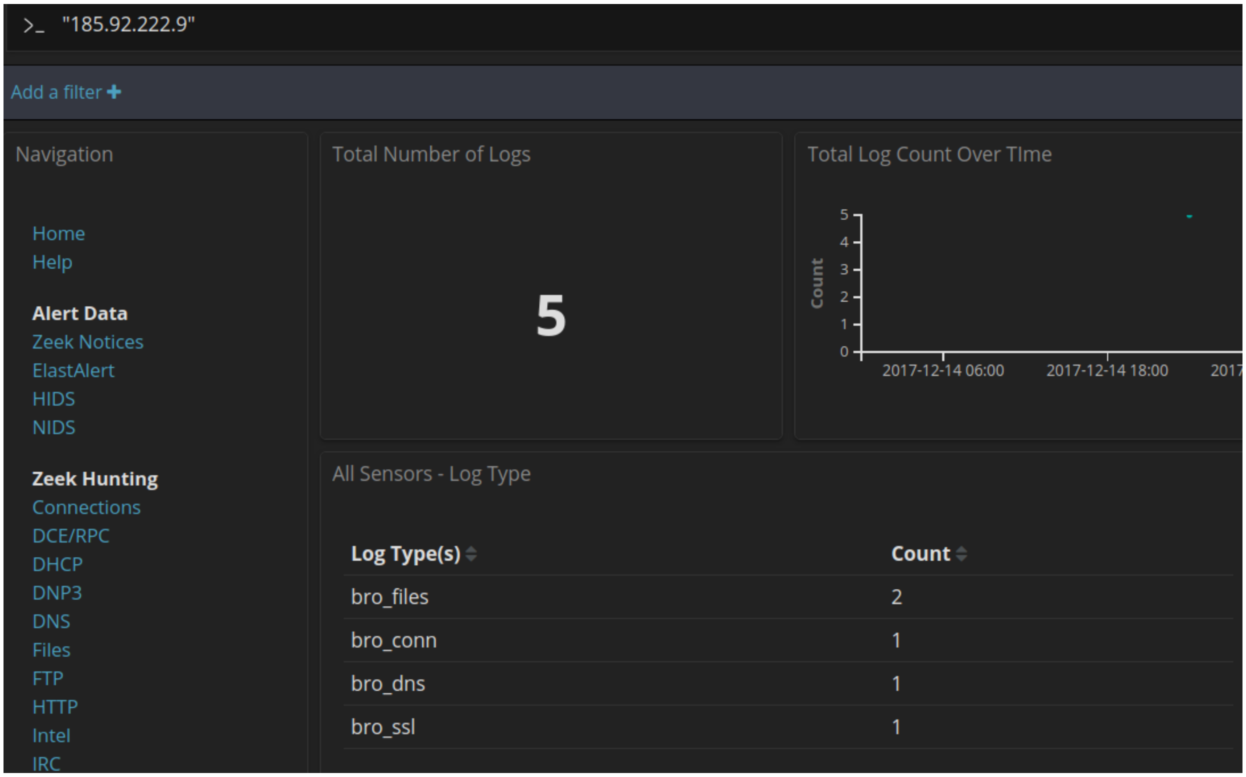
```
No.  Time                 Source      Destination  Protocol Host  Info
  1 2017-12-15 00:39:37 10.1.1.213  10.1.1.1     DNS            Standard query 0x0252 A forum.cryptopia.gdn
  2 2017-12-15 00:39:37 10.1.1.1    10.1.1.213   DNS            Standard query response 0x0252 A forum.cryptopia.gdn A 185.92.222.9

▸ Frame 2: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits)
▸ Ethernet II, Src: 84:34:97:bd:a1:2c, Dst: 00:08:7c:39:da:12
▸ Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.1.1.213
▸ User Datagram Protocol, Src Port: 53, Dst Port: 55269
▾ Domain Name System (response)
    Transaction ID: 0x0252
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 13
    Additional RRs: 13
  ▸ Queries
  ▾ Answers
    ▸ forum.cryptopia.gdn: type A, class IN, addr 185.92.222.9
  ▸ Authoritative nameservers
  ▸ Additional records
    [Request In: 1]
    [Time: 0.065055000 seconds]
```

IP Lookup Using Kibana

Upon further investigation, we found that this IP uses SSL, which means that the traffic is encrypted and leaving us with little details about what happened, we



```
▸ December 15th 2017, 00:39:37.442   10.1.1.213   49158   185.92.222.9   443
▸ December 15th 2017, 00:39:37.229   10.1.1.213   49158   185.92.222.9   443
```



```
>_ "185.92.222.9"
```

Total Number of Logs

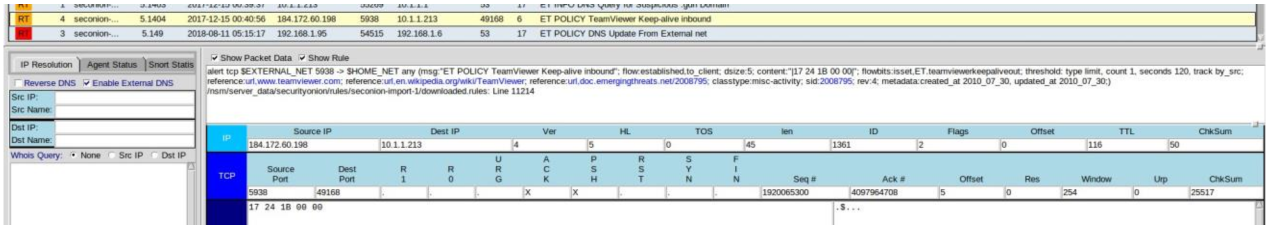
5

All Sensors - Log Type

Log Type(s)	Count
bro_files	2
bro_conn	1
bro_dns	1
bro_ssl	1

The second event message is “ET Policy TeamViewer Keep-alive inbound”.

We assume that the user has installed malware from the site “forum.cryptopia.gdn” which leads to the malware associated with TeamViewer.



```
RT  1  seconion-...  5.1403  2017-12-15 00:39:57  10.1.1.213      55269  10.1.1.1     53     17  ET INFO DNS Query for Suspicious .gq Domain
RT  4  seconion-...  5.1404  2017-12-15 00:40:56  184.172.60.198  5938   10.1.1.213   49168  6   ET POLICY TeamViewer Keep-alive inbound
RT  3  seconion-...  5.149   2018-08-11 05:15:17  192.168.1.95    54515  192.168.1.6  53     17  ET POLICY DNS Update From External net
```

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET 5938 -> $HOME_NET any (msg:"ET POLICY TeamViewer Keep-alive inbound"; flow:established,to_client; dsize:5; content:"|17 24 1B 00 00|"; flowbits:isset,ET.teamviewerkeepaliveout; threshold: type limit, count 1, seconds 120, track by_src; reference:url,www.teamviewer.com; reference:url,en.wikipedia.org/wiki/TeamViewer; reference:url,doc.emergingthreats.net/2008795; classtype:misc-activity; sid:2008795; rev:4; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
/nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 11214
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	184.172.60.198	10.1.1.213	4	5	0	45	1361	2	0	116	50

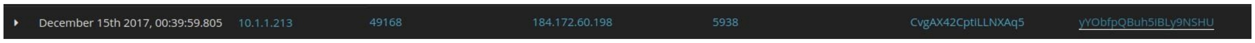
TCP	Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	5938	49168	.	.	.	X	X	.	.	.	1920065300	4097964708	5	0	254	0	25517

```
17 24 1B 00 00                                   .$...
```

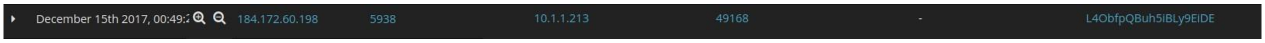
IP Resolution
Agent Status
Snort Statis
□ Reverse DNS ☑ Enable External DNS
Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: ● None ○ Src IP ○ Dst IP

Further Investigation Using Kibana

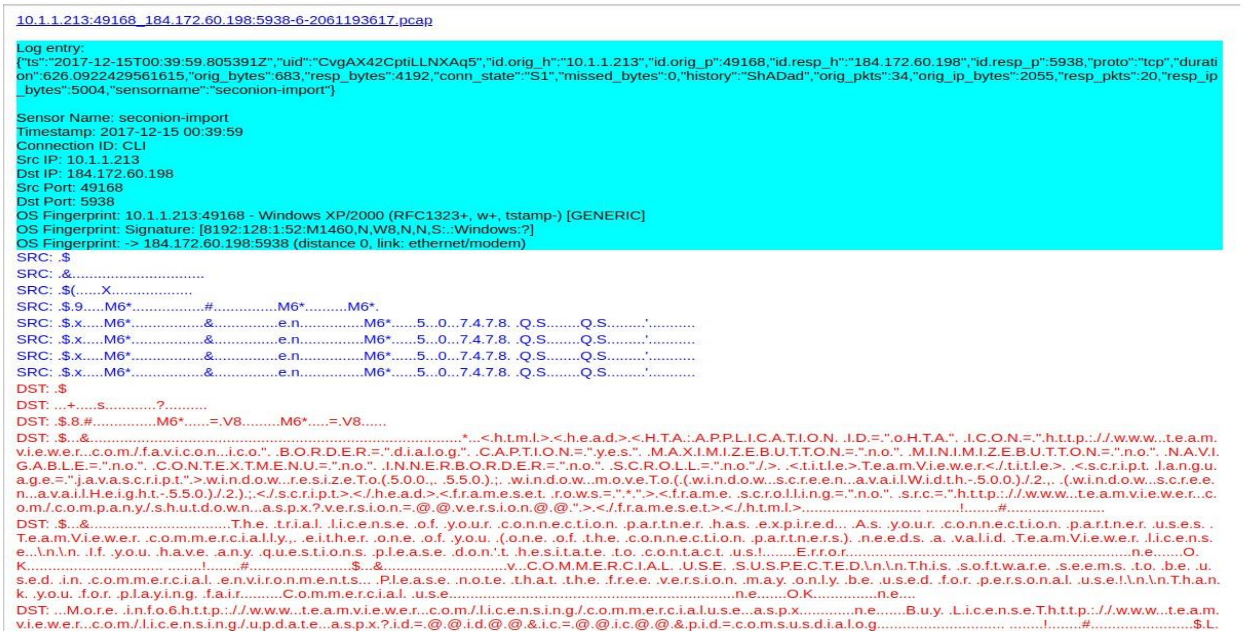
We can see that the user Chris “10.1.1.213” initiated the connection with “184.172.60.198”, upon more investigation we can also find the IP “184.172.60.198” is using port 5938, which upon Google search, we can conclude that it’s acting as a TeamViewer server that our user Chris “10.1.1.213” is trying to connect on.



```
December 15th 2017, 00:39:59.805   10.1.1.213   49168   184.172.60.198   5938   CvgAX42CptiLLNXAq5   yYObfpQBuh5iBLy9NSHU
```

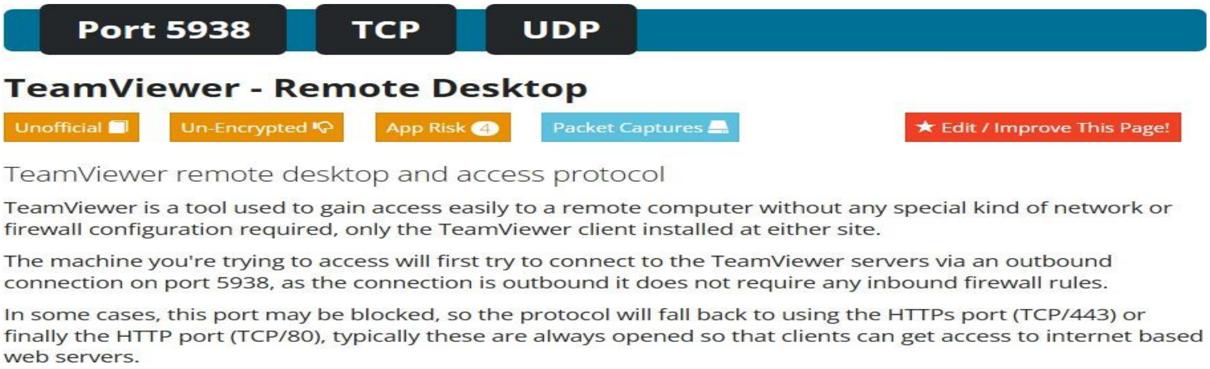


```
December 15th 2017, 00:49:2   184.172.60.198   5938   10.1.1.213   49168   -   L4ObfpQBuh5iBLy9EIDE
```



10.1.1.213:49168_184.172.60.198:5938-6-2061193617.pcap

```
Log entry:
{"ts":"2017-12-15T00:39:59.805391Z","uid":"CvgAX42CptiLLNXAq5","id.orig_h":"10.1.1.213","id.orig_p":49168,"id.resp_h":"184.172.60.198","id.resp_p":5938,"proto":"tcp","duration":626.0922429561615,"orig_bytes":683,"resp_bytes":4192,"conn_state":"S1","missed_bytes":0,"history":"ShADad","orig_pkts":34,"orig_ip_bytes":2055,"resp_pkts":20,"resp_ip_bytes":5004,"sensorname":"seconion-import"}

Sensor Name: seconion-import
Timestamp: 2017-12-15 00:39:59
Connection ID: CLI
Src IP: 10.1.1.213
Dst IP: 184.172.60.198
Src Port: 49168
Dst Port: 5938
OS Fingerprint: 10.1.1.213:49168 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint: -> 184.172.60.198:5938 (distance 0, link: ethernet/modem)
SRC: .$
SRC: .&..............................
SRC: .$(......X..................
SRC: .$.9.....M6*................#..............M6*..........M6*.
SRC: .$.x.....M6*................&..............e.n..............M6*......5...0...7.4.7.8. .Q.S........Q.S.........'..........
SRC: .$.x.....M6*................&..............e.n..............M6*......5...0...7.4.7.8. .Q.S........Q.S.........'..........
SRC: .$.x.....M6*................&..............e.n..............M6*......5...0...7.4.7.8. .Q.S........Q.S.........'..........
SRC: .$.x.....M6*................&..............e.n..............M6*......5...0...7.4.7.8. .Q.S........Q.S.........'..........
DST: .$
DST: ...+.....s............?..........
DST: .$.8.#...............M6*......=.V8.........M6*.....=.V8......
DST: .$...&..........................................................................*...<.h.t.m.l.>.<.h.e.a.d.>.<.H.T.A.:.A.P.P.L.I.C.A.T.I.O.N. .I.D.=.".o.H.T.A.". .I.C.O.N.=.".h.t.t.p.:././.w.w.w...t.e.a.m.v.i.e.w.e.r...c.o.m./.f.a.v.i.c.o.n...i.c.o.". .B.O.R.D.E.R.=.".d.i.a.l.o.g.". .C.A.P.T.I.O.N.=.".y.e.s.". .M.A.X.I.M.I.Z.E.B.U.T.T.O.N.=.".n.o.". .M.I.N.I.M.I.Z.E.B.U.T.T.O.N.=.".n.o.". .N.A.V.I.G.A.B.L.E.=.".n.o.". .C.O.N.T.E.X.T.M.E.N.U.=.".n.o.". .I.N.N.E.R.B.O.R.D.E.R.=.".n.o.". .S.C.R.O.L.L.=.".n.o."./.>. .<.t.i.t.l.e.>.T.e.a.m.V.i.e.w.e.r.<./.t.i.t.l.e.>. .<.s.c.r.i.p.t. .l.a.n.g.u.a.g.e.=.".j.a.v.a.s.c.r.i.p.t.".>.w.i.n.d.o.w...r.e.s.i.z.e.T.o.(.5.0.0.,. .5.5.0.).;. .w.i.n.d.o.w...m.o.v.e.T.o.(.(.w.i.n.d.o.w...s.c.r.e.e.n...a.v.a.i.l.W.i.d.t.h.-.5.0.0.)./.2.,. .(.w.i.n.d.o.w...s.c.r.e.e.n...a.v.a.i.l.H.e.i.g.h.t.-.5.5.0.)./.2.).;.<./.s.c.r.i.p.t.>.<./.h.e.a.d.>.<.f.r.a.m.e.s.e.t. .r.o.w.s.=.".*.".>.<.f.r.a.m.e. .s.c.r.o.l.l.i.n.g.=.".n.o.". .s.r.c.=.".h.t.t.p.:././.w.w.w...t.e.a.m.v.i.e.w.e.r...c.o.m./.c.o.m.p.a.n.y./.s.h.u.t.d.o.w.n...a.s.p.x.?.v.e.r.s.i.o.n.=.@.@.v.e.r.s.i.o.n.@.@.".>.<./.f.r.a.m.e.s.e.t.>.<./.h.t.m.l.>......................... ........!........#......................
DST: .$...&..............................T.h.e. .t.r.i.a.l. .l.i.c.e.n.s.e. .o.f. .y.o.u.r. .c.o.n.n.e.c.t.i.o.n. .p.a.r.t.n.e.r. .h.a.s. .e.x.p.i.r.e.d... .A.s. .y.o.u.r. .c.o.n.n.e.c.t.i.o.n. .p.a.r.t.n.e.r. .u.s.e.s. .T.e.a.m.V.i.e.w.e.r. .c.o.m.m.e.r.c.i.a.l.l.y.,. .e.i.t.h.e.r. .o.n.e. .o.f. .y.o.u. .(.o.n.e. .o.f. .t.h.e. .c.o.n.n.e.c.t.i.o.n. .p.a.r.t.n.e.r.s.). .n.e.e.d.s. .a. .v.a.l.i.d. .T.e.a.m.V.i.e.w.e.r. .l.i.c.e.n.s.e...\.n.\.n. .I.f. .y.o.u. .h.a.v.e. .a.n.y. .q.u.e.s.t.i.o.n.s. .p.l.e.a.s.e. .d.o.n.'.t. .h.e.s.i.t.a.t.e. .t.o. .c.o.n.t.a.c.t. .u.s.!........E.r.r.o.r...........................................................................n.e.......O.K.............................. ........!........#.......................$...&..........................v...C.O.M.M.E.R.C.I.A.L. .U.S.E. .S.U.S.P.E.C.T.E.D.\.n.\.n.T.h.i.s. .s.o.f.t.w.a.r.e. .s.e.e.m.s. .t.o. .b.e. .u.s.e.d. .i.n. .c.o.m.m.e.r.c.i.a.l. .e.n.v.i.r.o.n.m.e.n.t.s... .P.l.e.a.s.e. .n.o.t.e. .t.h.a.t. .t.h.e. .f.r.e.e. .v.e.r.s.i.o.n. .m.a.y. .o.n.l.y. .b.e. .u.s.e.d. .f.o.r. .p.e.r.s.o.n.a.l. .u.s.e.!.\.n.\.n.T.h.a.n.k. .y.o.u. .f.o.r. .p.l.a.y.i.n.g. .f.a.i.r.........C.o.m.m.e.r.c.i.a.l. .u.s.e...................................................................n.e.......O.K...............n.e....
DST: ...M.o.r.e. .i.n.f.o.6.h.t.t.p.:././.w.w.w...t.e.a.m.v.i.e.w.e.r...c.o.m./.l.i.c.e.n.s.i.n.g./.c.o.m.m.e.r.c.i.a.l.u.s.e...a.s.p.x............n.e.......B.u.y. .L.i.c.e.n.s.e.T.h.t.t.p.:././.w.w.w...t.e.a.m.v.i.e.w.e.r...c.o.m./.l.i.c.e.n.s.i.n.g./.u.p.d.a.t.e...a.s.p.x.?.i.d.=.@.@.i.d.@.@.&.i.c.=.@.@.i.c.@.@.&.p.i.d.=.c.o.m.s.u.s.d.i.a.l.o.g........................... ........!........#.......................$.L.
```



TeamViewer - Remote Desktop

TeamViewer remote desktop and access protocol

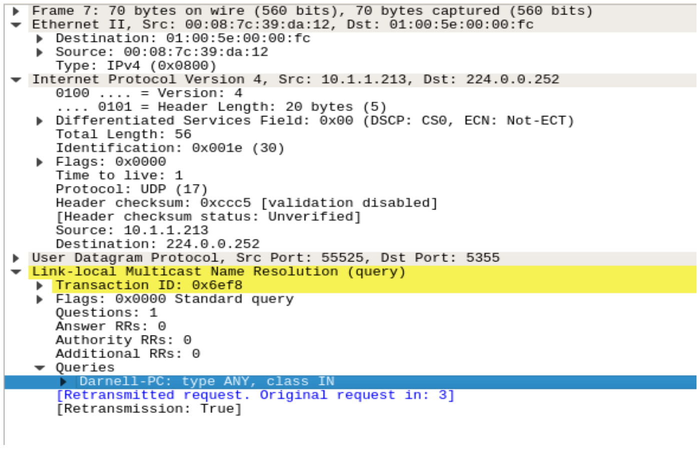
TeamViewer is a tool used to gain access easily to a remote computer without any special kind of network or firewall configuration required, only the TeamViewer client installed at either site.

The machine you're trying to access will first try to connect to the TeamViewer servers via an outbound connection on port 5938, as the connection is outbound it does not require any inbound firewall rules.

In some cases, this port may be blocked, so the protocol will fall back to using the HTTPs port (TCP/443) or finally the HTTP port (TCP/80), typically these are always opened so that clients can get access to internet based web servers.

Identifying The Host Using Wireshark

We have investigated the associated pcap file "2017-12-15-traffic-analysis-exercise-2-of-2.pcap", to extract the host information associated with the IP address "10.1.1.213", host-pc-name: "Darnell-PC", host-MAC-address: "00:08:7c:39:da:12".

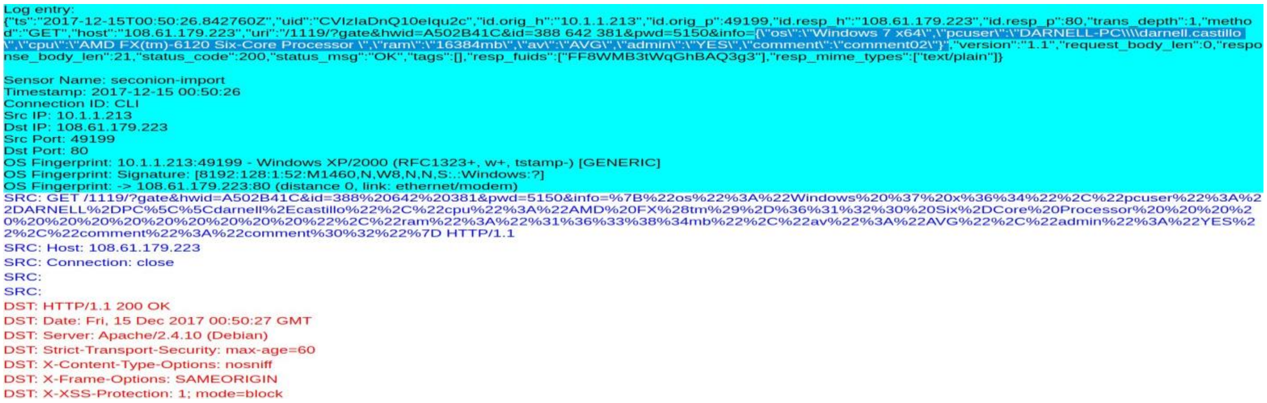


```
▶ Frame 7: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
▼ Ethernet II, Src: 00:08:7c:39:da:12, Dst: 01:00:5e:00:00:fc
  ▶ Destination: 01:00:5e:00:00:fc
  ▶ Source: 00:08:7c:39:da:12
    Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 10.1.1.213, Dst: 224.0.0.252
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x001e (30)
  ▶ Flags: 0x0000
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0xccc5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.1.1.213
    Destination: 224.0.0.252
▶ User Datagram Protocol, Src Port: 55525, Dst Port: 5355
▼ Link-local Multicast Name Resolution (query)
  ▶ Transaction ID: 0x6ef8
  ▶ Flags: 0x0000 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ Darnell-PC: type ANY, class IN
    [Retransmitted request. Original request in: 3]
    [Retransmission: True]
```

Further Investigation Using Kibana

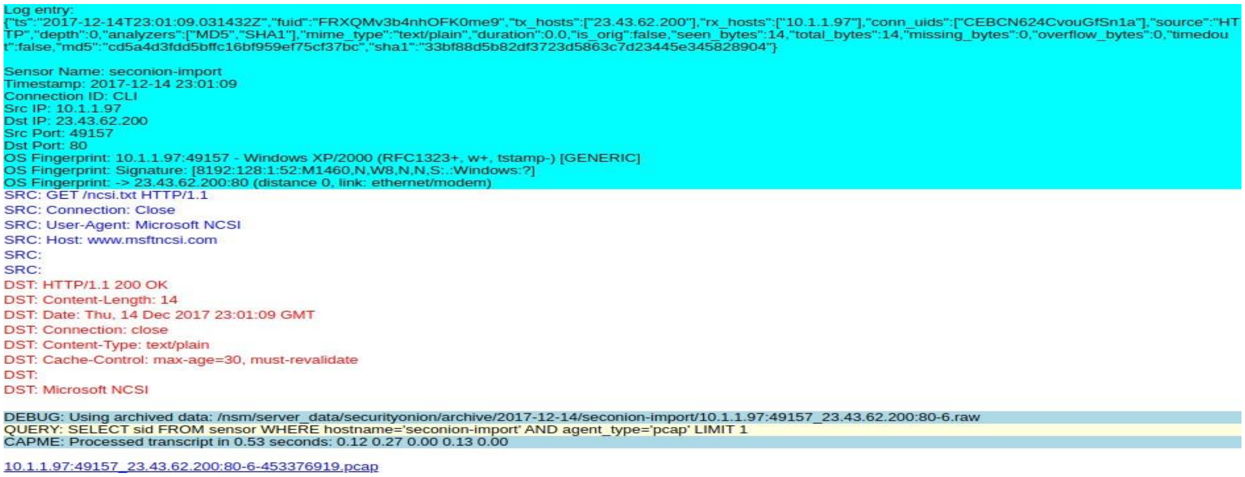
Suspicious Logs

We couldn't identify the motivation behind this log, however, the inclusion of PC information within it seems suspicious, We can identify a suspicious URL-encoded request with Darnell-PC Information.



```
Log entry:
{"ts":"2017-12-15T00:50:26.842760Z","uid":"CVIzIaDnQ10eIqu2c","id.orig_h":"10.1.1.213","id.orig_p":49199,"id.resp_h":"108.61.179.223","id.resp_p":80,"trans_depth":1,"metho
d":"GET","host":"108.61.179.223","uri":"/1119/?gate&hwid=A502B41C&id=388 642 381&pwd=5150&info={\"os\":\"Windows 7 x64\",\"pcuser\":\"DARNELL-PC\\\\darnell.castillo
\",\"cpu\":\"AMD FX(tm)-6120 Six-Core Processor \",\"ram\":\"16384mb\",\"av\":\"AVG\",\"admin\":\"YES\",\"comment\":\"comment02\"}","version":"1.1","request_body_len":0,"respo
nse_body_len":21,"status_code":200,"status_msg":"OK","tags":[],"resp_fuids":["FF8WMB3tWqGhBAQ3g3"],"resp_mime_types":["text/plain"]}

Sensor Name: seconion-import
Timestamp: 2017-12-15 00:50:26
Connection ID: CLI
Src IP: 10.1.1.213
Dst IP: 108.61.179.223
Src Port: 49199
Dst Port: 80
OS Fingerprint: 10.1.1.213:49199 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S::Windows:?]
OS Fingerprint: -> 108.61.179.223:80 (distance 0, link: ethernet/modem)
SRC: GET /1119/?gate&hwid=A502B41C&id=388%20642%20381&pwd=5150&info=%7B%22os%22%3A%22Windows%20%37%20x%36%34%22%2C%22pcuser%22%3A%2
2DARNELL%2DPC%5C%5Cdarnell%2Ecastillo%22%2C%22cpu%22%3A%22AMD%20FX%28tm%29%2D%36%31%32%30%20Six%2DCore%20Processor%20%20%20%2
0%20%20%20%20%20%20%20%20%20%22%2C%22ram%22%3A%22%31%36%33%38%34mb%22%2C%22av%22%3A%22AVG%22%2C%22admin%22%3A%22YES%2
2%2C%22comment%22%3A%22comment%30%32%22%7D HTTP/1.1
SRC: Host: 108.61.179.223
SRC: Connection: close
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 15 Dec 2017 00:50:27 GMT
DST: Server: Apache/2.4.10 (Debian)
DST: Strict-Transport-Security: max-age=60
DST: X-Content-Type-Options: nosniff
DST: X-Frame-Options: SAMEORIGIN
DST: X-XSS-Protection: 1; mode=block
```

Here is another log, that seems to be a request for a ncsi.txt file, which is associated with checking the network connection.



```
Log entry:
{"ts":"2017-12-14T23:01:09.031432Z","fuid":"FRXQMv3b4nhOFK0me9","tx_hosts":["23.43.62.200"],"rx_hosts":["10.1.1.97"],"conn_uids":["CEBCN624CvouGfSn1a"],"source":"HT
TP","depth":0,"analyzers":["MD5","SHA1"],"mime_type":"text/plain","duration":0.0,"is_orig":false,"seen_bytes":14,"total_bytes":14,"missing_bytes":0,"overflow_bytes":0,"timedou
t":false,"md5":"cd5a4d3fdd5bffc16bf959ef75cf37bc","sha1":"33bf88d5b82df3723d5863c7d23445e345828904"}

Sensor Name: seconion-import
Timestamp: 2017-12-14 23:01:09
Connection ID: CLI
Src IP: 10.1.1.97
Dst IP: 23.43.62.200
Src Port: 49157
Dst Port: 80
OS Fingerprint: 10.1.1.97:49157 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S::Windows:?]
OS Fingerprint: -> 23.43.62.200:80 (distance 0, link: ethernet/modem)
SRC: GET /ncsi.txt HTTP/1.1
SRC: Connection: Close
SRC: User-Agent: Microsoft NCSI
SRC: Host: www.msftncsi.com
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Content-Length: 14
DST: Date: Thu, 14 Dec 2017 23:01:09 GMT
DST: Connection: close
DST: Content-Type: text/plain
DST: Cache-Control: max-age=30, must-revalidate
DST:
DST: Microsoft NCSI

DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2017-12-14/seconion-import/10.1.1.97:49157_23.43.62.200:80-6.raw
QUERY: SELECT sid FROM sensor WHERE hostname='seconion-import' AND agent_type='pcap' LIMIT 1
CAPME: Processed transcript in 0.53 seconds: 0.12 0.27 0.00 0.13 0.00

10.1.1.97:49157_23.43.62.200:80-6-453376919.pcap
```

The Relationship Between The Two Incidents

We believe that those are two separate incidents for the following reasons:

- Usage of different company mails.
  Darnell is using the email darnell@castillomotorsports.com
  Chris is using the email chris.lyons@supercarcenterdetroit.com
- We have collected no evidence proving any relation between the two incidents.

Perhaps the similarity of the IP Addresses, “10.1.1.9” and “10.1.1.213” comes from the fact that they are private ip addresses, which can be used for different companies.

The similarities between the two incidents are:

- Both incidents started around the same date.

  The first incident alert was on 14 Dec 2017 at 23:03:58 PM.
  The second incident alert was on 15 Dec 2017 at 00:39:37 PM.

- Both victims were victims of a phishing mail containing malware.
  Darnel has installed the malware attachment “Black Friday.zip”.
  Chris has installed the malware attachment “Proforma Invoice P101092292891 TT slip .pdf.rar.zip”.

Mitigation Strategies:

Immediate actions:

- Isolate the infected devices
- Malware removal
- Disabling remote access
- Block the malicious IPs discovered

Long-term actions:

- DNS filtering
- Implement an email gateway solution
- Implement DLP solution
- Install EDR and A/V on endpoint devices