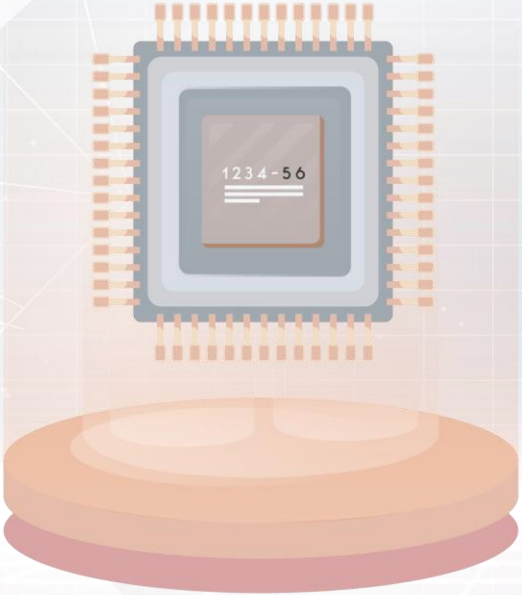


# NTI - CyberOps Presentation

# TABLE OF CONTENTS

01

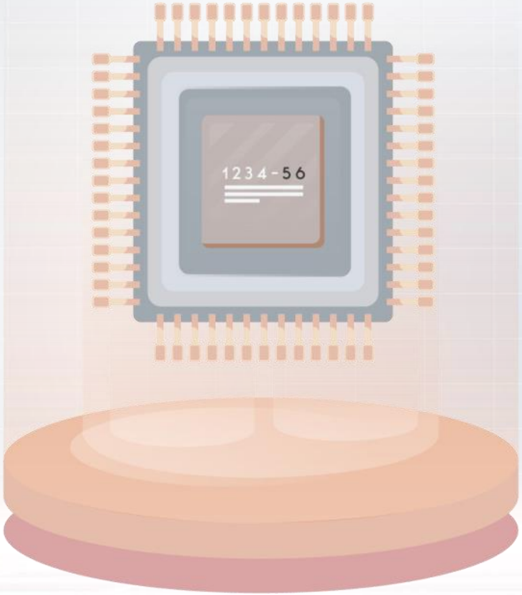
INCIDENT 01 Investigation

02

INCIDENT 02 Investigation

0
3

INVESTIGATION Conclusion

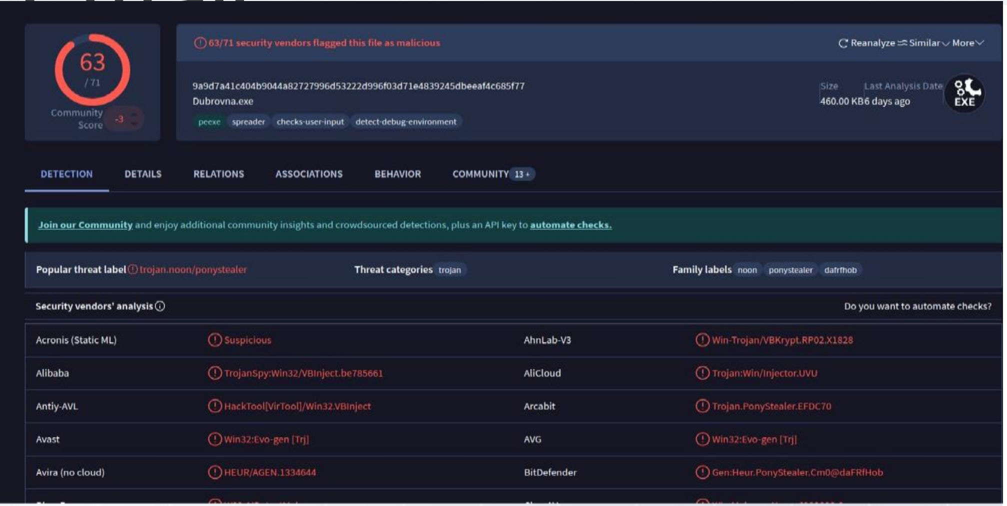


# 01

# INCIDENT 01

‘Investigating a Credential Stealer Malware.’

# A Look at The Phishing Email



63/71 security vendors flagged this file as malicious

9a9d7a41c404b9044a82727996d53222d996f03d71e4839245dbeeaf4c685f77
Dubrovna.exe
peexe spreader checks-user-input detect-debug-environment

Size 460.00 KB
Last Analysis Date 6 days ago

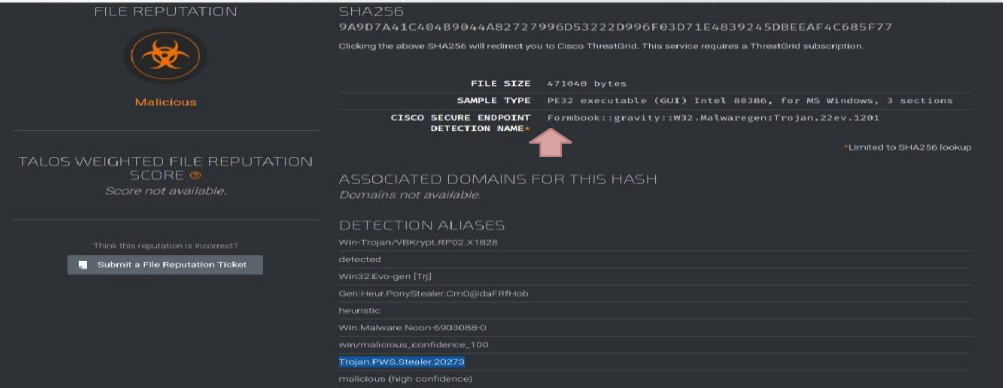
DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY 13 +

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

Popular threat label trojan.noon/ponystealer
Threat categories trojan
Family labels noon ponystealer dafrfhob

Security vendors' analysis
Do you want to automate checks?

| | | | |
|---|---|---|---|
| Acronis (Static ML) | Suspicious | AhnLab-V3 | Win-Trojan/VBKrypt.RP02.X1828 |
| Alibaba | TrojanSpy:Win32/VBInject.be785661 | AliCloud | Trojan:Win/Injector.UVU |
| Antiy-AVL | HackTool[VirTool]/Win32.VBInject | Arcabit | Trojan.PonyStealer.EFDC70 |
| Avast | Win32:Evo-gen [Trj] | AVG | Win32:Evo-gen [Trj] |
| Avira (no cloud) | HEUR/AGEN.1334644 | BitDefender | Gen:Heur.PonyStealer.Cm0@daFRfHob |



FILE REPUTATION

TALOS WEIGHTED FILE REPUTATION SCORE
*Score not available.*

Think this reputation is incorrect?

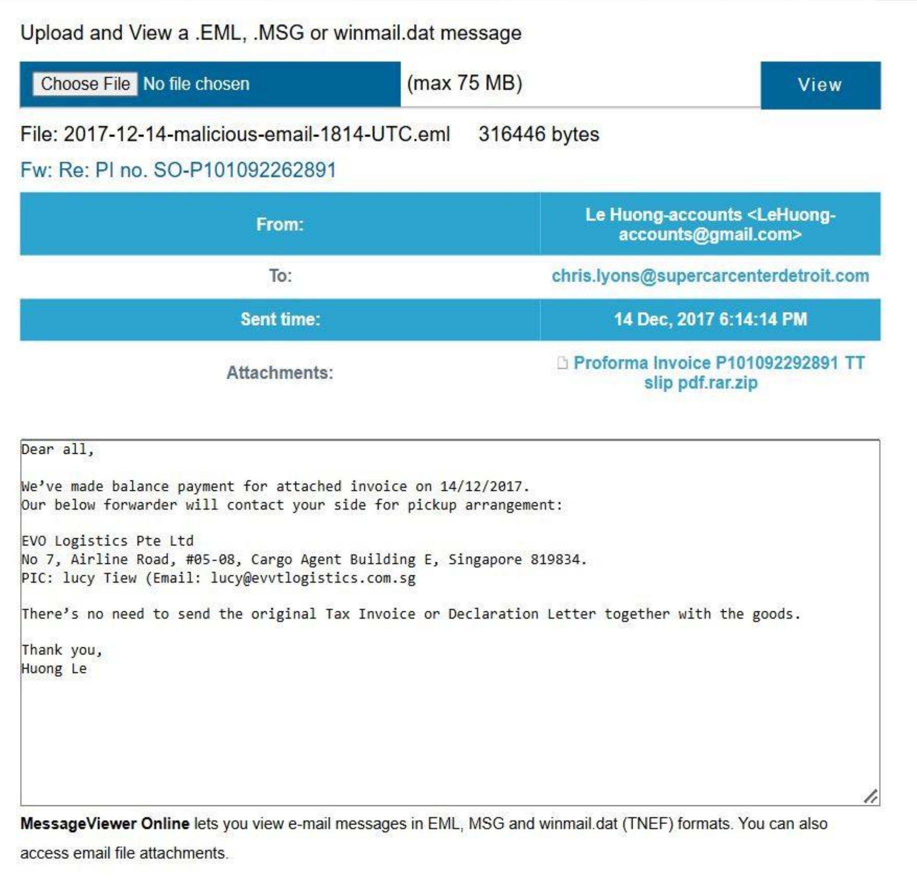
SHA256
9A9D7A41C404B9044A82727996D53222D996F03D71E4839245DBEEAF4C685F77
Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

| | |
|---|---|
| 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)



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

(max 75 MB)

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

Fw: Re: PI no. SO-P101092262891

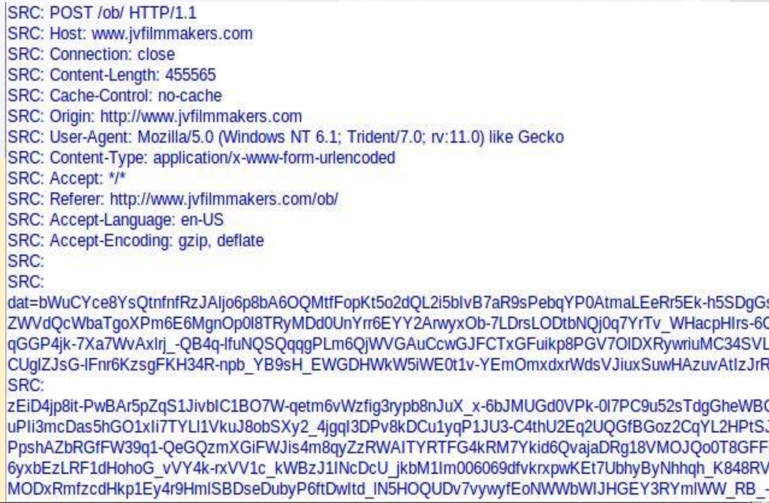
| | |
|---|---|
| From: | Le Huong-accounts <LeHuong-accounts@gmail.com> |
| To: | chris.lyons@supercarcenterdetroit.com |
| Sent time: | 14 Dec, 2017 6:14:14 PM |
| Attachments: | Proforma Invoice P101092292891 TT slip pdf.rar.zip |

```
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
```

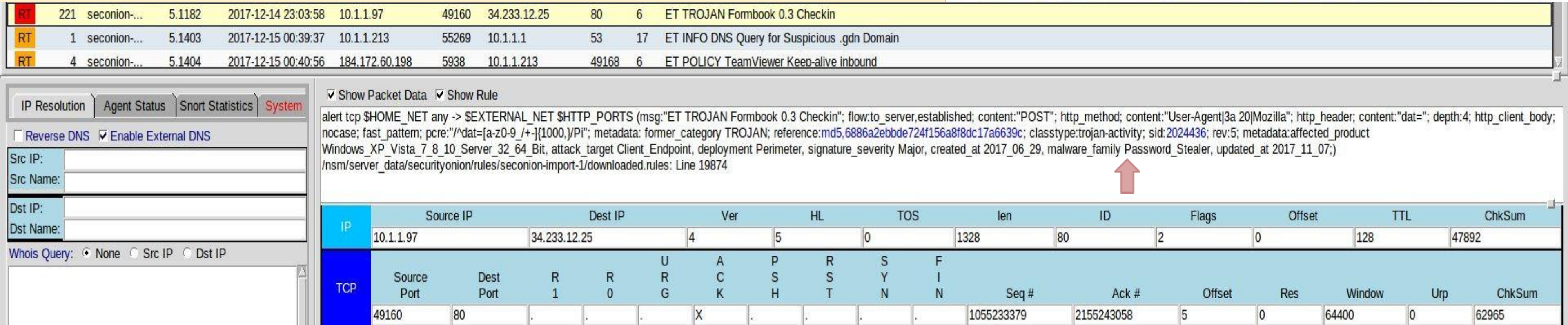
**MessageViewer Online** lets you view e-mail messages in EML, MSG and winmail.dat (TNEF) formats. You can also access email file attachments.

# Investigating Using SGUIL

- **Alert01 ET TROJAN Formbook 0.3 Checkin**
- **Possible Data Exfiltration**



```
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-h5SDgGs
ZWVdQcWbaTgoXPm6E6MgnOp0l8TRyMDd0UnYrr6EYY2ArwyxOb-7LDrsLODtbNQj0q7YrTv_WHacpHlrs-6C
qGGP4jk-7Xa7WvAxlrj_-QB4q-lfuNQSQqqgPLm6QjWVGAuCcwGJFCTxGFuikp8PGV7OlDXRywriuMC34SVL
CUglZJsG-lFnr6KzsgFKH34R-npb_YB9sH_EWGDHWkW5iWE0t1v-YEmOmxdxrWdsVJiuxSuwHAzuvAtIzJrR
SRC:
zEiD4jp8it-PwBAr5pZqS1JivblC1BO7W-qetm6vWzfig3rypb8nJuX_x-6bJMUGd0VPk-0l7PC9u52sTdgGheWBC
uPli3mcDas5hGO1xli7TYLI1VkuJ8obSXy2_4jgql3DPv8kDCu1yqP1JU3-C4thU2Eq2UQGfBGoz2CqYL2HPtSJ
PpshAZbRGfFW39q1-QeGQzmXGiFWJis4m8qyZzRWAITYRTFG4kRM7Ykid6QvajaDRg18VMOJQo0T8GFF
6yxbEzLRF1dHohoG_vVY4k-rxVV1c_kWBzJ1INcDcU_jkbM1Im006069dfvkrxpwKEt7UbhyByNhhqh_K848RV
MODxRmfzcdHkp1Ey4r9HmlSBDseDubyP6ftDwltd_IN5HOQUDv7vywyfEoNWWbWIJHGEY3RYmlWW_RB_-
```



```
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
```

☐ Reverse DNS ☑ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

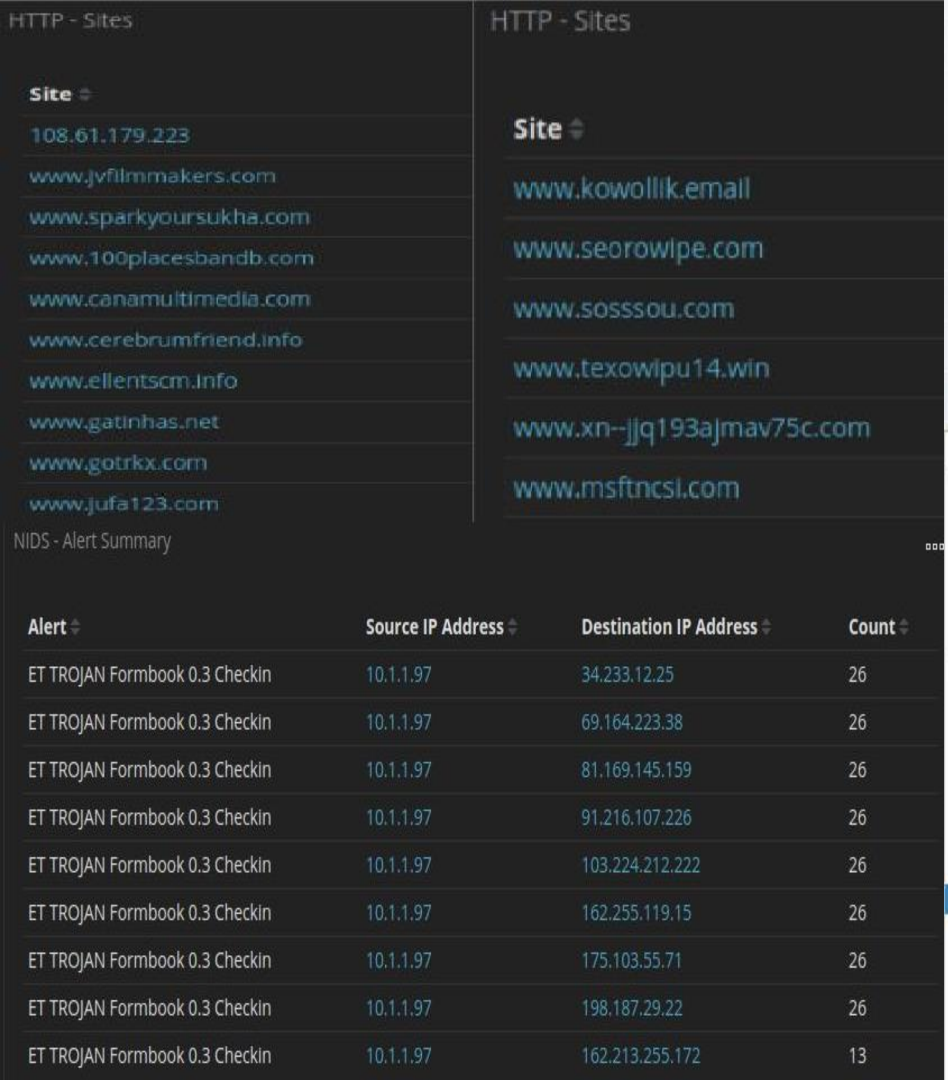
☑ Show Packet Data ☑ Show Rule

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

# Further Investigation



HTTP - Sites

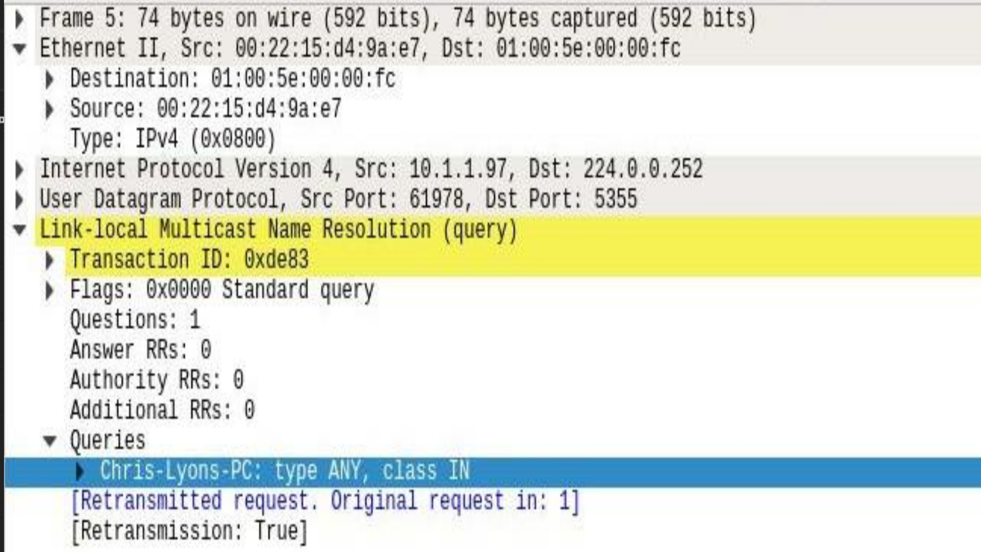
| Site |
|---|
| 108.61.179.223 |
| www.jvfilmmakers.com |
| www.sparkyoursukha.com |
| www.100placesbandb.com |
| www.canamultimedia.com |
| www.cerebrumfriend.info |
| www.ellentscm.info |
| www.gatinhas.net |
| www.gotrkx.com |
| www.jufa123.com |

HTTP - Sites

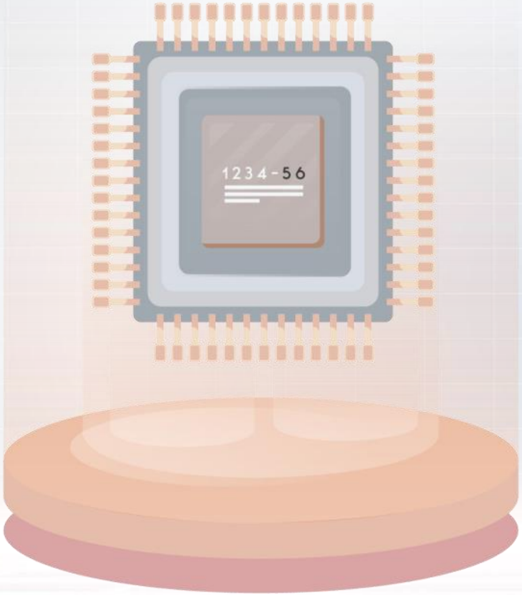
| Site |
|---|
| www.kowollik.email |
| www.seorowlpe.com |
| www.sosssou.com |
| www.texowipu14.win |
| www.xn--jjq193ajmav75c.com |
| www.msftncsi.com |

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 |



```
▸ 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]
```

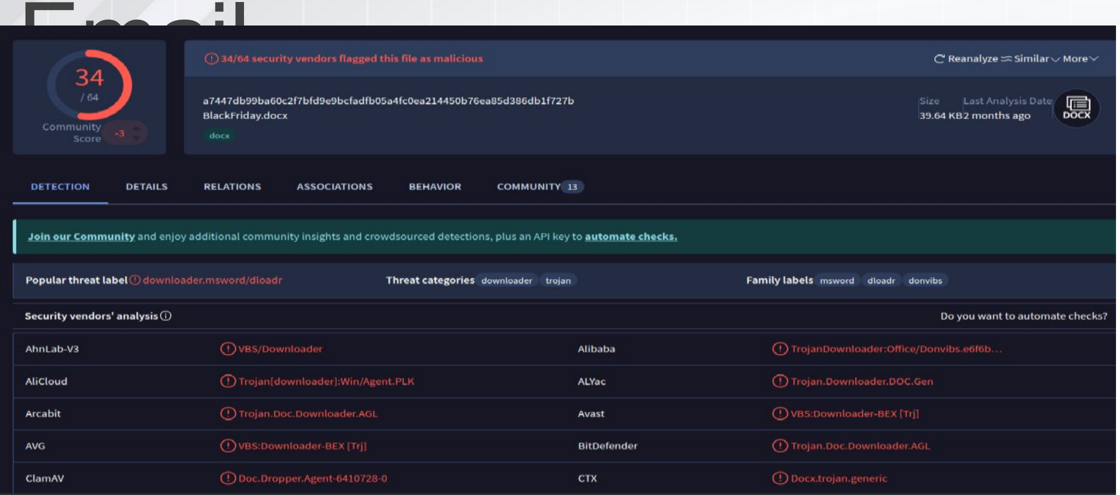


# 02

## INCIDENT 02

‘Investigating a Downloader Trojan.’

# A Look at The Phishing Email



34 / 64

Community Score -3

34/64 security vendors flagged this file as malicious

a7447db99ba60c2f7bfd9e9bcfadfb05a4fc0ea214450b76ea85d386db1f727b
BlackFriday.docx
docx

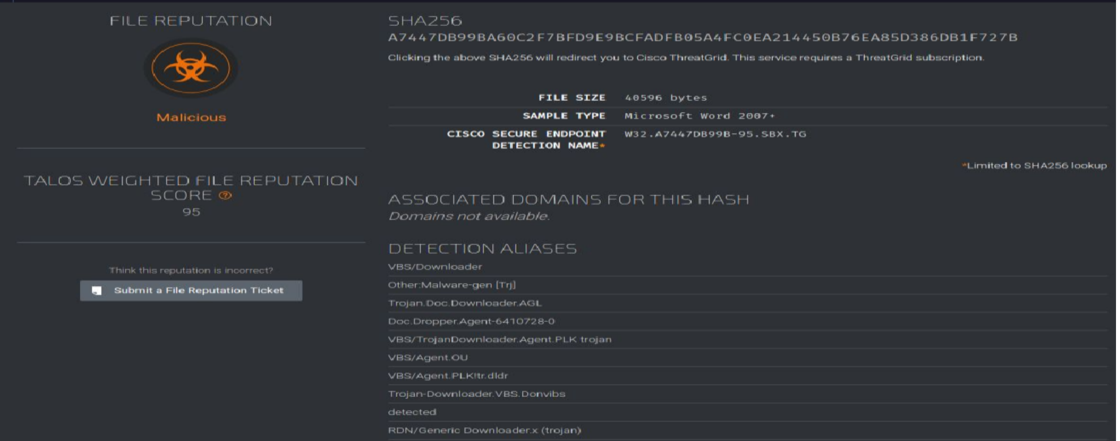
Size 39.64 KB
Last Analysis Date 2 months ago

**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 |
| ClamAV | ⓘ Doc.Dropper.Agent-6410728-0 | CTX | ⓘ Docx.trojan.generic |



FILE REPUTATION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE
95

Think this reputation is incorrect?

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 |

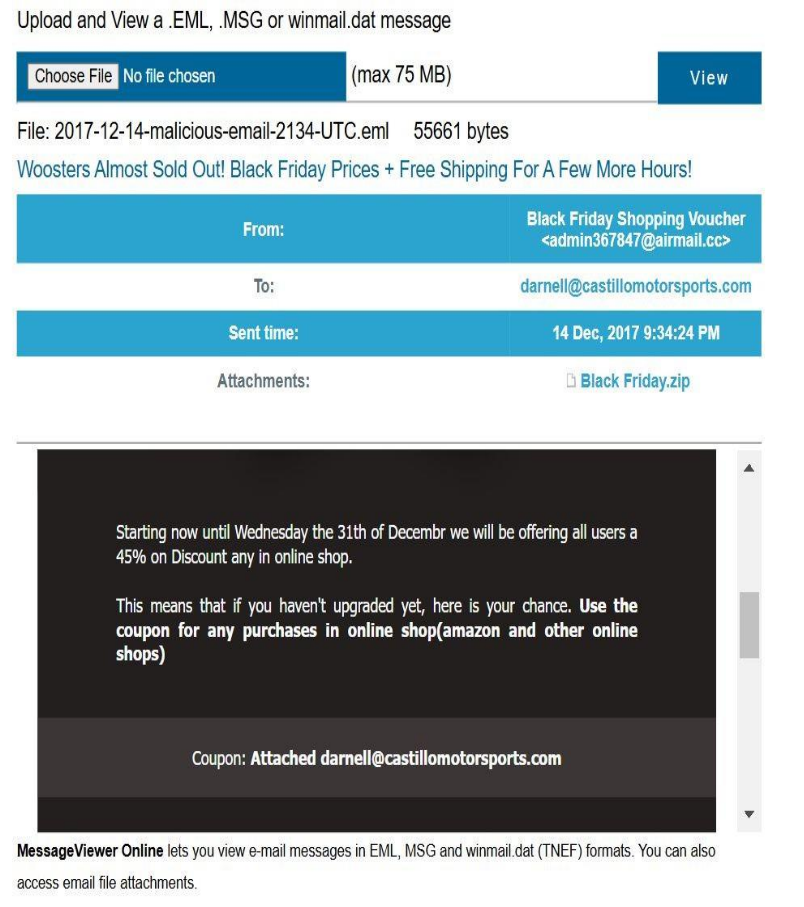
*Limited to SHA256 lookup

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
VBS/Agent.OU
VBS/Agent.PLK!tr.dldr
Trojan-Downloader.VBS.Donvibs
detected
RDN/Generic Downloader.x (trojan)



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

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 |

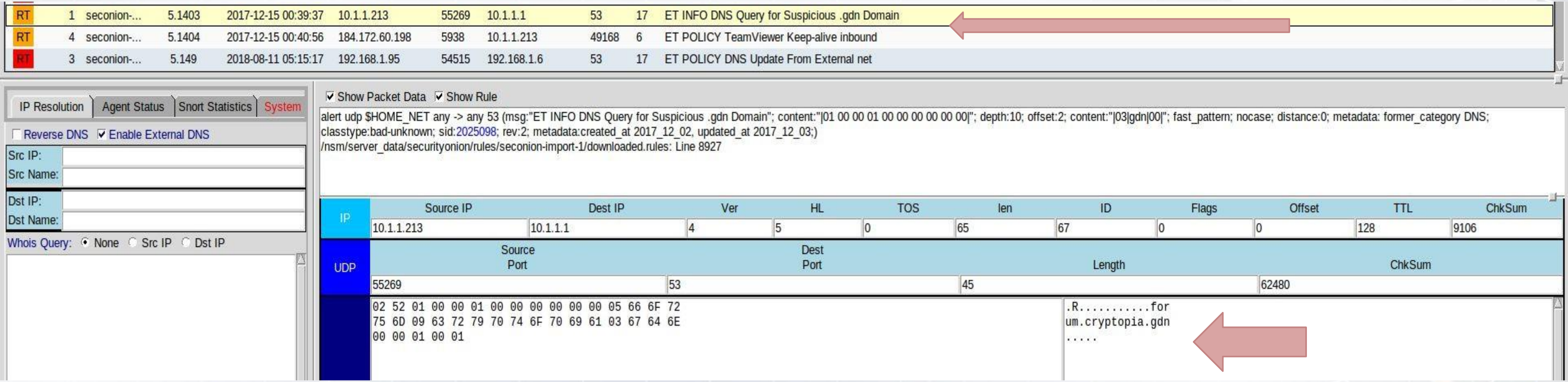
Starting now until Wednesday the 31th of Decembr we will be offering all users a 45% on Discount any in online shop.

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.

# Investigating Using SGUIL



```
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

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

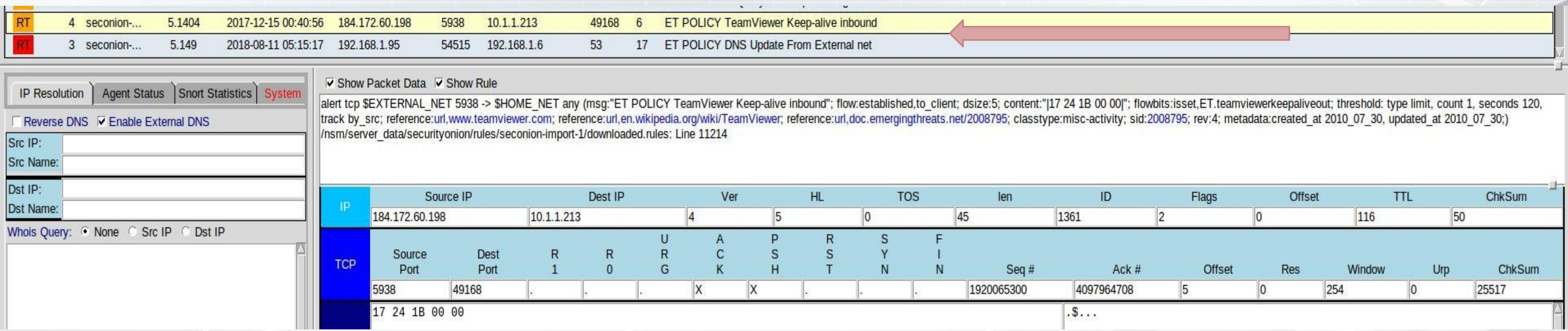
☑ Show Packet Data ☑ Show Rule

```
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                                      .....
```



```
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

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☑ 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
```

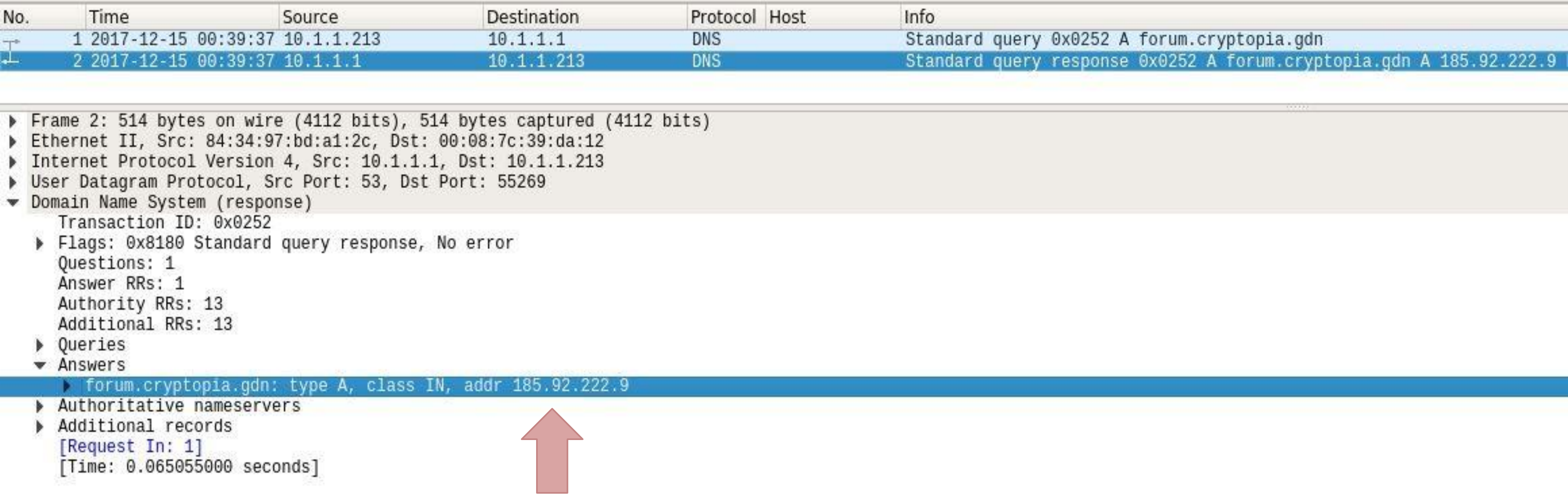
| IP | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ChkSum |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 184.172.60.198 | 10.1.1.213 | 4 | 5 | 0 | 45 | 1361 | 2 | 0 | 116 | 50 |

| 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     .$...
```

# Alert 02

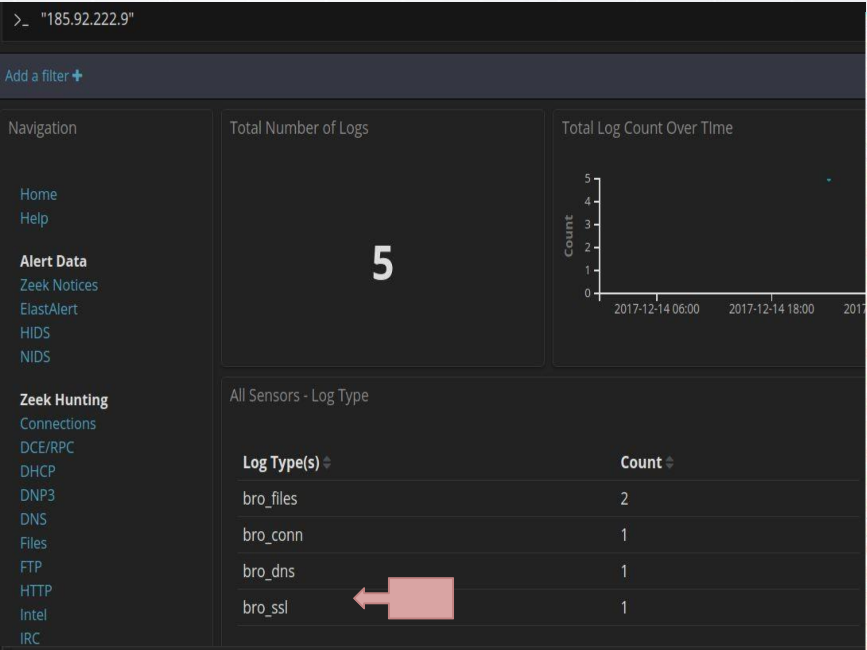
- **Alert02 ET INFO Query For Suspicious .gdn Domain**
- **Possibly Due To Downloader Trojan**



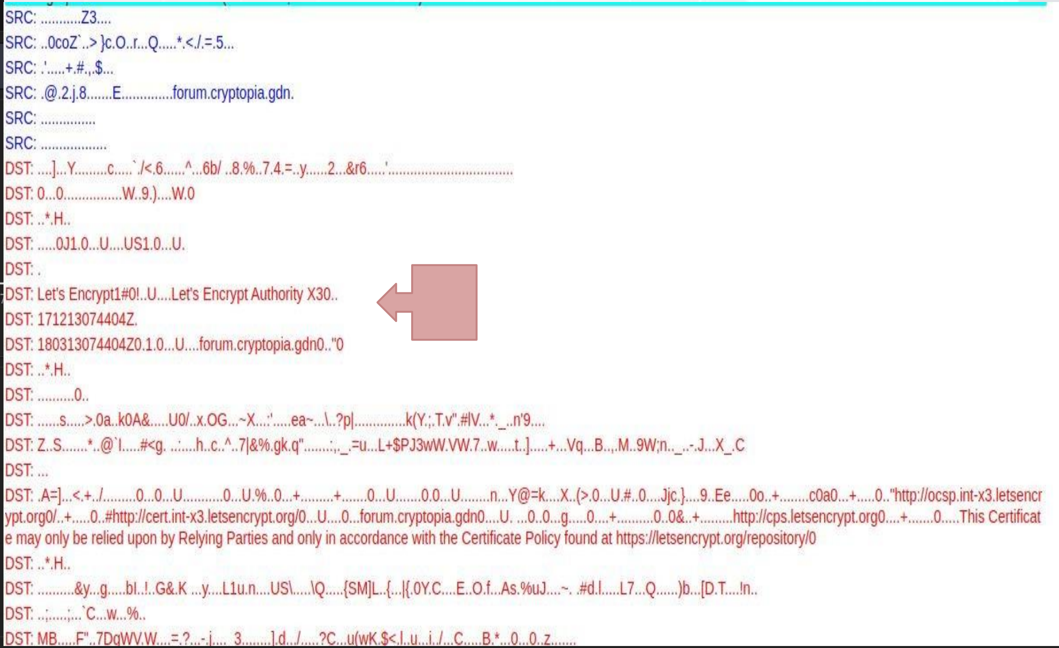
```
No.     Time                 Source       Destination  Protocol Host  Info
      1 2017-12-15 00:39:37 10.1.1.213   10.1.1.1     DNS            Standard query 0x0252 A forum.cryptopia.gdn
      2 2017-12-15 00:39:37 10.1.1.1     10.1.1.213   DNS            Standard query response 0x0252 A forum.cryptopia.gdn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

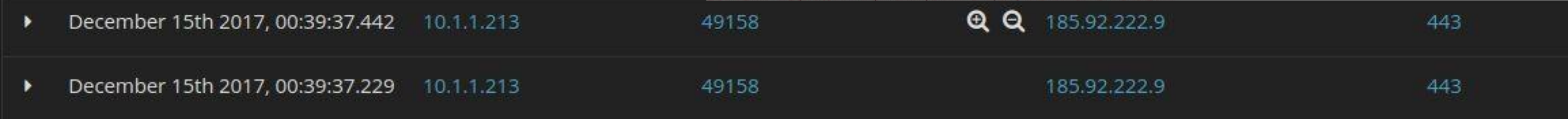
# Further Investigation Using Kibana



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



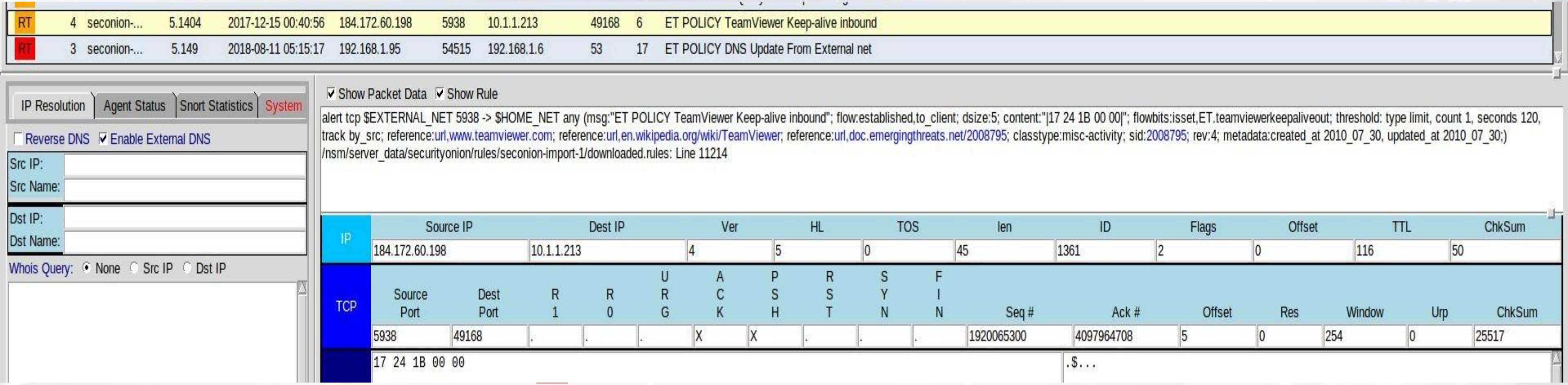
```
SRC: ...........Z3....
SRC: ..0coZ`..> }c.O..r...Q.....*.</.=.5...
SRC: .'.....+.#.,.$...
SRC: .@.2.j.8.......E.............forum.cryptopia.gdn.
SRC: ...............
SRC: .................
DST: ....]...Y.........c.....`./<.6......^...6b/ ..8.%..7.4.=..y......2...&r6.....'..................................
DST: 0...0................W..9.)....W.0
DST: ..*.H..
DST: .....0J1.0...U....US1.0...U.
DST: .
DST: Let's Encrypt1#0!..U....Let's Encrypt Authority X30..
DST: 171213074404Z.
DST: 180313074404Z0.1.0...U....forum.cryptopia.gdn0.."0
DST: ..*.H..
DST: ..........0..
DST: ......s.....>.0a..k0A&.....U0/..x.OG...~X...:'.....ea~...\..?p|..............k(Y.;.T.v".#lV...*._..n'9....
DST: Z..S.......*..@`l.....#<g. ..:....h..c..^..7|&%.gk.q".......:,._=u...L+$PJ3wW.VW.7..w.....t..].....+...Vq...B..,.M..9W;n.._..-.J...X_.C
DST: ...
DST: .A=]...<.+../.........0...0...U...........0...U.%..0...+.........+.......0...U.......0.0...U........n...Y@=k....X..(>.0...U.#..0....Jjc.}....9..Ee.....0o..+........c0a0...+.....0.."http://ocsp.int-x3.letsencr
ypt.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 Certificat
e may only be relied upon by Relying Parties and only in accordance with the Certificate Policy found at https://letsencrypt.org/repository/0
DST: ..*.H..
DST: ..........&y...g.....bl..!..G&.K ...y....L1u.n....US\.....\Q.....{SM]L..{...|{.0Y.C....E..O.f...As.%uJ....~. .#d.l.....L7...Q......)b...[D.T....!n..
DST: ..;.....;...`C...w...%..
DST: MB.....F"..7DqWV.W....=.?...-.j.... 3........].d../.....?C...u(wK.$<.l..u...i../...C.....B.*...0...0..z.......
```



```
▸  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
```

# Alert 03

- **Alert03 ET Policy TeamViewer Keep-alive inbound.**
- **Possibly Due To Downloaded Malware From forum.cryptopia.gdn.**



|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| 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

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

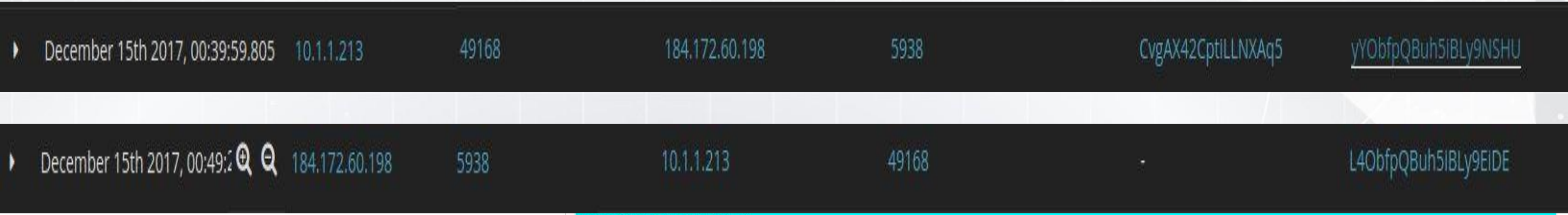
```
alert tcp $EXTERNAL_NET 5938 -> $HOME_NET any (msg:"ET POLICY TeamViewer Keep-alive inbound"; flow:established,to_client; dsize:5; content:"|17 24 1B 00 00|"; flowbits:isset,ET.teamviewerkeepaliveout; threshold: type limit, count 1, seconds 120, track by_src; reference:url,www.teamviewer.com; reference:url,en.wikipedia.org/wiki/TeamViewer; 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 |

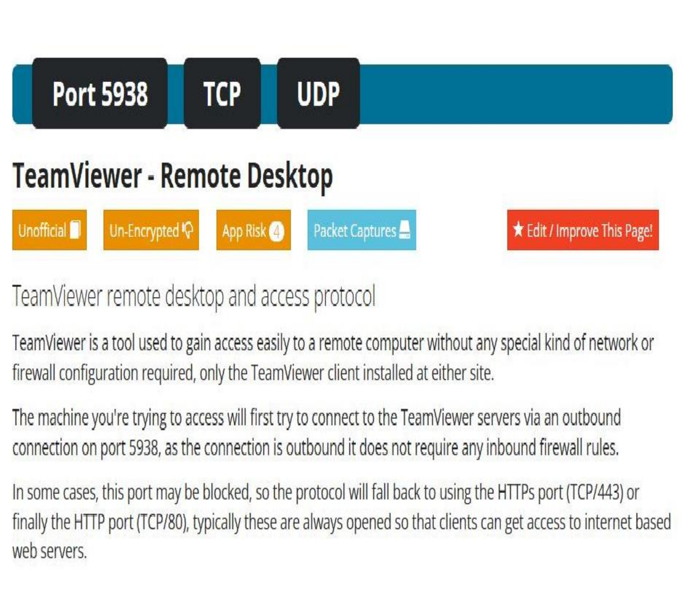
| TCP | Source Port | Dest Port | R 1 | R 0 | U R G | A C K | P S H | R S T | S Y N | F I N | Seq # | Ack # | Offset | Res | Window | Urp | ChkSum |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | 5938 | 49168 | . | . | . | X | X | . | . | . | 1920065300 | 4097964708 | 5 | 0 | 254 | 0 | 25517 |

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

# Further Investigation Using Kibana



```
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
```



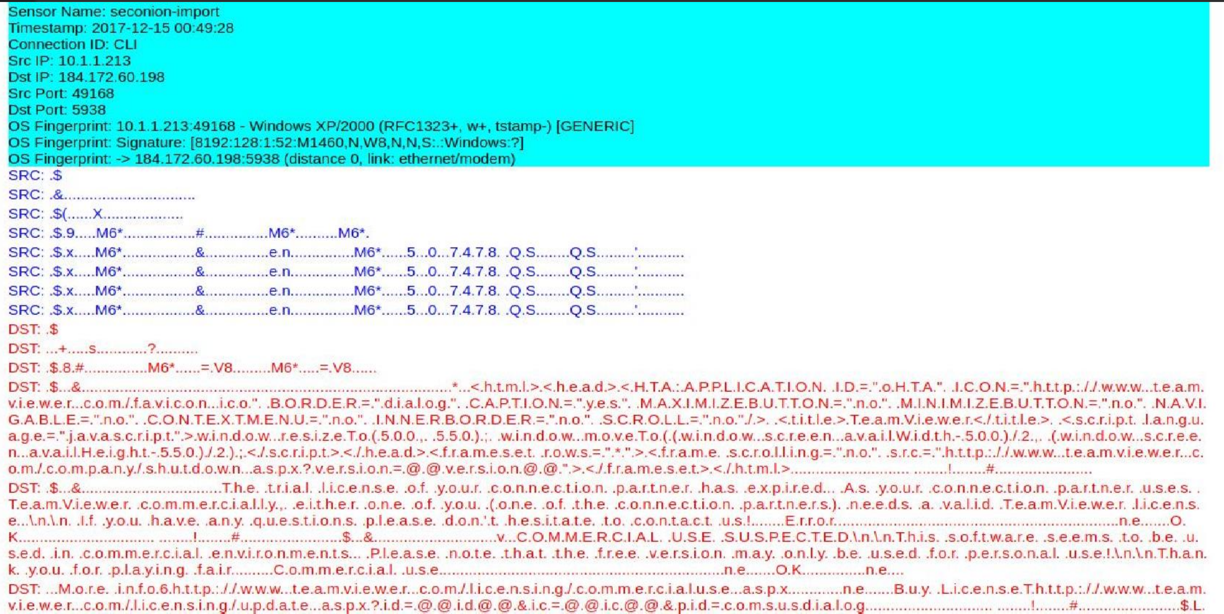
## TeamViewer - Remote Desktop

TeamViewer remote desktop and access protocol

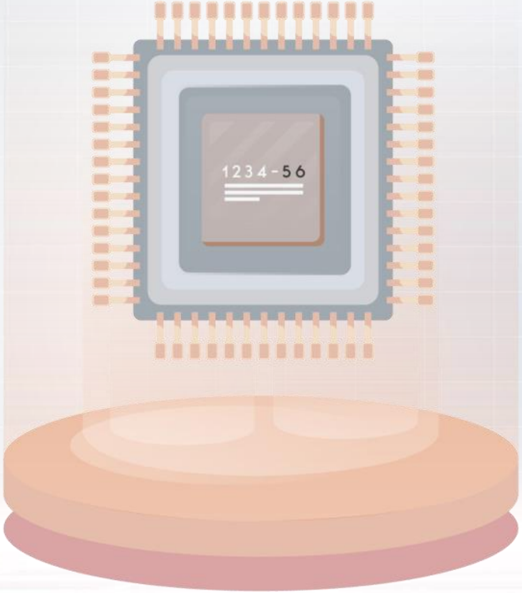
TeamViewer is a tool used to gain access easily to a remote computer without any special kind of network or firewall configuration required, only the TeamViewer client installed at either site.

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.



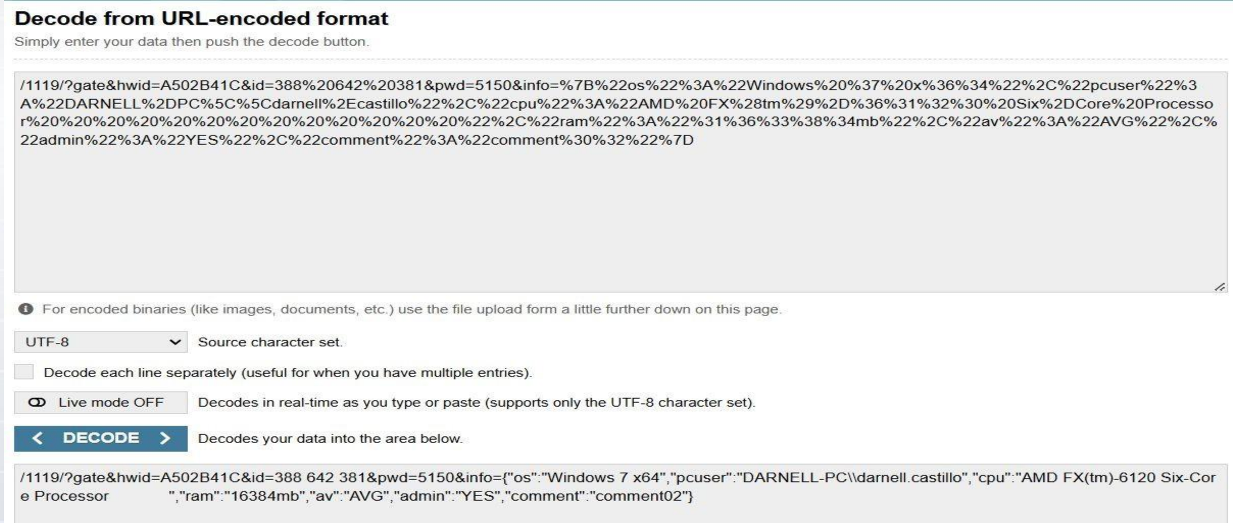
```
Sensor Name: seconion-import
Timestamp: 2017-12-15 00:49:28
Connection ID: CLI
Src IP: 10.1.1.213
Dst IP: 184.172.60.198
Src Port: 49168
Dst Port: 5938
OS Fingerprint: 10.1.1.213:49168 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
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.
```



# Summary of The Two Incidents

# SUMMARY

# More Suspicious Logs



## Decode from URL-encoded format

Simply enter your data then push the decode button.

```
/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%22DARNELL%2DPC%5C%5Cdarnell%2Ecastillo%22%2C%22cpu%22%3A%22AMD%20FX%28tm%29%2D%36%31%32%30%20Six%2DCore%20Processor%20%20%20%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%22%2C%22comment%22%3A%22comment%30%32%22%7D
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

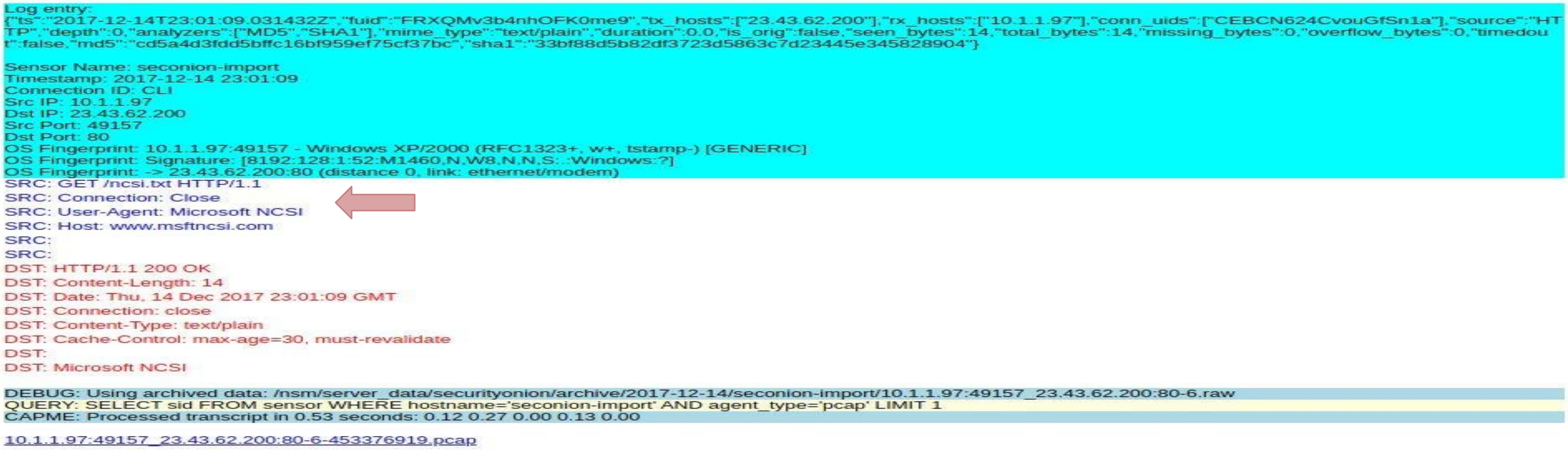
Source character set.

□ Decode each line separately (useful for when you have multiple entries).

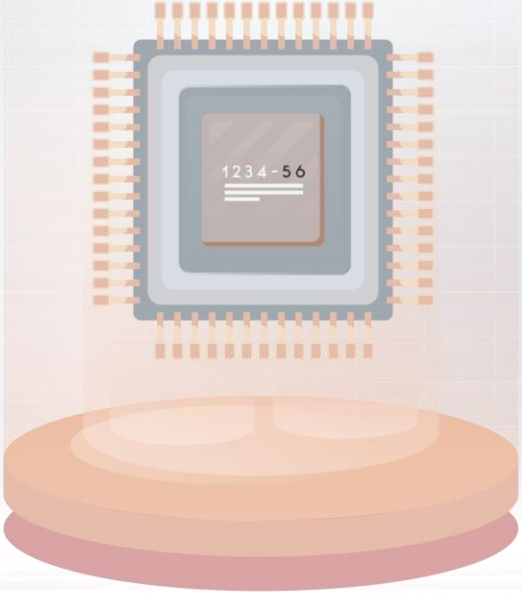
Decodes in real-time as you type or paste (supports only the UTF-8 character set).

Decodes your data into the area below.

```
/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"}
```



```
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":"HTTP","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,"timedout":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
```



# 03

# CONCLUSION

‘The Investigation Summary.’

# Is There Any Relationship?

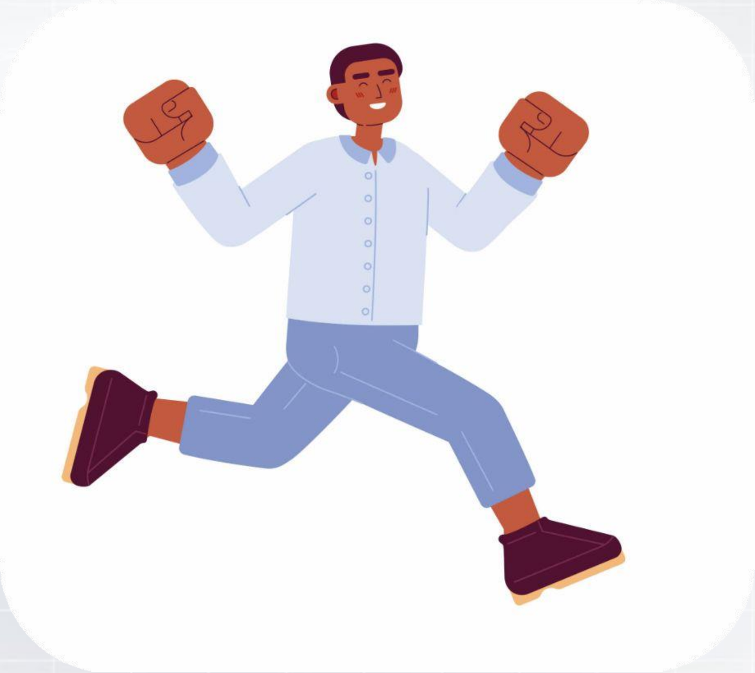
- Private IPs
- Phishing Mails

- Work Mail
- No Correlation

# Mitigation Strategies..

- Isolation
- Malware Removal
- Blocking IPs

- Implement DLP
- Email Gateway
- Increase Awareness
- Endpoint AVs



# THANK YOU!