# Security Onion

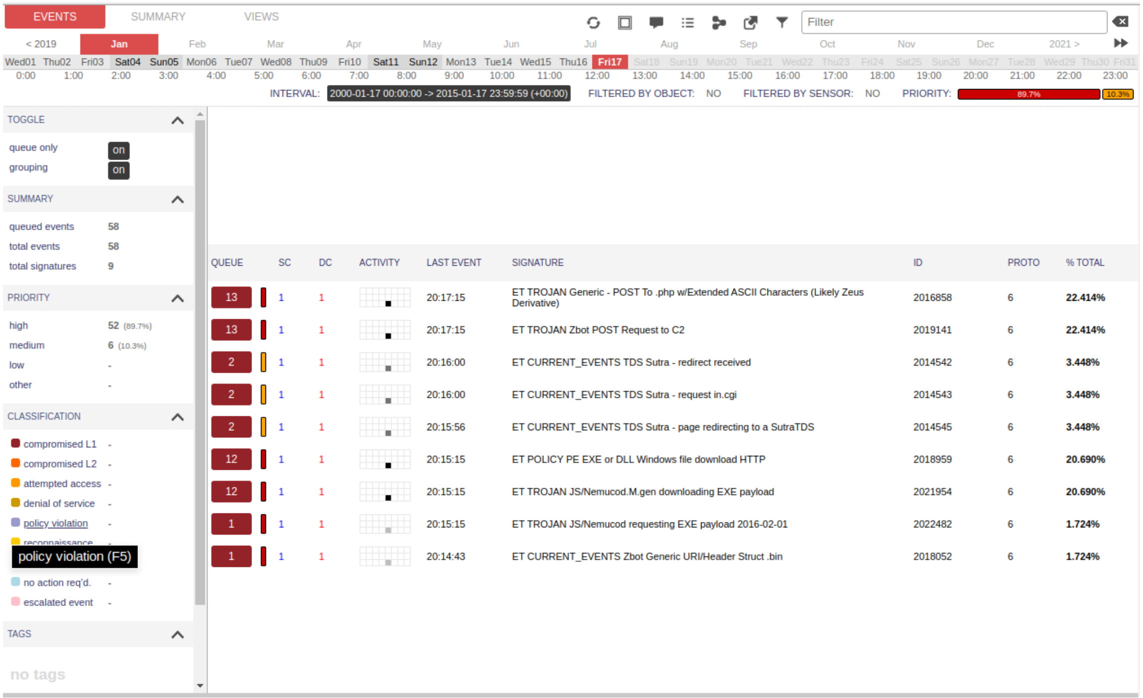
# Michał Wawrzyńczak

## Jako pierwsz do analizy wybrałem i zaimportowałem plik `zeus-sample-1`.

`sudo so-import-pcap zeus-sample-1` Analizę logów zacząłem od zapoznania się z infomacjami zwróconymi przez programy Squert i Kibana.

Przy użyciu narzędzia Squert udało mi sie uzyskać takie informacja jak adresy ip z którymi łączył się zaatakowany host, numery portów na których odbywała się komunikacja, państwa z których pochodziły adresy IP. A przede wszystkim Squert wskazał już sygnatury do których pasują analizowane logi.

**Sygnatury - informacja, że mamy doczynienia z TROJAN Generic**



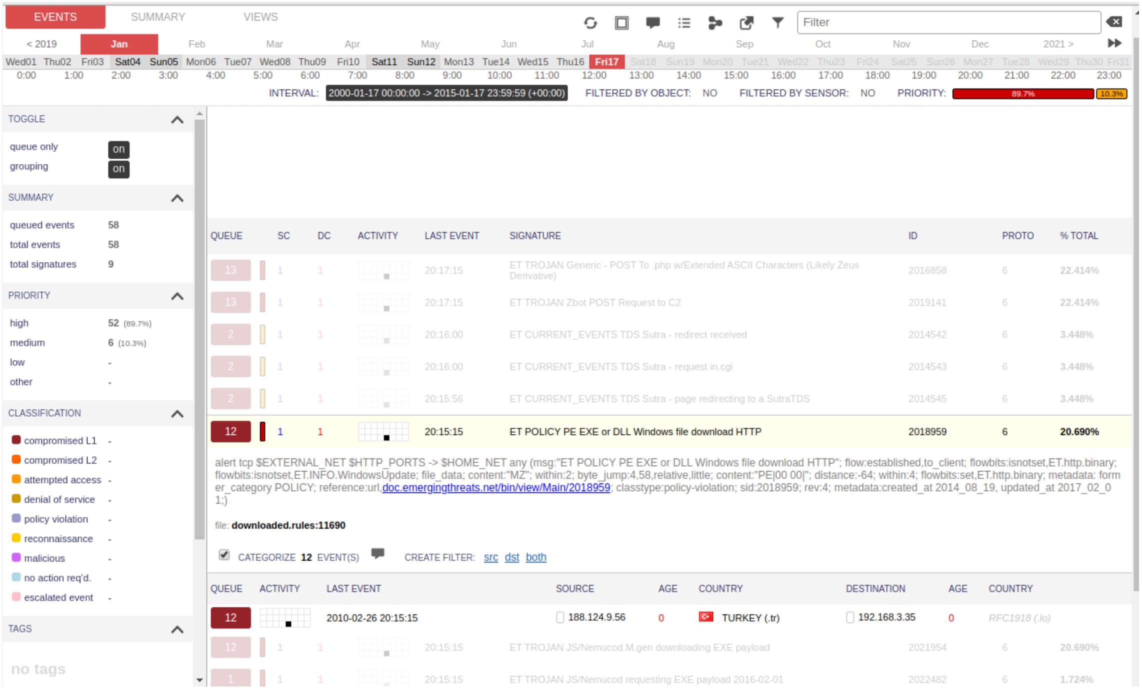
INTERVAL: 2000-01-17 00:00:00 -> 2015-01-17 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 89.7% 10.3%

queue only on
grouping on

queued events 58
total events 58
total signatures 9

high 52 (89.7%)
medium 6 (10.3%)
low -
other -

| QUEUE | SC | DC | ACTIVITY | LAST EVENT | SIGNATURE | ID | PROTO | % TOTAL |
|---|---|---|---|---|---|---|---|---|
| 13 | 1 | 1 | | 20:17:15 | ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative) | 2016858 | 6 | **22.414%** |
| 13 | 1 | 1 | | 20:17:15 | ET TROJAN Zbot POST Request to C2 | 2019141 | 6 | **22.414%** |
| 2 | 1 | 1 | | 20:16:00 | ET CURRENT_EVENTS TDS Sutra - redirect received | 2014542 | 6 | **3.448%** |
| 2 | 1 | 1 | | 20:16:00 | ET CURRENT_EVENTS TDS Sutra - request in.cgi | 2014543 | 6 | **3.448%** |
| 2 | 1 | 1 | | 20:15:56 | ET CURRENT_EVENTS TDS Sutra - page redirecting to a SutraTDS | 2014545 | 6 | **3.448%** |
| 12 | 1 | 1 | | 20:15:15 | ET POLICY PE EXE or DLL Windows file download HTTP | 2018959 | 6 | **20.690%** |
| 12 | 1 | 1 | | 20:15:15 | ET TROJAN JS/Nemucod.M.gen downloading EXE payload | 2021954 | 6 | **20.690%** |
| 1 | 1 | 1 | | 20:15:15 | ET TROJAN JS/Nemucod requesting EXE payload 2016-02-01 | 2022482 | 6 | **1.724%** |
| 1 | 1 | 1 | | 20:14:43 | ET CURRENT_EVENTS Zbot Generic URI/Header Struct .bin | 2018052 | 6 | **1.724%** |


EVENTS
SUMMARY
VIEWS
Filter
< 2019 Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2021 >
Wed01 Thu02 Fri03 Sat04 Sun05 Mon06 Tue07 Wed08 Thu09 Fri10 Sat11 Sun12 Mon13 Tue14 Wed15 Thu16 Fri17 Sat18 Sun19 Mon20 Tue21 Wed22 Thu23 Fri24 Sat25 Sun26 Mon27 Tue28 Wed29 Thu30 Fri31
0:00 1:00 2:00 3:00 4:00 5:00 6:00 7:00 8:00 9:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00

INTERVAL: 2000-01-17 00:00:00 -> 2015-01-17 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 89.7% 10.3%

TOGGLE

| | |
|---|---|
| queue only | on |
| grouping | on |

SUMMARY

| | |
|---|---|
| queued events | 58 |
| total events | 58 |
| total signatures | 9 |

PRIORITY

| | |
|---|---|
| high | 52 (89.7%) |
| medium | 6 (10.3%) |
| low | - |
| other | - |

CLASSIFICATION

| | |
|---|---|
| compromised L1 | - |
| compromised L2 | - |
| attempted access | - |
| denial of service | - |
| policy violation | - |
| reconnaissance | - |
| malicious | - |
| no action req'd. | - |
| escalated event | - |

TAGS

no tags

| QUEUE | SC | DC | ACTIVITY | LAST EVENT | SIGNATURE | ID | PROTO | % TOTAL |
|---|---|---|---|---|---|---|---|---|
| 13 | 1 | 1 | | 20:17:15 | ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative) | 2016858 | 6 | 22.414% |
| 13 | 1 | 1 | | 20:17:15 | ET TROJAN Zbot POST Request to C2 | 2019141 | 6 | 22.414% |
| 2 | 1 | 1 | | 20:16:00 | ET CURRENT_EVENTS TDS Sutra - redirect received | 2014542 | 6 | 3.448% |
| 2 | 1 | 1 | | 20:16:00 | ET CURRENT_EVENTS TDS Sutra - request in.cgi | 2014543 | 6 | 3.448% |
| 2 | 1 | 1 | | 20:15:56 | ET CURRENT_EVENTS TDS Sutra - page redirecting to a SutraTDS | 2014545 | 6 | 3.448% |
| 12 | 1 | 1 | | 20:15:15 | ET POLICY PE EXE or DLL Windows file download HTTP | 2018959 | 6 | 20.690% |

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY PE EXE or DLL Windows file download HTTP"; flow:established,to_client; flowbits:isnotset,ET.http.binary; flowbits:isnotset,ET.INFO.WindowsUpdate; file_data; content:"MZ"; within:2; byte_jump:4,58,relative,little; content:"PE|00 00|"; distance:-64; within:4; flowbits:set,ET.http.binary; metadata: former_category POLICY; reference:url,doc.emergingthreats.net/bin/view/Main/2018959; classtype:policy-violation; sid:2018959; rev:4; metadata:created_at 2014_08_19, updated_at 2017_02_01;)
```

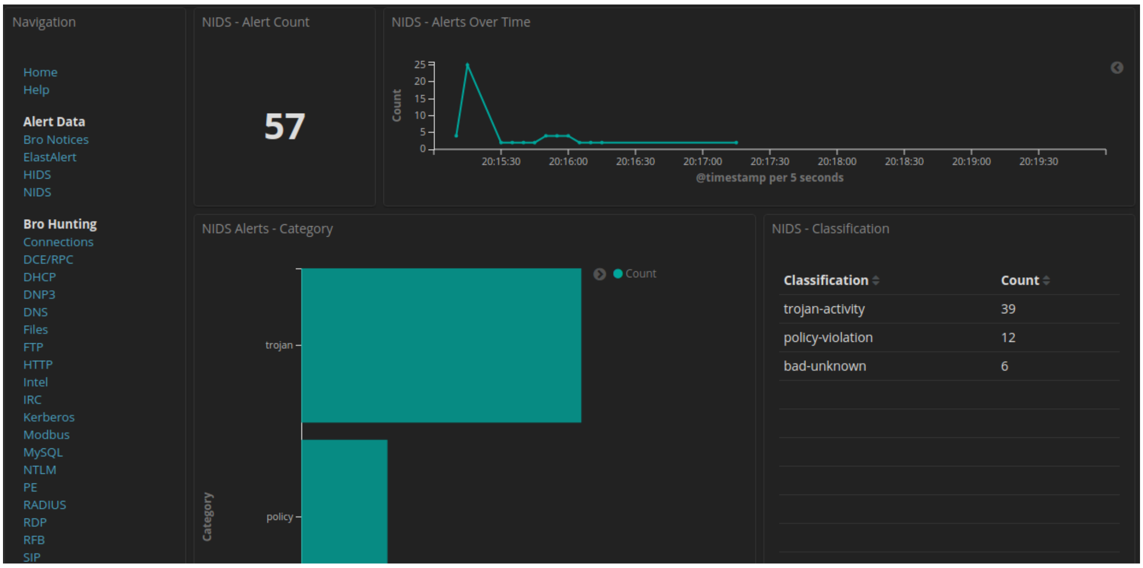
file: **downloaded.rules:11690**

☑ CATEGORIZE **12** EVENT(S) CREATE FILTER: src dst both

| QUEUE | ACTIVITY | LAST EVENT | SOURCE | AGE | COUNTRY | DESTINATION | AGE | COUNTRY |
|---|---|---|---|---|---|---|---|---|
| 12 | | 2010-02-26 20:15:15 | □ 188.124.9.56 | 0 | TURKEY (.tr) | □ 192.168.3.35 | 0 | RFC1918 (.lo) |

| QUEUE | SC | DC | ACTIVITY | LAST EVENT | SIGNATURE | ID | PROTO | % TOTAL |
|---|---|---|---|---|---|---|---|---|
| 12 | 1 | 1 | | 20:15:15 | ET TROJAN JS/Nemucod.M.gen downloading EXE payload | 2021954 | 6 | 20.690% |
| 1 | 1 | 1 | | 20:15:15 | ET TROJAN JS/Nemucod requesting EXE payload 2016-02-01 | 2022482 | 6 | 1.724% |

## Alerty NIDS



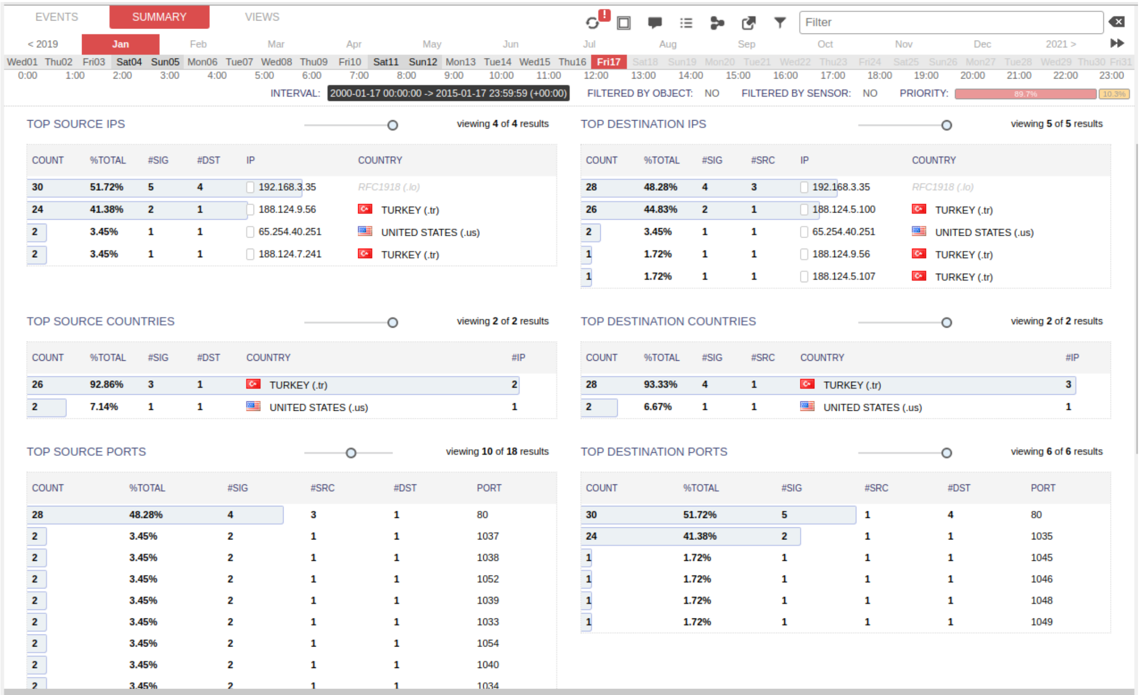
NIDS - Alert Count

57

NIDS - Classification

| Classification | Count |
|---|---|
| trojan-activity | 39 |
| policy-violation | 12 |
| bad-unknown | 6 |

Adresy IP wraz z pochodzeniem oraz porty



INTERVAL: 2000-01-17 00:00:00 -> 2015-01-17 23:59:59 (+00:00)   FILTERED BY OBJECT: NO   FILTERED BY SENSOR: NO   PRIORITY:

TOP SOURCE IPS — viewing **4** of **4** results

| COUNT | %TOTAL | #SIG | #DST | IP | COUNTRY |
|---|---|---|---|---|---|
| **30** | **51.72%** | **5** | **4** | □ 192.168.3.35 | *RFC1918 (.lo)* |
| **24** | **41.38%** | **2** | **1** | □ 188.124.9.56 | TURKEY (.tr) |
| **2** | **3.45%** | **1** | **1** | □ 65.254.40.251 | UNITED STATES (.us) |
| **2** | **3.45%** | **1** | **1** | □ 188.124.7.241 | TURKEY (.tr) |

TOP DESTINATION IPS — viewing **5** of **5** results

| COUNT | %TOTAL | #SIG | #SRC | IP | COUNTRY |
|---|---|---|---|---|---|
| **28** | **48.28%** | **4** | **3** | □ 192.168.3.35 | *RFC1918 (.lo)* |
| **26** | **44.83%** | **2** | **1** | □ 188.124.5.100 | TURKEY (.tr) |
| **2** | **3.45%** | **1** | **1** | □ 65.254.40.251 | UNITED STATES (.us) |
| **1** | **1.72%** | **1** | **1** | □ 188.124.9.56 | TURKEY (.tr) |
| **1** | **1.72%** | **1** | **1** | □ 188.124.5.107 | TURKEY (.tr) |

TOP SOURCE COUNTRIES — viewing **2** of **2** results

| COUNT | %TOTAL | #SIG | #DST | COUNTRY | #IP |
|---|---|---|---|---|---|
| **26** | **92.86%** | **3** | **1** | TURKEY (.tr) | **2** |
| **2** | **7.14%** | **1** | **1** | UNITED STATES (.us) | **1** |

TOP DESTINATION COUNTRIES — viewing **2** of **2** results

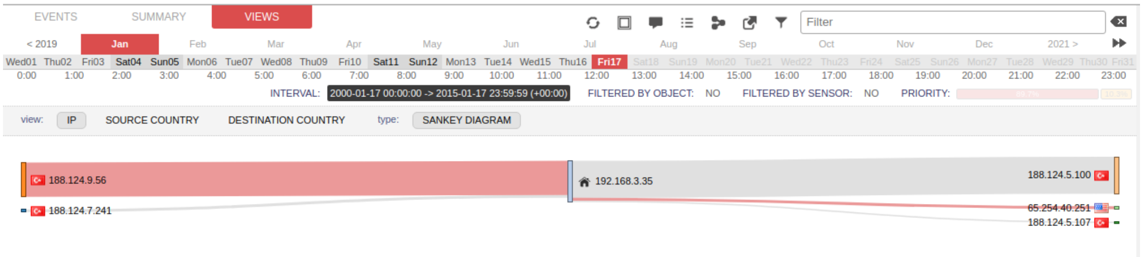
| COUNT | %TOTAL | #SIG | #SRC | COUNTRY | #IP |
|---|---|---|---|---|---|
| **28** | **93.33%** | **4** | **1** | TURKEY (.tr) | **3** |
| **2** | **6.67%** | **1** | **1** | UNITED STATES (.us) | **1** |

TOP SOURCE PORTS — viewing **10** of **18** results

| COUNT | %TOTAL | #SIG | #SRC | #DST | PORT |
|---|---|---|---|---|---|
| **28** | **48.28%** | **4** | **3** | **1** | 80 |
| **2** | **3.45%** | **2** | **1** | **1** | 1037 |
| **2** | **3.45%** | **2** | **1** | **1** | 1038 |
| **2** | **3.45%** | **2** | **1** | **1** | 1052 |
| **2** | **3.45%** | **2** | **1** | **1** | 1039 |
| **2** | **3.45%** | **2** | **1** | **1** | 1033 |
| **2** | **3.45%** | **2** | **1** | **1** | 1054 |
| **2** | **3.45%** | **2** | **1** | **1** | 1040 |
| **2** | **3.45%** | **2** | **1** | **1** | 1034 |

TOP DESTINATION PORTS — viewing **6** of **6** results

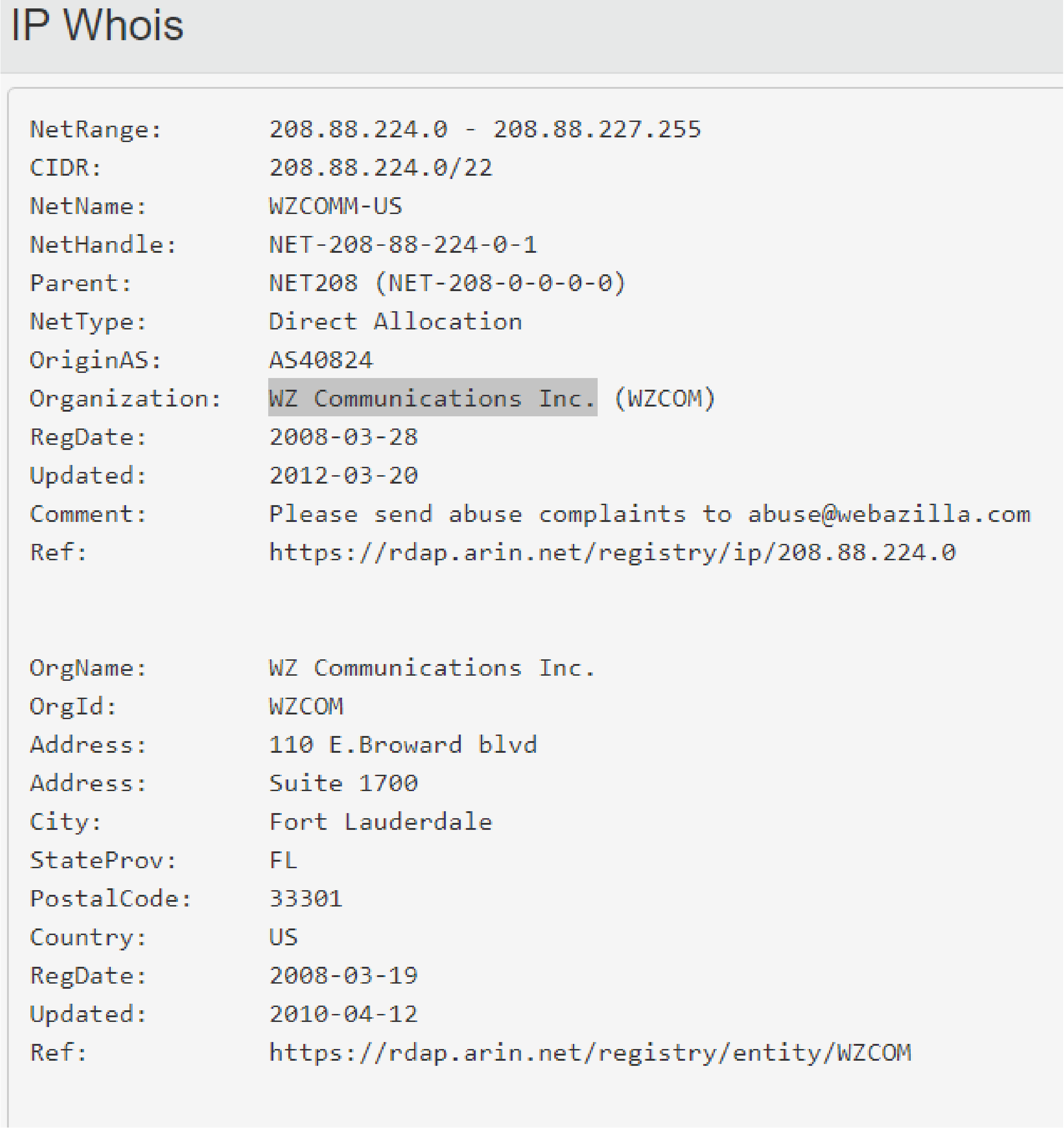
| COUNT | %TOTAL | #SIG | #SRC | #DST | PORT |
|---|---|---|---|---|---|
| **30** | **51.72%** | **5** | **1** | **4** | 80 |
| **24** | **41.38%** | **2** | **1** | **1** | 1035 |
| **1** | **1.72%** | **1** | **1** | **1** | 1045 |
| **1** | **1.72%** | **1** | **1** | **1** | 1046 |
| **1** | **1.72%** | **1** | **1** | **1** | 1048 |
| **1** | **1.72%** | **1** | **1** | **1** | 1049 |



INTERVAL: 2000-01-17 00:00:00 -> 2015-01-17 23:59:59 (+00:00)   FILTERED BY OBJECT: NO   FILTERED BY SENSOR: NO   PRIORITY:

view: IP   SOURCE COUNTRY   DESTINATION COUNTRY   type: SANKEY DIAGRAM

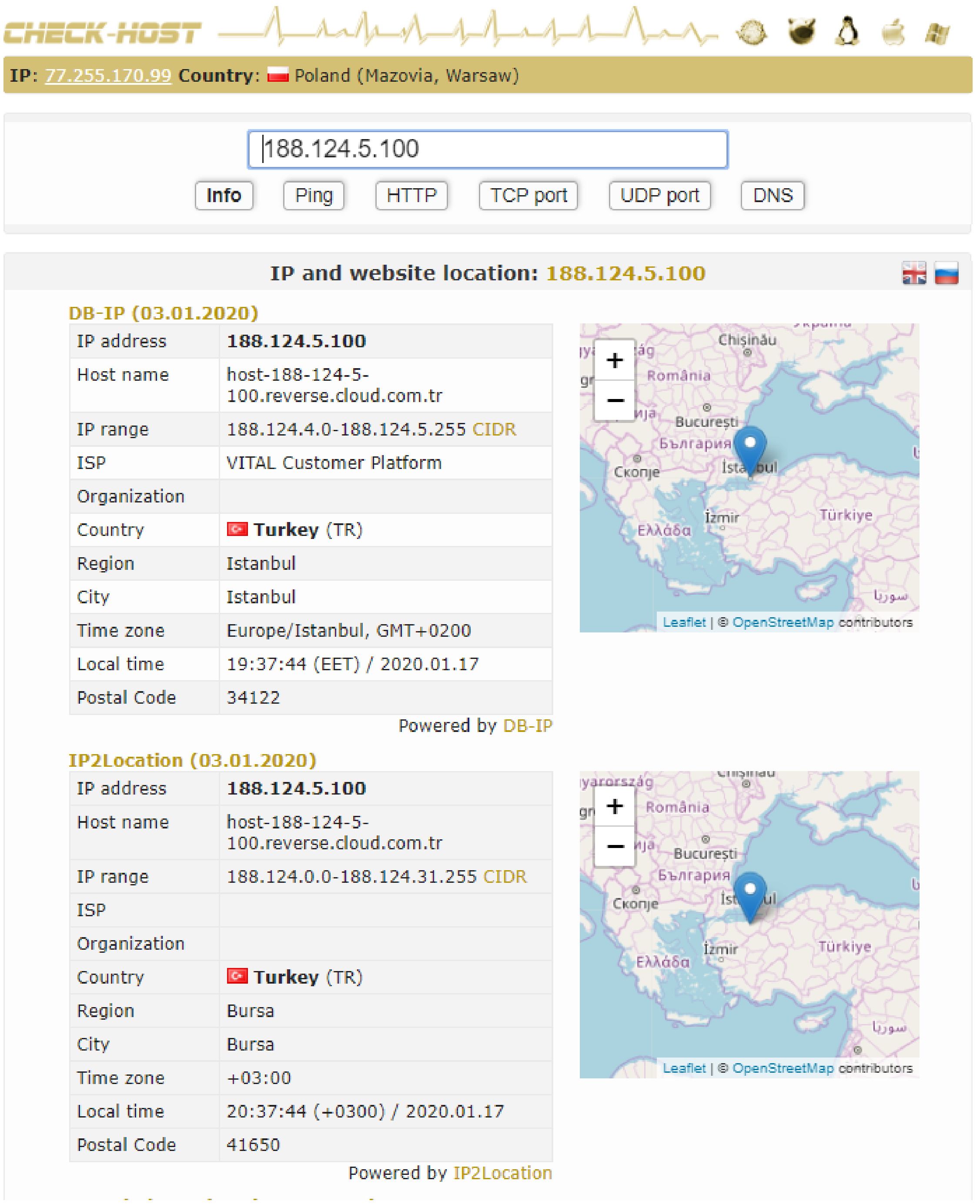
Posprawdzałem informacje o adresach IP celem określenia dokładniejszej lokalizacji, a także sprawdziłem je w bazie whoIs



IP Whois

```
NetRange:       208.88.224.0 - 208.88.227.255
CIDR:           208.88.224.0/22
NetName:        WZCOMM-US
NetHandle:      NET-208-88-224-0-1
Parent:         NET208 (NET-208-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS40824
Organization:   WZ Communications Inc. (WZCOM)
RegDate:        2008-03-28
Updated:        2012-03-20
Comment:        Please send abuse complaints to abuse@webazilla.com
Ref:            https://rdap.arin.net/registry/ip/208.88.224.0


OrgName:        WZ Communications Inc.
OrgId:          WZCOM
Address:        110 E.Broward blvd
Address:        Suite 1700
City:           Fort Lauderdale
StateProv:      FL
PostalCode:     33301
Country:        US
RegDate:        2008-03-19
Updated:        2010-04-12
Ref:            https://rdap.arin.net/registry/entity/WZCOM
```



**IP**: 77.255.170.99 **Country**: Poland (Mazovia, Warsaw)

**IP and website location: 188.124.5.100**

DB-IP (03.01.2020)

| | |
|---|---|
| IP address | **188.124.5.100** |
| Host name | host-188-124-5-100.reverse.cloud.com.tr |
| IP range | 188.124.4.0-188.124.5.255 CIDR |
| ISP | VITAL Customer Platform |
| Organization | |
| Country | **Turkey** (TR) |
| Region | Istanbul |
| City | Istanbul |
| Time zone | Europe/Istanbul, GMT+0200 |
| Local time | 19:37:44 (EET) / 2020.01.17 |
| Postal Code | 34122 |

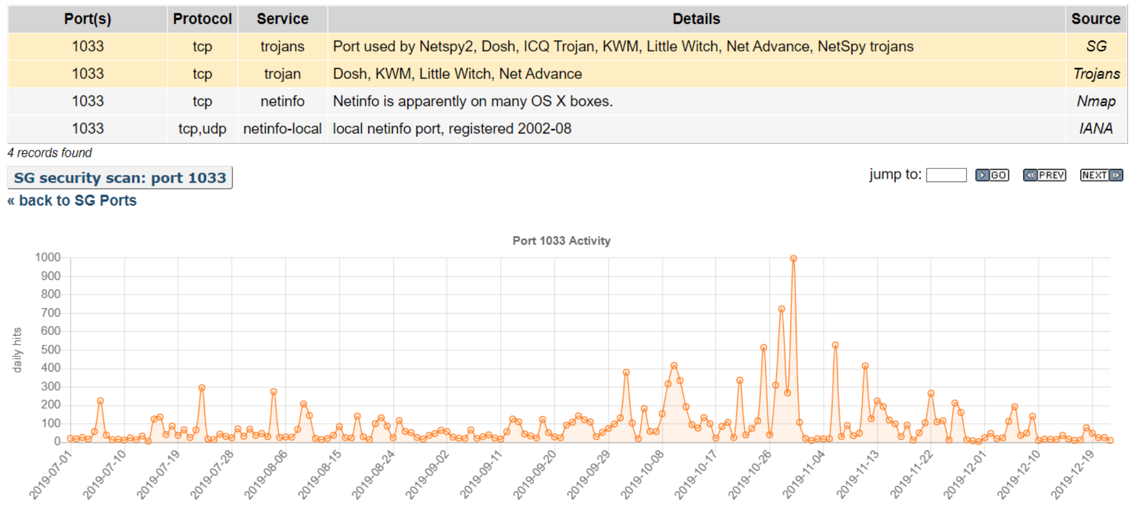
Powered by DB-IP

IP2Location (03.01.2020)

| | |
|---|---|
| IP address | **188.124.5.100** |
| Host name | host-188-124-5-100.reverse.cloud.com.tr |
| IP range | 188.124.0.0-188.124.31.255 CIDR |
| ISP | |
| Organization | |
| Country | **Turkey** (TR) |
| Region | Bursa |
| City | Bursa |
| Time zone | +03:00 |
| Local time | 20:37:44 (+0300) / 2020.01.17 |
| Postal Code | 41650 |

Powered by IP2Location

**Porty na których odbywała się komunikacja sprawdziłem w bazie. Okazało się, że na portach z zakresu ~1033-1050 często komunikują się trojany i backdory**



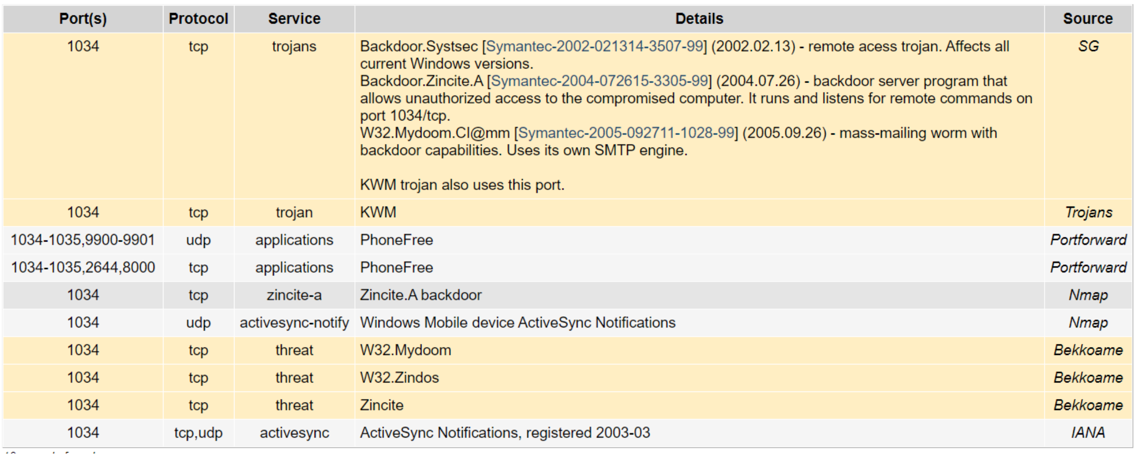
| Port(s) | Protocol | Service | Details | Source |
|---|---|---|---|---|
| 1033 | tcp | trojans | Port used by Netspy2, Dosh, ICQ Trojan, KWM, Little Witch, Net Advance, NetSpy trojans | *SG* |
| 1033 | tcp | trojan | Dosh, KWM, Little Witch, Net Advance | *Trojans* |
| 1033 | tcp | netinfo | Netinfo is apparently on many OS X boxes. | *Nmap* |
| 1033 | tcp,udp | netinfo-local | local netinfo port, registered 2002-08 | *IANA* |

*4 records found*

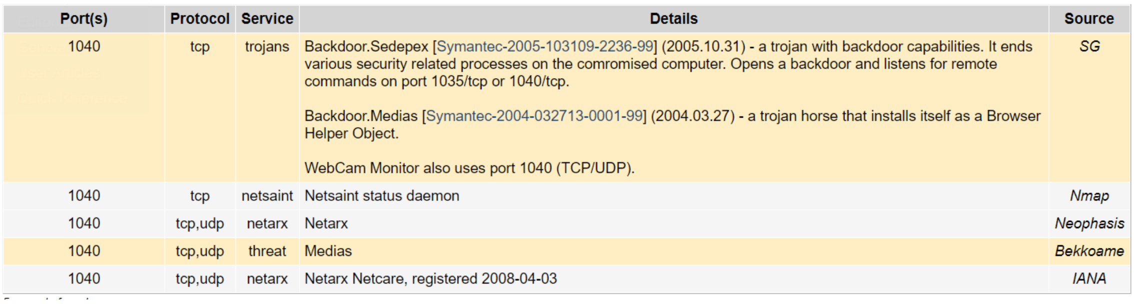
**SG security scan: port 1033**

jump to: GO PREV NEXT

**« back to SG Ports**

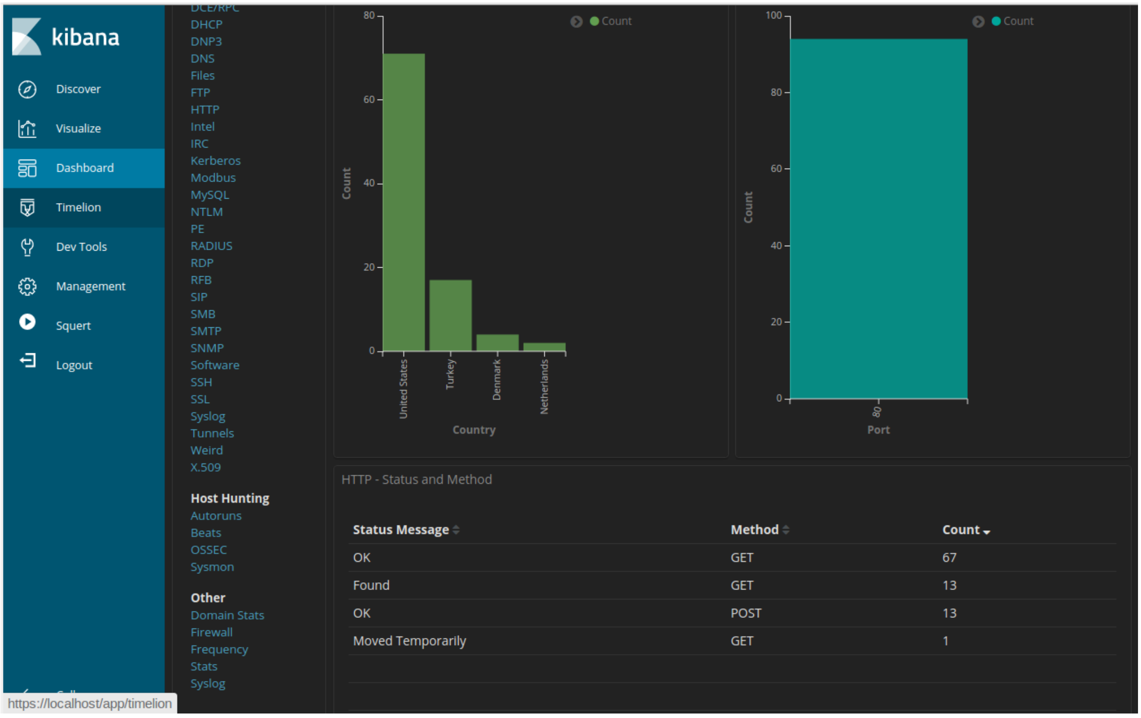


| Port(s) | Protocol | Service | Details | Source |
|---|---|---|---|---|
| 1034 | tcp | trojans | Backdoor.Systsec [Symantec-2002-021314-3507-99] (2002.02.13) - remote acess trojan. Affects all current Windows versions.<br>Backdoor.Zincite.A [Symantec-2004-072615-3305-99] (2004.07.26) - backdoor server program that allows unauthorized access to the compromised computer. It runs and listens for remote commands on port 1034/tcp.<br>W32.Mydoom.CI@mm [Symantec-2005-092711-1028-99] (2005.09.26) - mass-mailing worm with backdoor capabilities. Uses its own SMTP engine.<br><br>KWM trojan also uses this port. | *SG* |
| 1034 | tcp | trojan | KWM | *Trojans* |
| 1034-1035,9900-9901 | udp | applications | PhoneFree | *Portforward* |
| 1034-1035,2644,8000 | tcp | applications | PhoneFree | *Portforward* |
| 1034 | tcp | zincite-a | Zincite.A backdoor | *Nmap* |
| 1034 | udp | activesync-notify | Windows Mobile device ActiveSync Notifications | *Nmap* |
| 1034 | tcp | threat | W32.Mydoom | *Bekkoame* |
| 1034 | tcp | threat | W32.Zindos | *Bekkoame* |
| 1034 | tcp | threat | Zincite | *Bekkoame* |
| 1034 | tcp,udp | activesync | ActiveSync Notifications, registered 2003-03 | *IANA* |



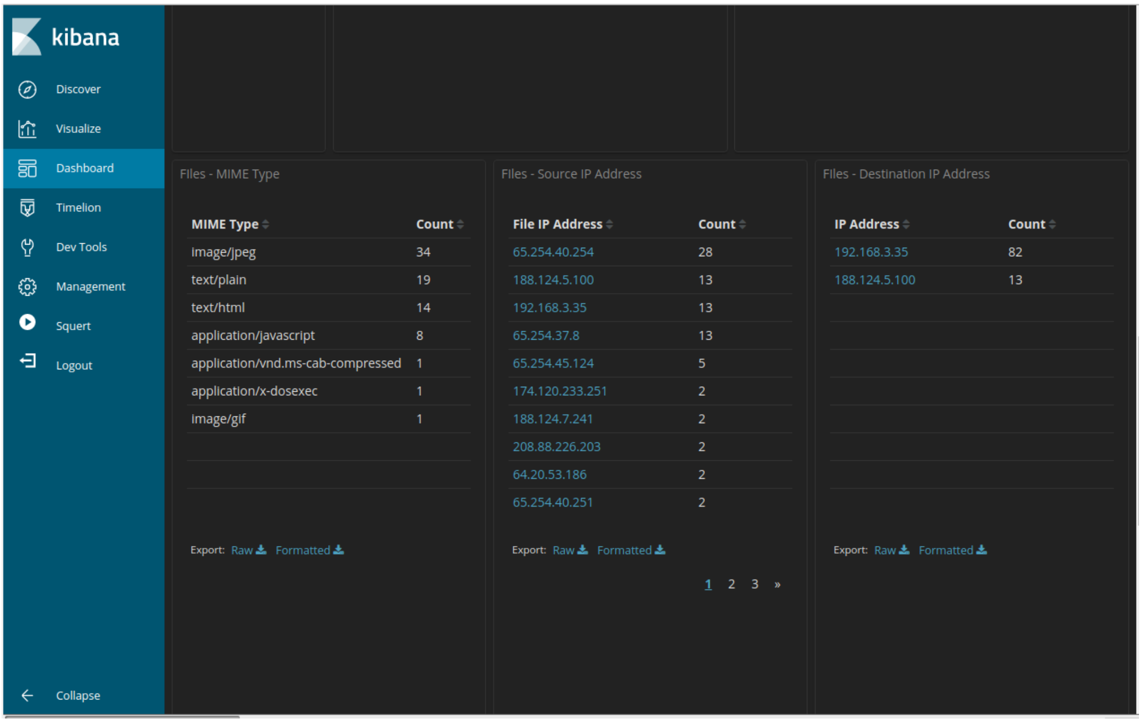
| Port(s) | Protocol | Service | Details | Source |
|---|---|---|---|---|
| 1040 | tcp | trojans | Backdoor.Sedepex [Symantec-2005-103109-2236-99] (2005.10.31) - a trojan with backdoor capabilities. It ends various security related processes on the comromised computer. Opens a backdoor and listens for remote commands on port 1035/tcp or 1040/tcp.<br><br>Backdoor.Medias [Symantec-2004-032713-0001-99] (2004.03.27) - a trojan horse that installs itself as a Browser Helper Object.<br><br>WebCam Monitor also uses port 1040 (TCP/UDP). | *SG* |
| 1040 | tcp | netsaint | Netsaint status daemon | *Nmap* |
| 1040 | tcp,udp | netarx | Netarx | *Neophasis* |
| 1040 | tcp,udp | threat | Medias | *Bekkoame* |
| 1040 | tcp,udp | netarx | Netarx Netcare, registered 2008-04-03 | *IANA* |

Podobne czynności wykonałem przy użyciu Kibany, wyniki jak się spodziewałem były bardzo podobne, udało się jeszcze pozyskać informacje o tym jakie pliki, z jakich i na jakie adresy były wysyłane.



HTTP - Status and Method

| Status Message | Method | Count |
|---|---|---|
| OK | GET | 67 |
| Found | GET | 13 |
| OK | POST | 13 |
| Moved Temporarily | GET | 1 |



Files - MIME Type

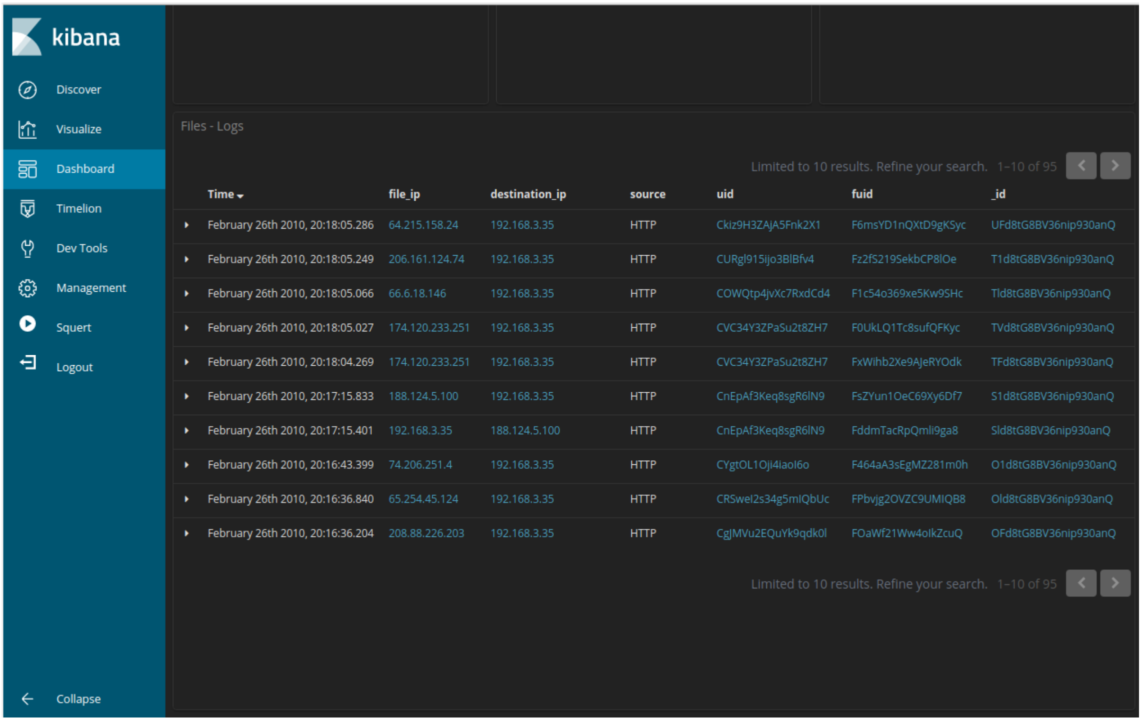
| MIME Type | Count |
|---|---|
| image/jpeg | 34 |
| text/plain | 19 |
| text/html | 14 |
| application/javascript | 8 |
| application/vnd.ms-cab-compressed | 1 |
| application/x-dosexec | 1 |
| image/gif | 1 |

Files - Source IP Address

| File IP Address | Count |
|---|---|
| 65.254.40.254 | 28 |
| 188.124.5.100 | 13 |
| 192.168.3.35 | 13 |
| 65.254.37.8 | 13 |
| 65.254.45.124 | 5 |
| 174.120.233.251 | 2 |
| 188.124.7.241 | 2 |
| 208.88.226.203 | 2 |
| 64.20.53.186 | 2 |
| 65.254.40.251 | 2 |

Files - Destination IP Address

| IP Address | Count |
|---|---|
| 192.168.3.35 | 82 |
| 188.124.5.100 | 13 |

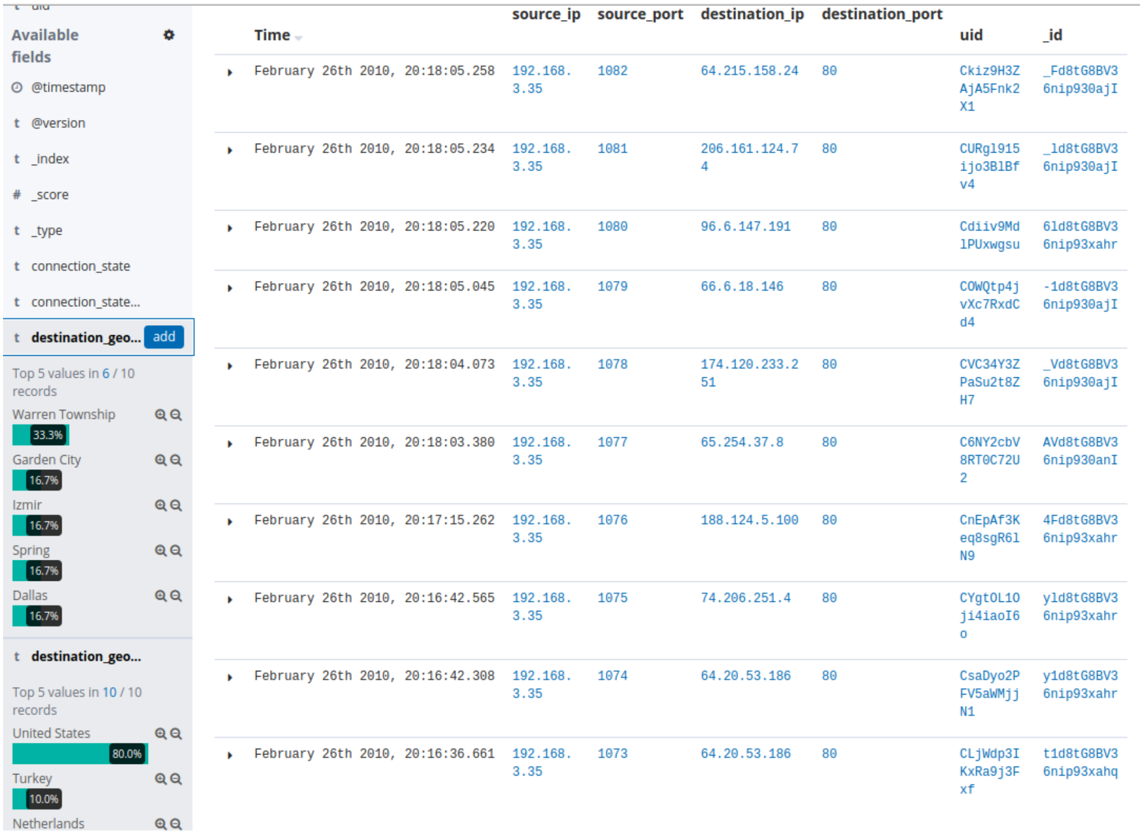


Files - Logs

Limited to 10 results. Refine your search. 1–10 of 95

| | Time | file_ip | destination_ip | source | uid | fuid | _id |
|---|---|---|---|---|---|---|---|
| ▸ | February 26th 2010, 20:18:05.286 | 64.215.158.24 | 192.168.3.35 | HTTP | Ckiz9H3ZAjA5Fnk2X1 | F6msYD1nQXtD9gKSyc | UFd8tG8BV36nip930anQ |
| ▸ | February 26th 2010, 20:18:05.249 | 206.161.124.74 | 192.168.3.35 | HTTP | CURgl915ijo3BlBfv4 | Fz2fS219SekbCP8lOe | T1d8tG8BV36nip930anQ |
| ▸ | February 26th 2010, 20:18:05.066 | 66.6.18.146 | 192.168.3.35 | HTTP | COWQtp4jvXc7RxdCd4 | F1c54o369xe5Kw9SHc | Tld8tG8BV36nip930anQ |
| ▸ | February 26th 2010, 20:18:05.027 | 174.120.233.251 | 192.168.3.35 | HTTP | CVC34Y3ZPaSu2t8ZH7 | F0UkLQ1Tc8sufQFKyc | TVd8tG8BV36nip930anQ |
| ▸ | February 26th 2010, 20:18:04.269 | 174.120.233.251 | 192.168.3.35 | HTTP | CVC34Y3ZPaSu2t8ZH7 | FxWihb2Xe9AJeRYOdk | TFd8tG8BV36nip930anQ |
| ▸ | February 26th 2010, 20:17:15.833 | 188.124.5.100 | 192.168.3.35 | HTTP | CnEpAf3Keq8sgR6lN9 | FsZYun1OeC69Xy6Df7 | S1d8tG8BV36nip930anQ |
| ▸ | February 26th 2010, 20:17:15.401 | 192.168.3.35 | 188.124.5.100 | HTTP | CnEpAf3Keq8sgR6lN9 | FddmTacRpQmli9ga8 | Sld8tG8BV36nip930anQ |
| ▸ | February 26th 2010, 20:16:43.399 | 74.206.251.4 | 192.168.3.35 | HTTP | CYgtOL1Oji4iaoI6o | F464aA3sEgMZ281m0h | O1d8tG8BV36nip930anQ |
| ▸ | February 26th 2010, 20:16:36.840 | 65.254.45.124 | 192.168.3.35 | HTTP | CRSweI2s34g5mIQbUc | FPbvjg2OVZC9UMIQB8 | Old8tG8BV36nip930anQ |
| ▸ | February 26th 2010, 20:16:36.204 | 208.88.226.203 | 192.168.3.35 | HTTP | CgJMVu2EQuYk9qdk0l | FOaWf21Ww4oIkZcuQ | OFd8tG8BV36nip930anQ |

Limited to 10 results. Refine your search. 1–10 of 95



⊙ @timestamp
t @version
t _index
# _score
t _type
t connection_state
t connection_state...
t destination_geo...

Top 5 values in 6 / 10 records

| | |
|---|---|
| Warren Township | 33.3% |
| Garden City | 16.7% |
| Izmir | 16.7% |
| Spring | 16.7% |
| Dallas | 16.7% |

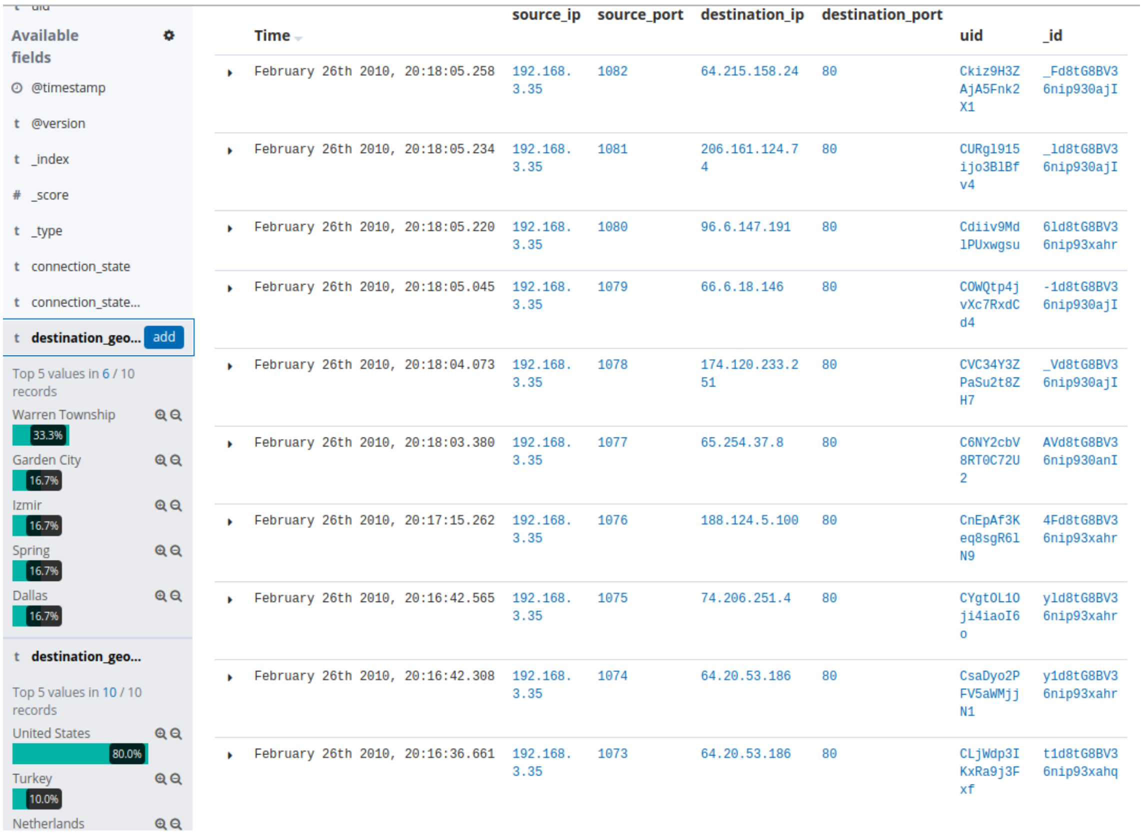
t destination_geo...

Top 5 values in 10 / 10 records

| | |
|---|---|
| United States | 80.0% |
| Turkey | 10.0% |
| Netherlands | |

| | Time | source_ip | source_port | destination_ip | destination_port | uid | _id |
|---|---|---|---|---|---|---|---|
| ▸ | February 26th 2010, 20:18:05.258 | 192.168.3.35 | 1082 | 64.215.158.24 | 80 | Ckiz9H3ZAjA5Fnk2X1 | _Fd8tG8BV36nip930ajI |
| ▸ | February 26th 2010, 20:18:05.234 | 192.168.3.35 | 1081 | 206.161.124.74 | 80 | CURgl915ijo3BlBfv4 | _ld8tG8BV36nip930ajI |
| ▸ | February 26th 2010, 20:18:05.220 | 192.168.3.35 | 1080 | 96.6.147.191 | 80 | Cdiiv9Md1PUxwgsu | 6ld8tG8BV36nip93xahr |
| ▸ | February 26th 2010, 20:18:05.045 | 192.168.3.35 | 1079 | 66.6.18.146 | 80 | COWQtp4jvXc7RxdCd4 | -1d8tG8BV36nip930ajI |
| ▸ | February 26th 2010, 20:18:04.073 | 192.168.3.35 | 1078 | 174.120.233.251 | 80 | CVC34Y3ZPaSu2t8ZH7 | _Vd8tG8BV36nip930ajI |
| ▸ | February 26th 2010, 20:18:03.380 | 192.168.3.35 | 1077 | 65.254.37.8 | 80 | C6NY2cbV8RT0C72U2 | AVd8tG8BV36nip930anI |
| ▸ | February 26th 2010, 20:17:15.262 | 192.168.3.35 | 1076 | 188.124.5.100 | 80 | CnEpAf3Keq8sgR6lN9 | 4Fd8tG8BV36nip93xahr |
| ▸ | February 26th 2010, 20:16:42.565 | 192.168.3.35 | 1075 | 74.206.251.4 | 80 | CYgtOL1Oji4iaoI6o | yld8tG8BV36nip93xahr |
| ▸ | February 26th 2010, 20:16:42.308 | 192.168.3.35 | 1074 | 64.20.53.186 | 80 | CsaDyo2PFV5aWMjjN1 | y1d8tG8BV36nip93xahr |
| ▸ | February 26th 2010, 20:16:36.661 | 192.168.3.35 | 1073 | 64.20.53.186 | 80 | CLjWdp3IKxRa9j3Fxf | t1d8tG8BV36nip93xahq |

**Znalazłem informacje o kolejnych portach na których odbywała się komunikacja, a także przesyłane były pliki i postanowiłem je sprawdzić**



t uid

Available fields

- @timestamp
- t @version
- t _index
- # _score
- t _type
- t connection_state
- t connection_state...
- t destination_geo... add

Top 5 values in 6 / 10 records

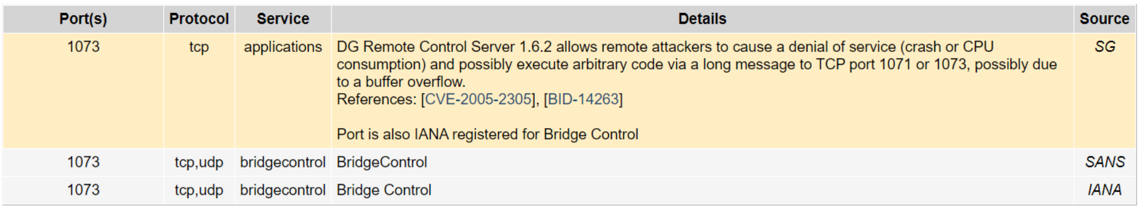
| | |
|---|---|
| Warren Township | 33.3% |
| Garden City | 16.7% |
| Izmir | 16.7% |
| Spring | 16.7% |
| Dallas | 16.7% |

- t destination_geo...

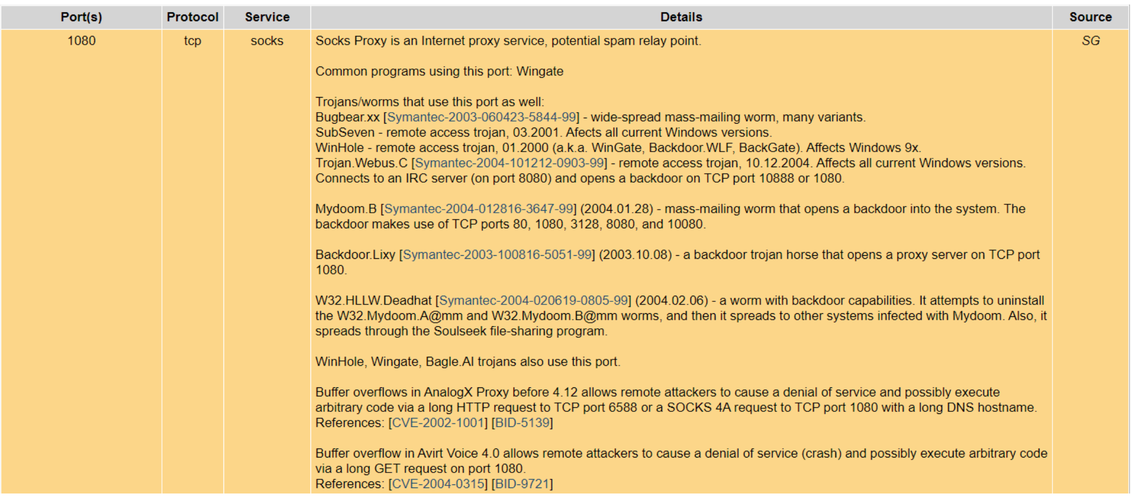
Top 5 values in 10 / 10 records

| | |
|---|---|
| United States | 80.0% |
| Turkey | 10.0% |
| Netherlands | |

| Time | source_ip | source_port | destination_ip | destination_port | uid | _id |
|---|---|---|---|---|---|---|
| February 26th 2010, 20:18:05.258 | 192.168.3.35 | 1082 | 64.215.158.24 | 80 | Ckiz9H3ZAjA5Fnk2X1 | _Fd8tG8BV36nip930ajI |
| February 26th 2010, 20:18:05.234 | 192.168.3.35 | 1081 | 206.161.124.74 | 80 | CURgl915ijo3BlBfv4 | _ld8tG8BV36nip930ajI |
| February 26th 2010, 20:18:05.220 | 192.168.3.35 | 1080 | 96.6.147.191 | 80 | Cdiiv9Md1PUxwgsu | 6ld8tG8BV36nip93xahr |
| February 26th 2010, 20:18:05.045 | 192.168.3.35 | 1079 | 66.6.18.146 | 80 | COWQtp4jvXc7RxdCd4 | -1d8tG8BV36nip930ajI |
| February 26th 2010, 20:18:04.073 | 192.168.3.35 | 1078 | 174.120.233.251 | 80 | CVC34Y3ZPaSu2t8ZH7 | _Vd8tG8BV36nip930ajI |
| February 26th 2010, 20:18:03.380 | 192.168.3.35 | 1077 | 65.254.37.8 | 80 | C6NY2cbV8RT0C72U2 | AVd8tG8BV36nip930anI |
| February 26th 2010, 20:17:15.262 | 192.168.3.35 | 1076 | 188.124.5.100 | 80 | CnEpAf3Keq8sgR6lN9 | 4Fd8tG8BV36nip93xahr |
| February 26th 2010, 20:16:42.565 | 192.168.3.35 | 1075 | 74.206.251.4 | 80 | CYgtOL1Oji4iaoI6o | yld8tG8BV36nip93xahr |
| February 26th 2010, 20:16:42.308 | 192.168.3.35 | 1074 | 64.20.53.186 | 80 | CsaDyo2PFV5aWMjjN1 | y1d8tG8BV36nip93xahr |
| February 26th 2010, 20:16:36.661 | 192.168.3.35 | 1073 | 64.20.53.186 | 80 | CLjWdp3IKxRa9j3Fxf | t1d8tG8BV36nip93xahq |

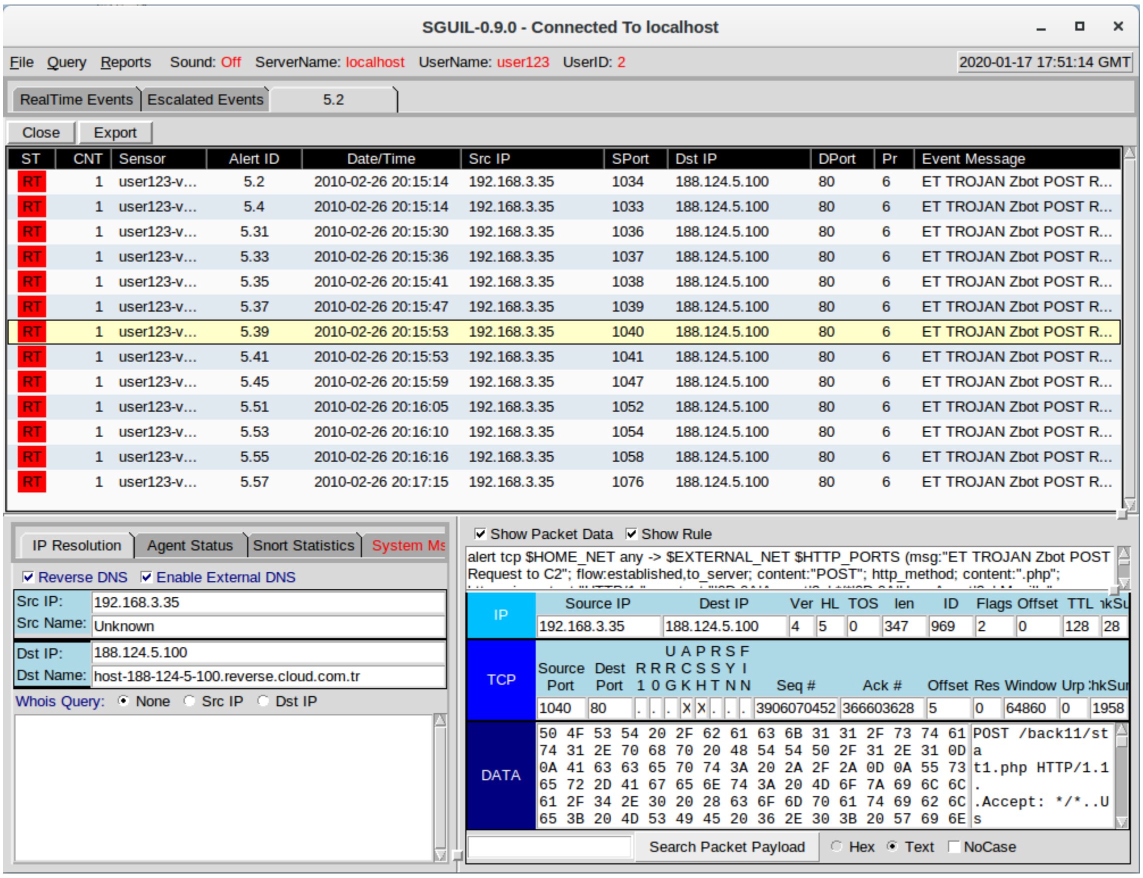


| Port(s) | Protocol | Service | Details | Source |
|---|---|---|---|---|
| 1073 | tcp | applications | DG Remote Control Server 1.6.2 allows remote attackers to cause a denial of service (crash or CPU consumption) and possibly execute arbitrary code via a long message to TCP port 1071 or 1073, possibly due to a buffer overflow.<br>References: [CVE-2005-2305], [BID-14263]<br>Port is also IANA registered for Bridge Control | *SG* |
| 1073 | tcp,udp | bridgecontrol | BridgeControl | *SANS* |
| 1073 | tcp,udp | bridgecontrol | Bridge Control | *IANA* |



| Port(s) | Protocol | Service | Details | Source |
|---|---|---|---|---|
| 1080 | tcp | socks | Socks Proxy is an Internet proxy service, potential spam relay point.<br>Common programs using this port: Wingate<br>Trojans/worms that use this port as well:<br>Bugbear.xx [Symantec-2003-060423-5844-99] - wide-spread mass-mailing worm, many variants.<br>SubSeven - remote access trojan, 03.2001. Afects all current Windows versions.<br>WinHole - remote access trojan, 01.2000 (a.k.a. WinGate, Backdoor.WLF, BackGate). Affects Windows 9x.<br>Trojan.Webus.C [Symantec-2004-101212-0903-99] - remote access trojan, 10.12.2004. Affects all current Windows versions. Connects to an IRC server (on port 8080) and opens a backdoor on TCP port 10888 or 1080.<br>Mydoom.B [Symantec-2004-012816-3647-99] (2004.01.28) - mass-mailing worm that opens a backdoor into the system. The backdoor makes use of TCP ports 80, 1080, 3128, 8080, and 10080.<br>Backdoor.Lixy [Symantec-2003-100816-5051-99] (2003.10.08) - a backdoor trojan horse that opens a proxy server on TCP port 1080.<br>W32.HLLW.Deadhat [Symantec-2004-020619-0805-99] (2004.02.06) - a worm with backdoor capabilities. It attempts to uninstall the W32.Mydoom.A@mm and W32.Mydoom.B@mm worms, and then it spreads to other systems infected with Mydoom. Also, it spreads through the Soulseek file-sharing program.<br>WinHole, Wingate, Bagle.AI trojans also use this port.<br>Buffer overflows in AnalogX Proxy before 4.12 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a long HTTP request to TCP port 6588 or a SOCKS 4A request to TCP port 1080 with a long DNS hostname.<br>References: [CVE-2002-1001] [BID-5139]<br>Buffer overflow in Avirt Voice 4.0 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long GET request on port 1080.<br>References: [CVE-2004-0315] [BID-9721] | *SG* |

**Uruchomiłem także program Sguily i przejżałem logi**



Sound: Off ServerName: localhost UserName: user123 UserID: 2 2020-01-17 17:51:14 GMT

| ST | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|---|---|---|---|---|---|---|---|---|---|---|
| RT | 1 | user123-v... | 5.2 | 2010-02-26 20:15:14 | 192.168.3.35 | 1034 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.4 | 2010-02-26 20:15:14 | 192.168.3.35 | 1033 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.31 | 2010-02-26 20:15:30 | 192.168.3.35 | 1036 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.33 | 2010-02-26 20:15:36 | 192.168.3.35 | 1037 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.35 | 2010-02-26 20:15:41 | 192.168.3.35 | 1038 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.37 | 2010-02-26 20:15:47 | 192.168.3.35 | 1039 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.39 | 2010-02-26 20:15:53 | 192.168.3.35 | 1040 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.41 | 2010-02-26 20:15:53 | 192.168.3.35 | 1041 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.45 | 2010-02-26 20:15:59 | 192.168.3.35 | 1047 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.51 | 2010-02-26 20:16:05 | 192.168.3.35 | 1052 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.53 | 2010-02-26 20:16:10 | 192.168.3.35 | 1054 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.55 | 2010-02-26 20:16:16 | 192.168.3.35 | 1058 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |
| RT | 1 | user123-v... | 5.57 | 2010-02-26 20:17:15 | 192.168.3.35 | 1076 | 188.124.5.100 | 80 | 6 | ET TROJAN Zbot POST R... |

☑ Reverse DNS ☑ Enable External DNS

Src IP: 192.168.3.35
Src Name: Unknown

Dst IP: 188.124.5.100
Dst Name: host-188-124-5-100.reverse.cloud.com.tr

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Zbot POST
Request to C2"; flow:established,to_server; content:"POST"; http_method; content:".php";
```

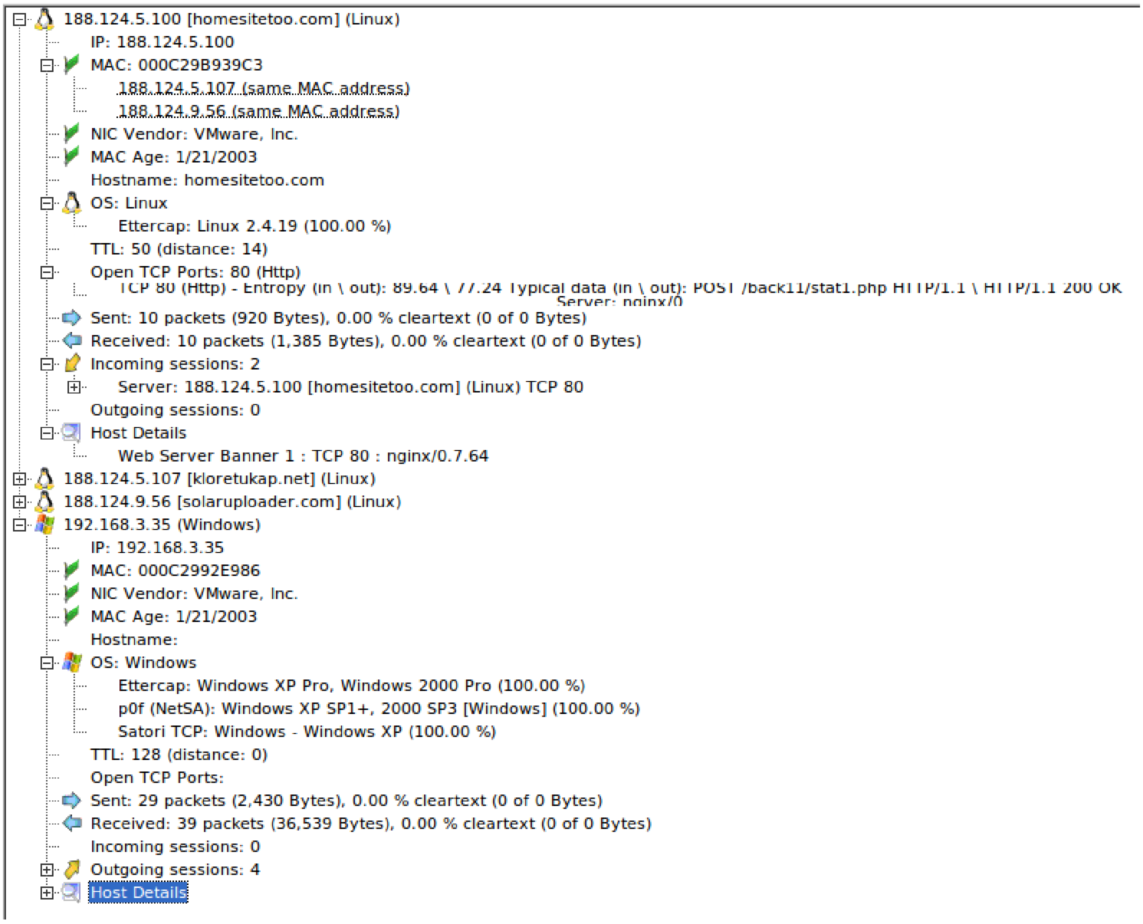
| IP | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ıkSu |
|---|---|---|---|---|---|---|---|---|---|---|---|
|  | 192.168.3.35 | 188.124.5.100 | 4 | 5 | 0 | 347 | 969 | 2 | 0 | 128 | 28 |

| 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 | :hkSur |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | 1040 | 80 | . | . | . | X | X | . | . | . | 3906070452 | 366603628 | 5 | 0 | 64860 | 0 | 1958 |

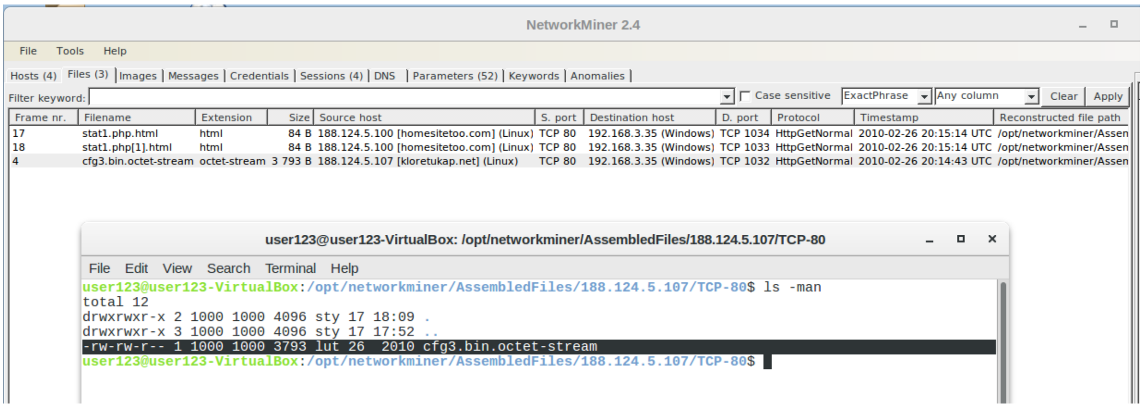
```
DATA
50 4F 53 54 20 2F 62 61 63 6B 31 31 2F 73 74 61 POST /back11/st
74 31 2E 70 68 70 20 48 54 54 50 2F 31 2E 31 0D a
0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 55 73 t1.php HTTP/1.1
65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C .
61 2F 34 2E 30 20 28 63 6F 6D 70 61 74 69 62 6C .Accept: */*..U
65 3B 20 4D 53 49 45 20 36 2E 30 3B 20 57 69 6E s
```

○ Hex ● Text □ NoCase

**W NetworkMainer również znalazłem kilka dodatkowych informacji, a także udało mi się uzyskac pliki, które mogą zostać poddane dalszej analizie.



```
188.124.5.100 [homesitetoo.com] (Linux)
    IP: 188.124.5.100
    MAC: 000C29B939C3
        188.124.5.107 (same MAC address)
        188.124.9.56 (same MAC address)
    NIC Vendor: VMware, Inc.
    MAC Age: 1/21/2003
    Hostname: homesitetoo.com
    OS: Linux
        Ettercap: Linux 2.4.19 (100.00 %)
    TTL: 50 (distance: 14)
    Open TCP Ports: 80 (Http)
        TCP 80 (Http) - Entropy (in \ out): 89.64 \ 77.24 Typical data (in \ out): POST /back11/stat1.php HTTP/1.1 \ HTTP/1.1 200 OK
                                                  Server: nginx/0
    Sent: 10 packets (920 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 10 packets (1,385 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 2
        Server: 188.124.5.100 [homesitetoo.com] (Linux) TCP 80
    Outgoing sessions: 0
    Host Details
        Web Server Banner 1 : TCP 80 : nginx/0.7.64
188.124.5.107 [kloretukap.net] (Linux)
188.124.9.56 [solaruploader.com] (Linux)
192.168.3.35 (Windows)
    IP: 192.168.3.35
    MAC: 000C2992E986
    NIC Vendor: VMware, Inc.
    MAC Age: 1/21/2003
    Hostname:
    OS: Windows
        Ettercap: Windows XP Pro, Windows 2000 Pro (100.00 %)
        p0f (NetSA): Windows XP SP1+, 2000 SP3 [Windows] (100.00 %)
        Satori TCP: Windows - Windows XP (100.00 %)
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 29 packets (2,430 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 39 packets (36,539 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 4
    Host Details
```



NetworkMiner 2.4
File Tools Help
Hosts (4) | Files (3) | Images | Messages | Credentials | Sessions (4) | DNS | Parameters (52) | Keywords | Anomalies
Filter keyword:
□ Case sensitive
ExactPhrase
Any column
Clear
Apply

| Frame nr. | Filename | Extension | Size | Source host | S. port | Destination host | D. port | Protocol | Timestamp | Reconstructed file path |
|---|---|---|---|---|---|---|---|---|---|---|
| 17 | stat1.php.html | html | 84 B | 188.124.5.100 [homesitetoo.com] (Linux) | TCP 80 | 192.168.3.35 (Windows) | TCP 1034 | HttpGetNormal | 2010-02-26 20:15:14 UTC | /opt/networkminer/Assen |
| 18 | stat1.php[1].html | html | 84 B | 188.124.5.100 [homesitetoo.com] (Linux) | TCP 80 | 192.168.3.35 (Windows) | TCP 1033 | HttpGetNormal | 2010-02-26 20:15:14 UTC | /opt/networkminer/Assen |
| 4 | cfg3.bin.octet-stream | octet-stream | 3 793 B | 188.124.5.107 [kloretukap.net] (Linux) | TCP 80 | 192.168.3.35 (Windows) | TCP 1032 | HttpGetNormal | 2010-02-26 20:14:43 UTC | /opt/networkminer/Assen |

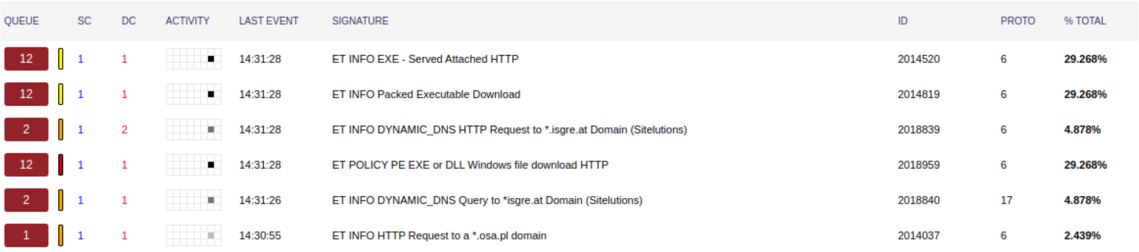
user123@user123-VirtualBox: /opt/networkminer/AssembledFiles/188.124.5.107/TCP-80
File Edit View Search Terminal Help

```
user123@user123-VirtualBox:/opt/networkminer/AssembledFiles/188.124.5.107/TCP-80$ ls -man
total 12
drwxrwxr-x 2 1000 1000 4096 sty 17 18:09 .
drwxrwxr-x 3 1000 1000 4096 sty 17 17:52 ..
-rw-rw-r-- 1 1000 1000 3793 lut 26  2010 cfg3.bin.octet-stream
user123@user123-VirtualBox:/opt/networkminer/AssembledFiles/188.124.5.107/TCP-80$
```

## Jako drugi do analizy wybrałem i zaimportowałem plik `best-malwere-protection.pcap` .

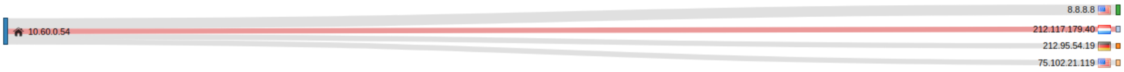
`sudo so-import-pcap best-malwere-protection.pcap` Ponownie zacząłem od Kibany i Squerta.

**Widok zaimportowanego ruchu w Squert - dopasowane sygnatury**

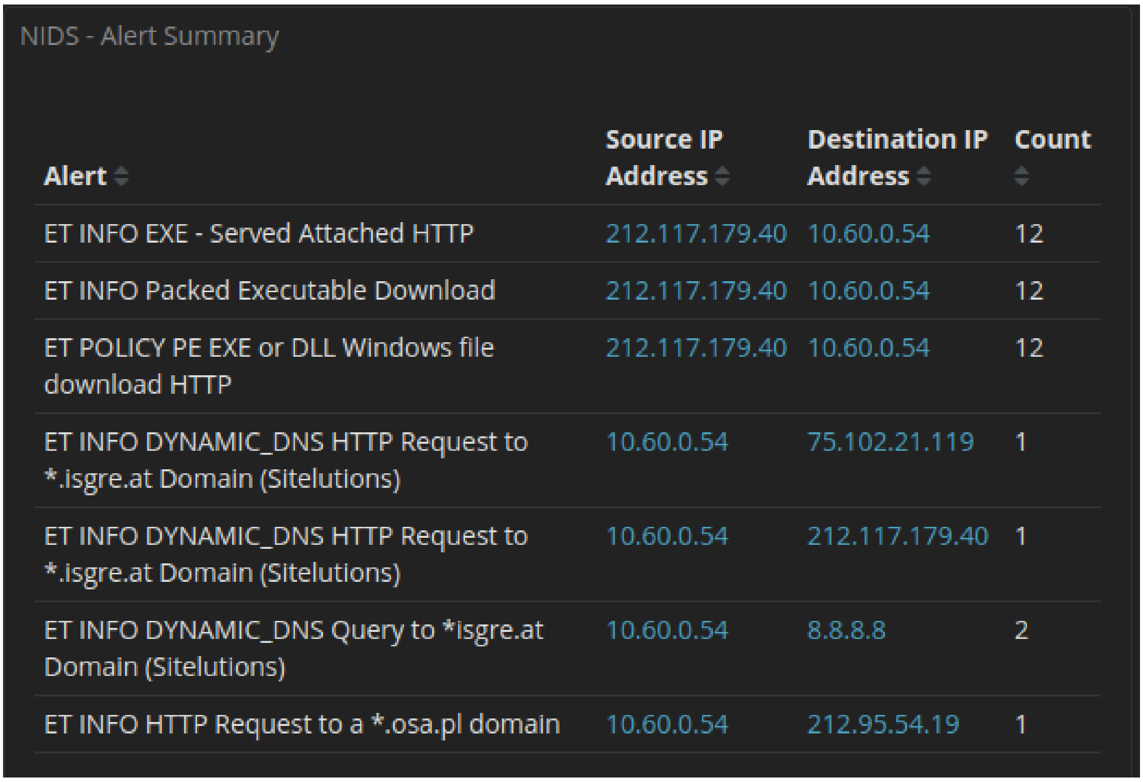


| QUEUE | SC | DC | ACTIVITY | LAST EVENT | SIGNATURE | ID | PROTO | % TOTAL |
|---|---|---|---|---|---|---|---|---|
| 12 | 1 | 1 | ■ | 14:31:28 | ET INFO EXE - Served Attached HTTP | 2014520 | 6 | **29.268%** |
| 12 | 1 | 1 | ■ | 14:31:28 | ET INFO Packed Executable Download | 2014819 | 6 | **29.268%** |
| 2 | 1 | 2 | ■ | 14:31:28 | ET INFO DYNAMIC_DNS HTTP Request to *.isgre.at Domain (Sitelutions) | 2018839 | 6 | **4.878%** |
| 12 | 1 | 1 | ■ | 14:31:28 | ET POLICY PE EXE or DLL Windows file download HTTP | 2018959 | 6 | **29.268%** |
| 2 | 1 | 1 | ■ | 14:31:26 | ET INFO DYNAMIC_DNS Query to *isgre.at Domain (Sitelutions) | 2018840 | 17 | **4.878%** |
| 1 | 1 | 1 | ■ | 14:30:55 | ET INFO HTTP Request to a *.osa.pl domain | 2014037 | 6 | **2.439%** |

**Następnie w Squert sprawdziłem takie informacje jak: sygnatury dopasowane przez program, adresy IP z którymi najczęściej występowała komunikacja, oraz porty.** ![portsCountryIp](https://user-images.githubusercontent.com/56591106/72671097-ab574880-3a45-11ea-929c-062cf9c13f98.PNG



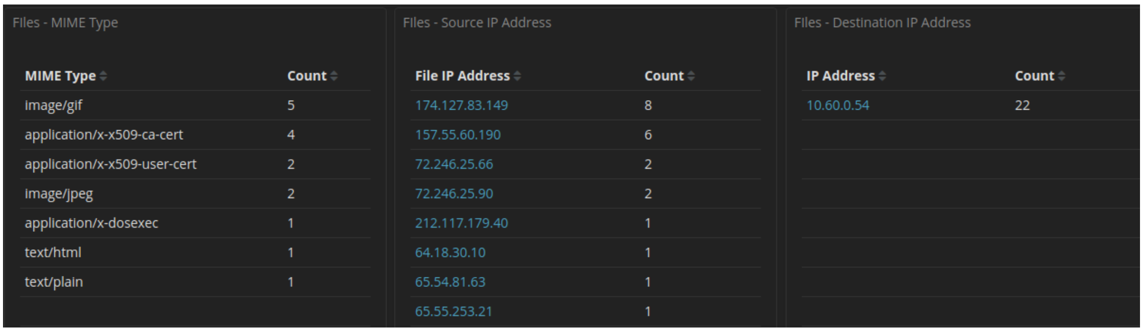
**Alerty NIDS wraz z powiązanami adresami IP**



NIDS - Alert Summary

| Alert | Source IP Address | Destination IP Address | Count |
|---|---|---|---|
| ET INFO EXE - Served Attached HTTP | 212.117.179.40 | 10.60.0.54 | 12 |
| ET INFO Packed Executable Download | 212.117.179.40 | 10.60.0.54 | 12 |
| ET POLICY PE EXE or DLL Windows file download HTTP | 212.117.179.40 | 10.60.0.54 | 12 |
| ET INFO DYNAMIC_DNS HTTP Request to *.isgre.at Domain (Sitelutions) | 10.60.0.54 | 75.102.21.119 | 1 |
| ET INFO DYNAMIC_DNS HTTP Request to *.isgre.at Domain (Sitelutions) | 10.60.0.54 | 212.117.179.40 | 1 |
| ET INFO DYNAMIC_DNS Query to *isgre.at Domain (Sitelutions) | 10.60.0.54 | 8.8.8.8 | 2 |
| ET INFO HTTP Request to a *.osa.pl domain | 10.60.0.54 | 212.95.54.19 | 1 |

## Typy odbieranych/wysyłanych plików oraz adresy z którymi się to odbywało



Files - MIME Type

| MIME Type | Count |
|---|---|
| image/gif | 5 |
| application/x-x509-ca-cert | 4 |
| application/x-x509-user-cert | 2 |
| image/jpeg | 2 |
| application/x-dosexec | 1 |
| text/html | 1 |
| text/plain | 1 |

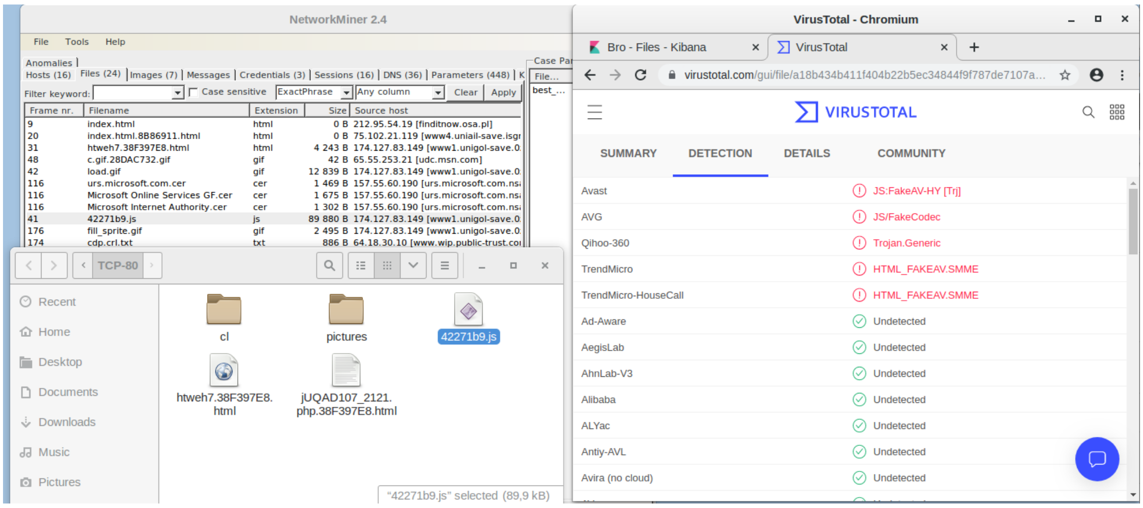
Files - Source IP Address

| File IP Address | Count |
|---|---|
| 174.127.83.149 | 8 |
| 157.55.60.190 | 6 |
| 72.246.25.66 | 2 |
| 72.246.25.90 | 2 |
| 212.117.179.40 | 1 |
| 64.18.30.10 | 1 |
| 65.54.81.63 | 1 |
| 65.55.253.21 | 1 |

Files - Destination IP Address

| IP Address | Count |
|---|---|
| 10.60.0.54 | 22 |

## Pliki wyodrębnione NetworkMinerem oraz ich analizy w VirusTotal

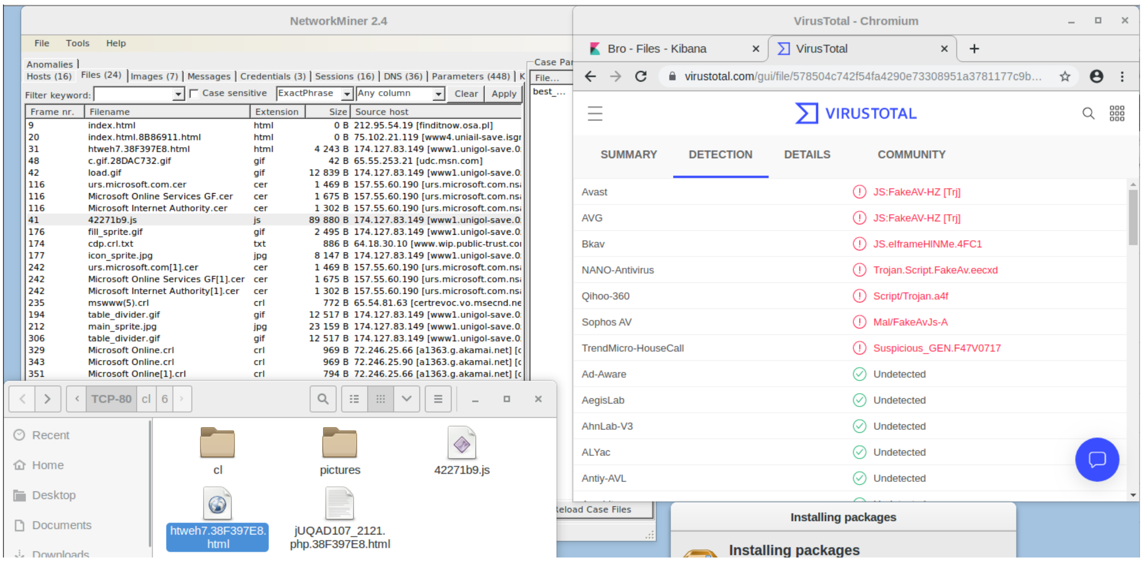


NetworkMiner 2.4
File Tools Help
Anomalies
Hosts (16) Files (24) Images (7) Messages Credentials (3) Sessions (16) DNS (36) Parameters (448) K
Filter keyword: ☐ Case sensitive ExactPhrase Any column Clear Apply
Case Par
File...
best_...

| Frame nr. | Filename | Extension | Size | Source host |
|---|---|---|---|---|
| 9 | index.html | html | 0 B | 212.95.54.19 [finditnow.osa.pl] |
| 20 | index.html.8B86911.html | html | 0 B | 75.102.21.119 [www4.uniail-save.isgr |
| 31 | htweh7.38F397E8.html | html | 4 243 B | 174.127.83.149 [www1.unigol-save.0. |
| 48 | c.gif.28DAC732.gif | gif | 42 B | 65.55.253.21 [udc.msn.com] |
| 42 | load.gif | gif | 12 839 B | 174.127.83.149 [www1.unigol-save.0. |
| 116 | urs.microsoft.com.cer | cer | 1 469 B | 157.55.60.190 [urs.microsoft.com.nsa |
| 116 | Microsoft Online Services GF.cer | cer | 1 675 B | 157.55.60.190 [urs.microsoft.com.nsa |
| 116 | Microsoft Internet Authority.cer | cer | 1 302 B | 157.55.60.190 [urs.microsoft.com.nsa |
| 41 | 42271b9.js | js | 89 880 B | 174.127.83.149 [www1.unigol-save.0. |
| 176 | fill_sprite.gif | gif | 2 495 B | 174.127.83.149 [www1.unigol-save.0. |
| 174 | cdp.crl.txt | txt | 886 B | 64.18.30.10 [www.wip.public-trust.co |

"42271b9.js" selected (89,9 kB)

| | |
|---|---|
| Avast | JS:FakeAV-HY [Trj] |
| AVG | JS/FakeCodec |
| Qihoo-360 | Trojan.Generic |
| TrendMicro | HTML_FAKEAV.SMME |
| TrendMicro-HouseCall | HTML_FAKEAV.SMME |
| Ad-Aware | Undetected |
| AegisLab | Undetected |
| AhnLab-V3 | Undetected |
| Alibaba | Undetected |
| ALYac | Undetected |
| Antiy-AVL | Undetected |
| Avira (no cloud) | Undetected |

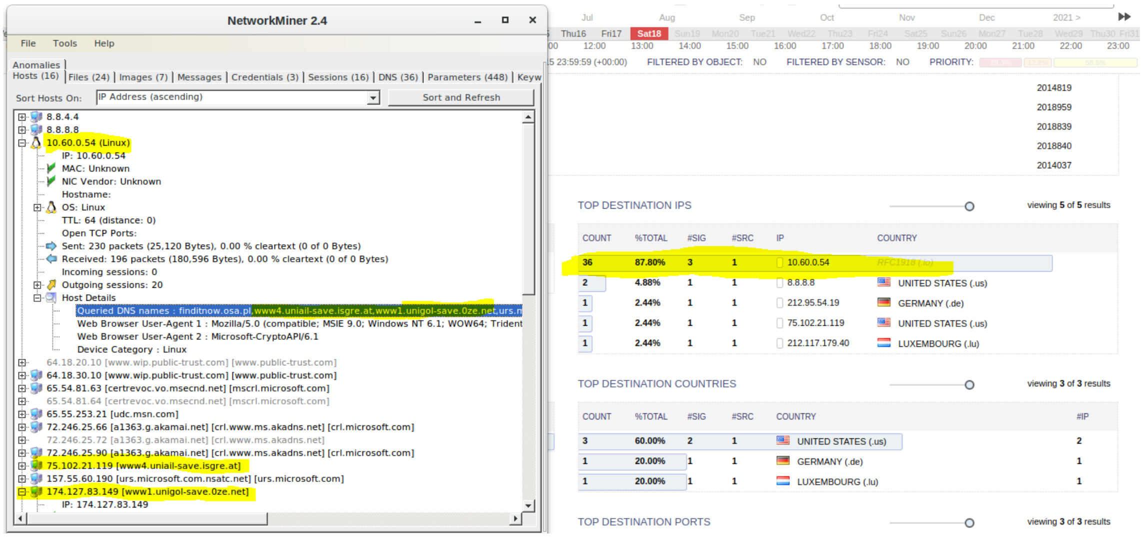


NetworkMiner 2.4
File Tools Help
Anomalies
Hosts (16) Files (24) Images (7) Messages Credentials (3) Sessions (16) DNS (36) Parameters (448) K
Filter keyword: ☐ Case sensitive ExactPhrase Any column Clear Apply
Case Par
File...
best_...

| Frame nr. | Filename | Extension | Size | Source host |
|---|---|---|---|---|
| 9 | index.html | html | 0 B | 212.95.54.19 [finditnow.osa.pl] |
| 20 | index.html.8B86911.html | html | 0 B | 75.102.21.119 [www4.uniail-save.isgr |
| 31 | htweh7.38F397E8.html | html | 4 243 B | 174.127.83.149 [www1.unigol-save.0. |
| 48 | c.gif.28DAC732.gif | gif | 42 B | 65.55.253.21 [udc.msn.com] |
| 42 | load.gif | gif | 12 839 B | 174.127.83.149 [www1.unigol-save.0. |
| 116 | urs.microsoft.com.cer | cer | 1 469 B | 157.55.60.190 [urs.microsoft.com.nsa |
| 116 | Microsoft Online Services GF.cer | cer | 1 675 B | 157.55.60.190 [urs.microsoft.com.nsa |
| 116 | Microsoft Internet Authority.cer | cer | 1 302 B | 157.55.60.190 [urs.microsoft.com.nsa |
| 41 | 42271b9.js | js | 89 880 B | 174.127.83.149 [www1.unigol-save.0. |
| 176 | fill_sprite.gif | gif | 2 495 B | 174.127.83.149 [www1.unigol-save.0. |
| 174 | cdp.crl.txt | txt | 886 B | 64.18.30.10 [www.wip.public-trust.co |
| 177 | icon_sprite.jpg | jpg | 8 147 B | 174.127.83.149 [www1.unigol-save.0. |
| 242 | urs.microsoft.com[1].cer | cer | 1 469 B | 157.55.60.190 [urs.microsoft.com.nsa |
| 242 | Microsoft Online Services GF[1].cer | cer | 1 675 B | 157.55.60.190 [urs.microsoft.com.nsa |
| 242 | Microsoft Internet Authority[1].cer | cer | 1 302 B | 157.55.60.190 [urs.microsoft.com.nsa |
| 235 | mswww(5).crl | crl | 772 B | 65.54.81.63 [certrevoc.vo.msecnd.ne |
| 194 | table_divider.gif | gif | 12 517 B | 174.127.83.149 [www1.unigol-save.0. |
| 212 | main_sprite.jpg | jpg | 23 159 B | 174.127.83.149 [www1.unigol-save.0. |
| 306 | table_divider.gif | gif | 12 517 B | 174.127.83.149 [www1.unigol-save.0. |
| 329 | Microsoft Online.crl | crl | 969 B | 72.246.25.66 [a1363.g.akamai.net] [c |
| 343 | Microsoft Online.crl | crl | 969 B | 72.246.25.90 [a1363.g.akamai.net] [c |
| 351 | Microsoft Online[1].crl | crl | 794 B | 72.246.25.66 [a1363.g.akamai.net] [c |

| | |
|---|---|
| Avast | JS:FakeAV-HZ [Trj] |
| AVG | JS:FakeAV-HZ [Trj] |
| Bkav | JS.elframeHINMe.4FC1 |
| NANO-Antivirus | Trojan.Script.FakeAv.eecxd |
| Qihoo-360 | Script/Trojan.a4f |
| Sophos AV | Mal/FakeAvJs-A |
| TrendMicro-HouseCall | Suspicious_GEN.F47V0717 |
| Ad-Aware | Undetected |
| AegisLab | Undetected |
| AhnLab-V3 | Undetected |
| ALYac | Undetected |
| Antiy-AVL | Undetected |

**Powiązanie analizowanych plików z adresem IP**



```
8.8.4.4
8.8.8.8
10.60.0.54 (Linux)
    IP: 10.60.0.54
    MAC: Unknown
    NIC Vendor: Unknown
    Hostname:
    OS: Linux
    TTL: 64 (distance: 0)
    Open TCP Ports:
    Sent: 230 packets (25,120 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 196 packets (180,596 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 20
    Host Details
        Queried DNS names : finditnow.osa.pl,www4.uniail-save.isgre.at,www1.unigol-save.0ze.net,urs.n
        Web Browser User-Agent 1 : Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident
        Web Browser User-Agent 2 : Microsoft-CryptoAPI/6.1
        Device Category : Linux
64.18.20.10 [www.wip.public-trust.com] [www.public-trust.com]
64.18.30.10 [www.wip.public-trust.com] [www.public-trust.com]
65.54.81.63 [certrevoc.vo.msecnd.net] [mscrl.microsoft.com]
65.54.81.64 [certrevoc.vo.msecnd.net] [mscrl.microsoft.com]
65.55.253.21 [udc.msn.com]
72.246.25.66 [a1363.g.akamai.net] [crl.www.ms.akadns.net] [crl.microsoft.com]
72.246.25.72 [a1363.g.akamai.net] [crl.www.ms.akadns.net]
72.246.25.90 [a1363.g.akamai.net] [crl.www.ms.akadns.net] [crl.microsoft.com]
75.102.21.119 [www4.uniail-save.isgre.at]
157.55.60.190 [urs.microsoft.com.nsatc.net] [urs.microsoft.com]
174.127.83.149 [www1.unigol-save.0ze.net]
    IP: 174.127.83.149
```

5 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY:

2014819
2018959
2018839
2018840
2014037

TOP DESTINATION IPS — viewing **5** of **5** results

| COUNT | %TOTAL | #SIG | #SRC | IP | COUNTRY |
|---|---|---|---|---|---|
| 36 | 87.80% | 3 | 1 | 10.60.0.54 | RFC1918 (.lo) |
| 2 | 4.88% | 1 | 1 | 8.8.8.8 | UNITED STATES (.us) |
| 1 | 2.44% | 1 | 1 | 212.95.54.19 | GERMANY (.de) |
| 1 | 2.44% | 1 | 1 | 75.102.21.119 | UNITED STATES (.us) |
| 1 | 2.44% | 1 | 1 | 212.117.179.40 | LUXEMBOURG (.lu) |

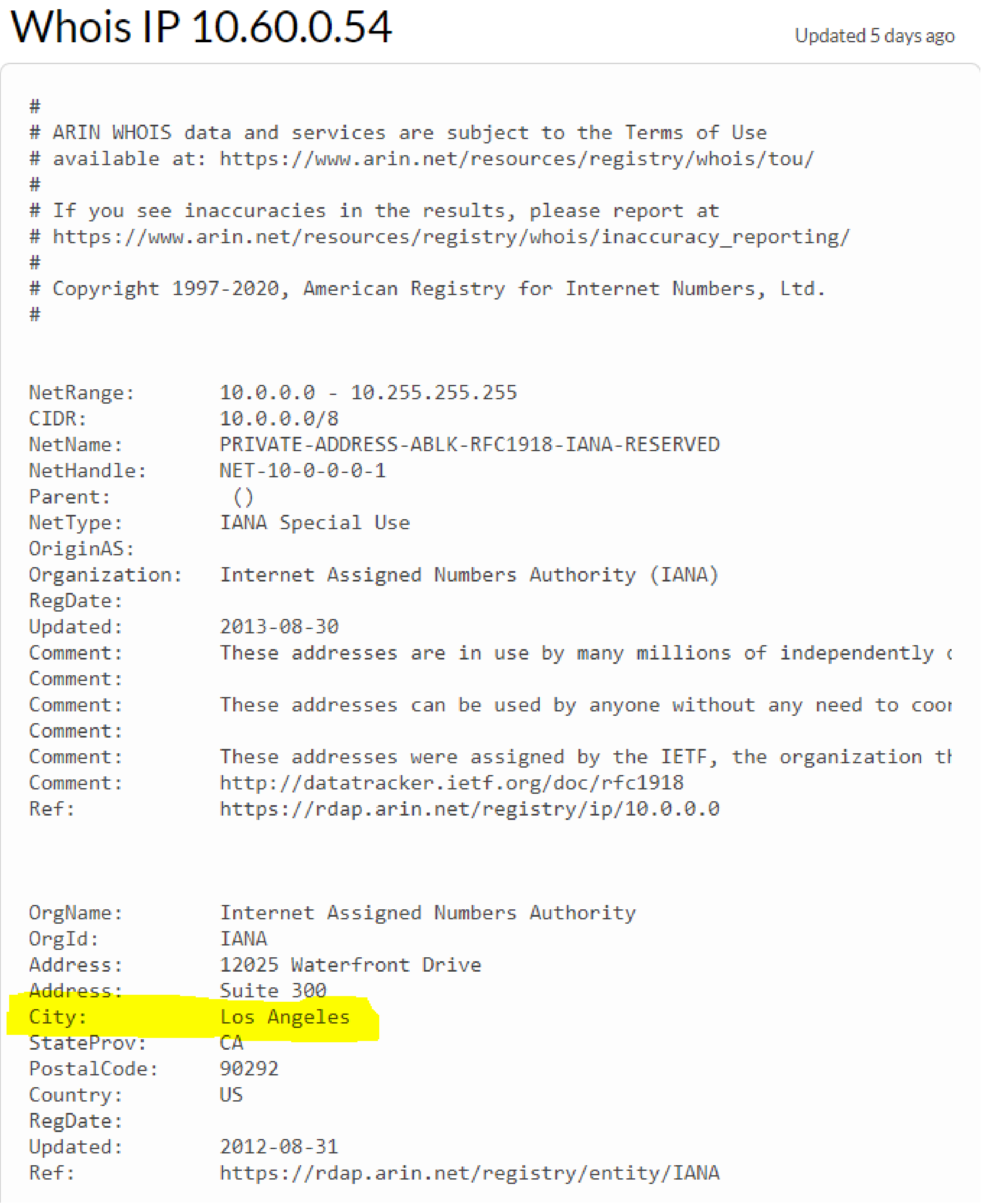
TOP DESTINATION COUNTRIES — viewing **3** of **3** results

| COUNT | %TOTAL | #SIG | #SRC | COUNTRY | #IP |
|---|---|---|---|---|---|
| 3 | 60.00% | 2 | 1 | UNITED STATES (.us) | 2 |
| 1 | 20.00% | 1 | 1 | GERMANY (.de) | 1 |
| 1 | 20.00% | 1 | 1 | LUXEMBOURG (.lu) | 1 |

TOP DESTINATION PORTS — viewing **3** of **3** results

**Adres `174.127.83.149` widnieje w jadnej z baz danych jako zagrożenie** ![image](https://user-images.githubusercontent.com/56591106/72671346-1fdfb680-3a49-11ea-8236-b4b689cd1d35.png

**Podejrzany adres IP w whoIs, adres również z USA**



## Whois IP 10.60.0.54

Updated 5 days ago

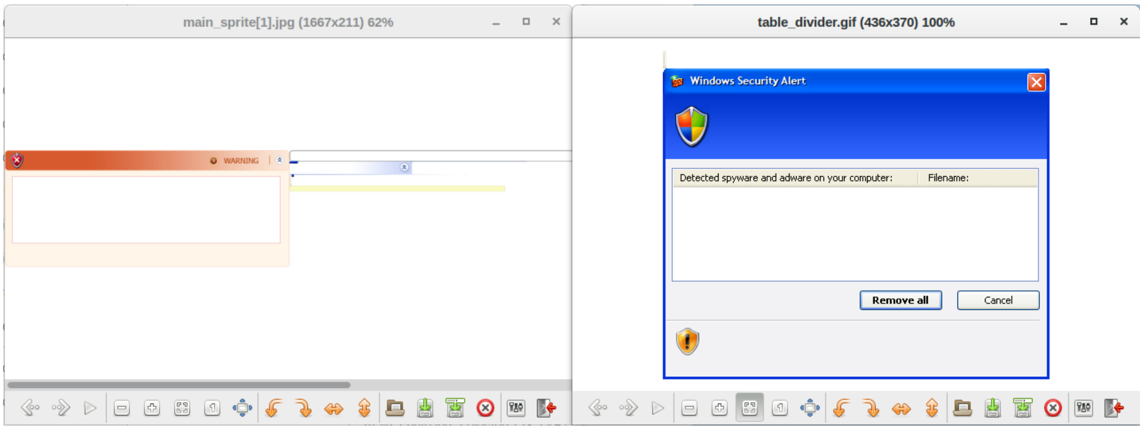
```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#


NetRange:       10.0.0.0 - 10.255.255.255
CIDR:           10.0.0.0/8
NetName:        PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle:      NET-10-0-0-0-1
Parent:          ()
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:
Updated:        2013-08-30
Comment:        These addresses are in use by many millions of independently c
Comment:
Comment:        These addresses can be used by anyone without any need to coor
Comment:
Comment:        These addresses were assigned by the IETF, the organization th
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/10.0.0.0



OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA
```

**Obrazy wyodrębnione przez NetworkMiner, moim zdaniem podejrzane


main_sprite[1].jpg (1667x211) 62%
WARNING
table_divider.gif (436x370) 100%
Windows Security Alert
Filename:
Remove all
Cancel

Detected spyware and adware on your computer: