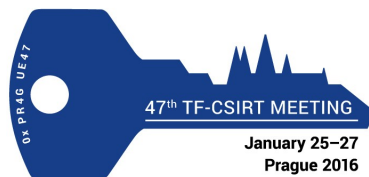


# altrail – Malicious traffic detection system

Miroslav Stampar

(mstampar@zsis.hr; miroslav@sqlmap.org; @stamparm)



# Project motivation

- Idea of a system that would produce less “noise” by condensing numerous events into “threats”
- Prioritization of malicious activities coming from inside (e.g. malware) - e.g. from CERT perspective, malware infection is a more severe problem than “mass scans”
- Usage of available “knowledge” in form of publicly available blacklists and custom lists of malicious trails (IOCs) per malware campaign
- System should not be (too) resource intensive

# Short glossary (used terms)

- Trail – suspicious and/or malicious IP address, DNS name, URL (path), HTTP User-Agent, etc.
- Blacklist – list of trails
- Event – log record with details of a single detected trail occurrence
- Threat – all trail related events coming from the same source IP (or multiple in case of distributed attacks)
- Heuristics – non-trail related mechanisms for recognition of suspicious and/or malicious threats

# Short history

- 2014. – Croatia heavily struck with banking malware (ZeuS VM – KINS)
- Nov. 2014. – started creation of custom free and open-source passive network monitoring “tool” (mainly for in-house usage)
- Dec. 2014. – “DNScrutinize” (only DNS traffic monitoring)
- Dec. 2014. – renamed to “Maltrail” (expansion from DNS only to IP/DNS/URL monitoring)
- Feb. 2015. – started with usage in production environment (HITRONet – over 25 .HR government bodies)

# Repository (GitHub)

GitHub, Inc. (US) | <https://github.com/stamparm/maltrail> | Search

This repository Search Pull requests Issues Gist

stamparm / maltrail Unwatch 119 Star 1,086 Fork 113

Code Issues 18 Pull requests 0 Wiki Pulse Graphs Settings

Malicious traffic detection system — Edit

843 commits 1 branch 1 release 3 contributors

Branch: master New pull request New file Find file SSH git@github.com:stamparm/mal Download ZIP

stamparm Adding new mass scanner Latest commit 9b27115 15 hours ago


core	Adding new mass scanner	15 hours ago
html	Minor style update	18 hours ago
misc	Some fine tuning	21 hours ago
plugins	Update of plugins	3 days ago
trails	Adding new mass scanner	15 hours ago
attributes	Minor update	6 days ago

# First commit

## Adding a new file

🔑 master 📁 0.9

[Browse files](#)

 stamparm committed on 4 Dec 2014

0 parents    commit bd2083e5939081886ae92e2b332bd7db56230646

📄 Showing 1 changed file with 126 additions and 0 deletions.

Unified

Split

126 ■■■■■ dnsscrutinize.py

```
...      ...      @@ -0,0 +1,126 @@
1  +import logging, pickle, optparse, os, re, socket, subprocess, tempfile, time, urllib2, zipfile, zlib
2  +
3  +NAME, VERSION, AUTHOR, LICENSE = "DNScrutinize", "0.1b", "Miroslav Stampar (@stamparm)", "Public domain (FREE)"
4  +
5  +try:
6  +    logging.getLogger("scapy.runtime").setLevel(logging.ERROR)
7  +
8  +    from scapy.all import *
9  +except ImportError:
10 +    exit("[!] please install Scapy (e.g. '%s')" % ("sudo apt-get install scapy" if not subprocess.mswindows else "http://www
11 +
12 +TIMEOUT = 30
13 +FRESH_LISTS_DELTA_DAYS = 2
14 +DOMAINS_FILE = "domains.bin"
15 +OUTPUT_FORMAT = "|{0:^16}|{1:^19s}|{2:^40s}|{3:^15s}|{4:^20s}|"
16 +
17 +MALWAREDOMAINLIST_URL = "http://www.malwaredomainlist.com/hostslist/hosts.txt"
18 +MALWAREDOMAINS_URL = "http://malwaredomains.lehigh.edu/files/domains.txt"
19 +ZEUS_ABUSECH_URL = "https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist"
20 +
```

# Current status (Jan. 2016.)

- 51 daily pulled blacklist feeds (e.g. alienvault, autoshun, badips, etc.)
- 31 (manually collected) static sinkhole trail lists
- 103 malware static trail lists based on IOCs from AV reports
- 12 static lists of “suspicious” trails (e.g. browser\_hijacking, computrace, dynamic\_domain, ipinfo, superfish, etc.)
- 13 heuristic mechanisms (e.g. port scanning, long domains, sinkhole responses, suspicious HTTP requests, suspicious HTTP user agents, excessive NXDOMAIN, etc.)

# Blacklist feeds (example)

```
osint.bambenekconsulting.com/feeds/dga-feed.txt

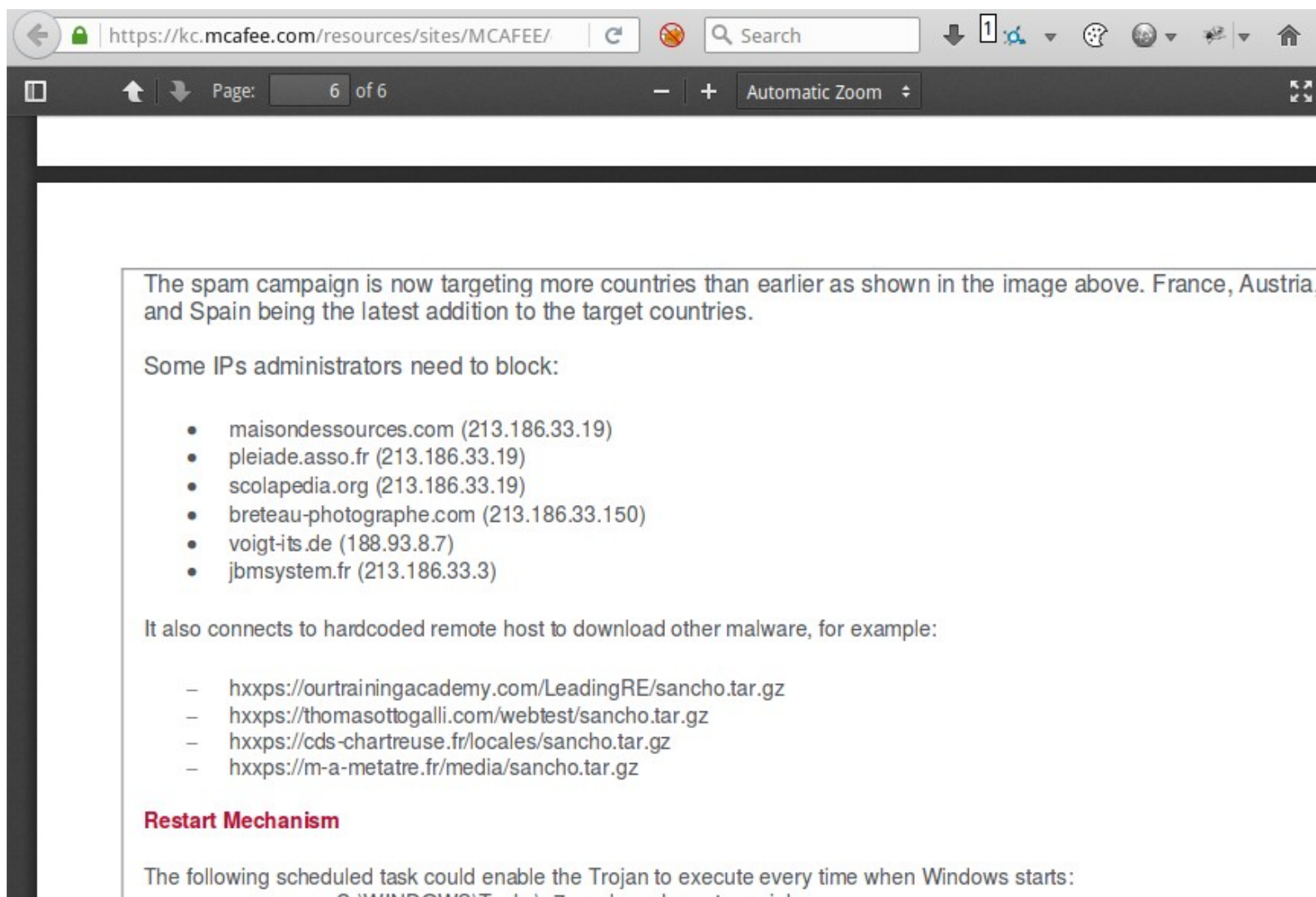
#####
## Domain feed of known DGA domains from -2 to +3 days
##
## Feed generated at: Mon Jan 25 00:15:01 UTC 2016
##
## Feed Provided By: John Bambenek of Bambenek Consulting
## jcb@bambenekconsulting.com // http://bambenekconsulting.com
##
## Use of this feed is governed by the license here:
## http://osint.bambenekconsulting.com/license.txt
## For more information on this feed go to:
## http://osint.bambenekconsulting.com/manual/dga-feed.txt
##
#####
rmynennkoyldg.com,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
faxnvfjthywrh.net,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
snokpwwpgiug.biz,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
gbnkhorgigtjx.ru,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
tveipswfrhmag.org,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
hjdihksokhxoh.co.uk,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
uwtfbcfsojrn.info,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
iksfsfbblougf.com,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
vdjmsynjoyuyj.net,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
wfiyqhvhvgfs.biz,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
weyjeivvpgqj.ru,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
xgxxkapkiddwj.org,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
xmoheewerhvvx.co.uk,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
yonvkvqskehch.info,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
yneepnfqsosnf.com,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
apdsvfylletf.net,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
cukniunihij.biz,Domain used by Cryptolocker - Flashback DGA for 23 Jan 2016,2016-01-23,http://osint.bambenekconsulting.com/manual/cl.txt
```



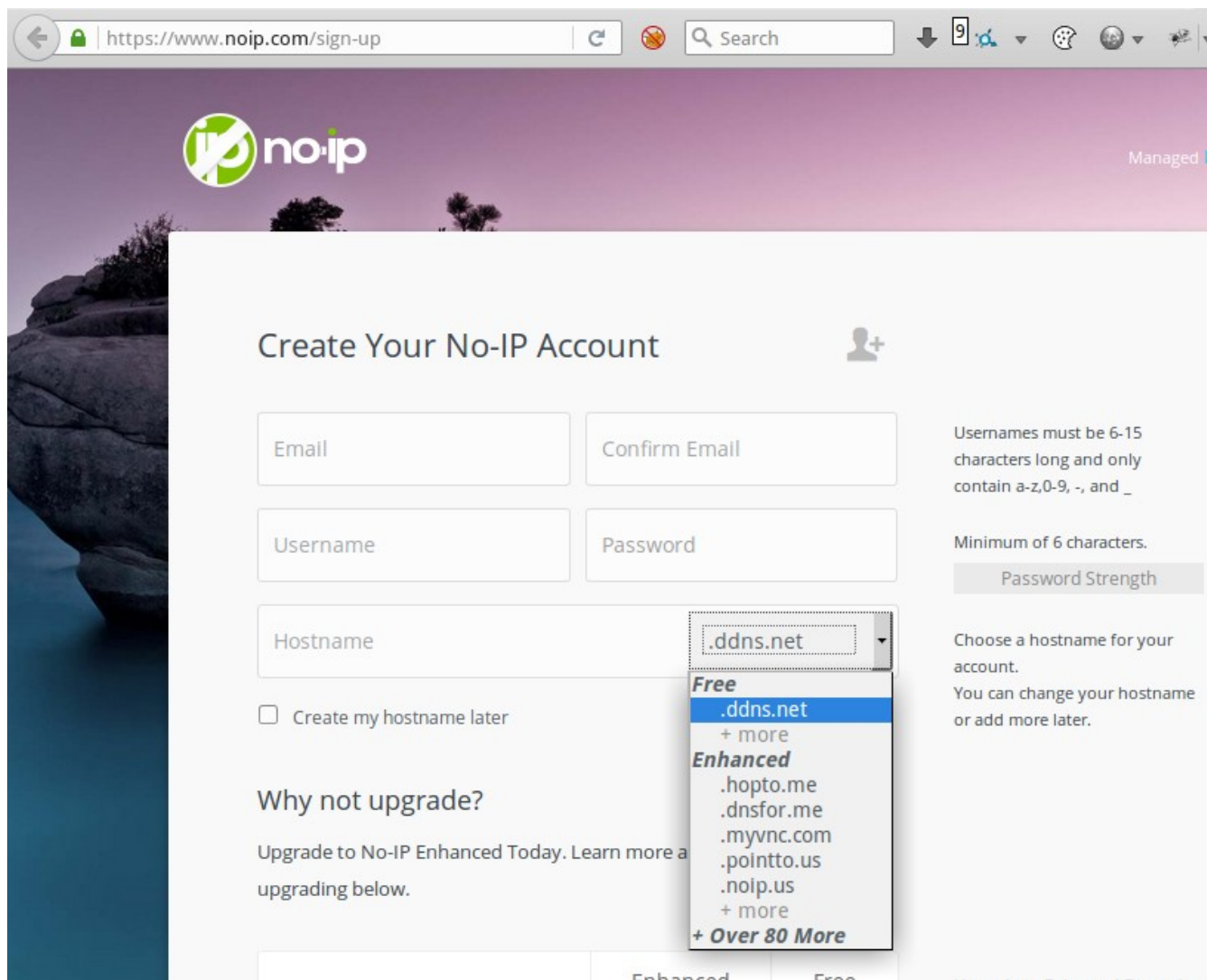
# Sinkhole server (example)

```
stamparm@Laptop:~/Dropbox/Work/maltrail$ curl -vv 192.42.119.41
* Rebuilt URL to: 192.42.119.41/
* Hostname was NOT found in DNS cache
*   Trying 192.42.119.41...
* Connected to 192.42.119.41 (192.42.119.41) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 192.42.119.41
> Accept: */*
>
< HTTP/1.1 200 OK
< X-Sinkhole: Malware sinkhole
< Content-Type: text/html
* Server nginx/0.7.65 is not blacklisted
< Server: nginx/0.7.65
< Date: Mon, 25 Jan 2016 20:39:30 GMT
< Content-Length: 0
<
* Connection #0 to host 192.42.119.41 left intact
```

# AV report(s) IOCs (example)



# Suspicious trails (example)



The screenshot shows the No-IP sign-up page in a web browser. The browser's address bar displays `https://www.noip.com/sign-up`. The page features the No-IP logo and a "Create Your No-IP Account" heading. The registration form includes fields for Email, Confirm Email, Username, Password, and Hostname. A dropdown menu is open for the Hostname field, showing options like `.ddns.net`, `.hopto.me`, `.dnsfor.me`, `.myvnc.com`, `.pointto.us`, `.noip.us`, and `+ Over 80 More`. To the right of the form, there are instructions: "Usernames must be 6-15 characters long and only contain a-z, 0-9, -, and \_", "Minimum of 6 characters.", and "Choose a hostname for your account. You can change your hostname or add more later."

Create Your No-IP Account

Email Confirm Email

Username Password

Hostname

☐ Create my hostname later

**Why not upgrade?**

Upgrade to No-IP Enhanced Today. Learn more about upgrading below.

Usernames must be 6-15 characters long and only contain a-z, 0-9, -, and \_

Minimum of 6 characters.

Password Strength

Choose a hostname for your account. You can change your hostname or add more later.

**Free**

- `.ddns.net`
- + more

**Enhanced**

- `.hopto.me`
- `.dnsfor.me`
- `.myvnc.com`
- `.pointto.us`
- `.noip.us`
- + more

**+ Over 80 More**

# Heuristic mechanisms (example)

```
sensor.py (Editing) X
if len(parts) > 2:
    part = parts[0] if parts[0] != "www" else parts[1]
    trail = "(%s).%s" % ('.'.join(parts[:-2]), '.'.join(parts[-2:]))
elif len(parts) == 2:
    part = parts[0]
    trail = "(%s).%s" % (parts[0], parts[1])
else:
    part = query
    trail = query

result = _result_cache.get(part)

if part:
    if result is None:
        # Reference: https://github.com/exp0se/dga_detector
        probabilities = (float(part.count(c)) / len(part) for c in set(_ for _ in part))
        entropy = -sum(p * math.log(p) / math.log(2.0) for p in probabilities)
        if entropy > SUSPICIOUS_DOMAIN_ENTROPY_THRESHOLD:
            result = "entropy threshold no such domain (suspicious)"

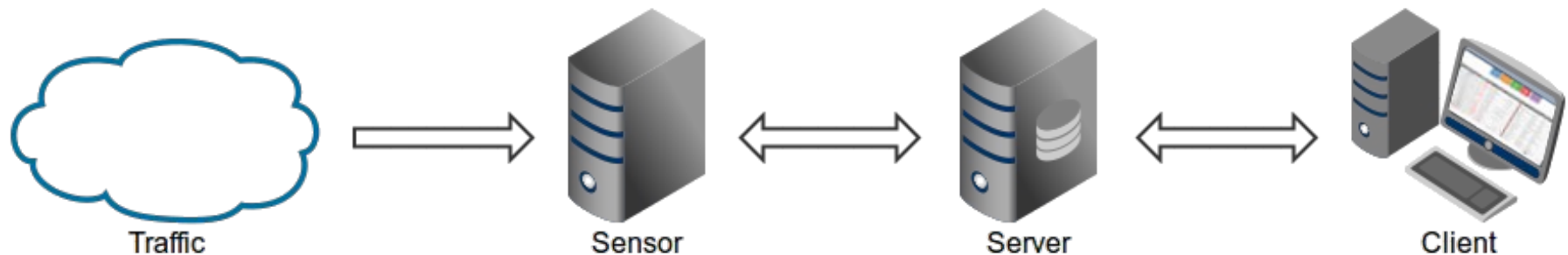
        if not result:
            consonants = re.findall("(?i)[bcdfghjklmnpqrstvwxyz]", part)
            if len(consonants) > SUSPICIOUS_DOMAIN_CONSONANT_THRESHOLD:
                result = "consonant threshold no such domain (suspicious)"

        _result_cache[part] = result or False

if result:
    log_event((sec, usec, src_ip, src_port, dst_ip, dst_port, PROTO.UDP, TRAIL.DNS, trail, result, "(heuristic)"), packet)
```

# Architecture

- **Sensor** component for traffic monitoring in search for “trails” (i.e. blacklisted features)
- **Server** component for log storage of (sensor) triggered events in form of CSV and serving on demand for further (client) analysis
- **Client** component for further analysis and reporting of raw log data



# Configuration

```
maltrail.conf (Editing) X
# [Server]

# Listen address of (reporting) HTTP server
HTTP_ADDRESS 0.0.0.0

# Listen port of (reporting) HTTP server
HTTP_PORT 8338

# Use SSL/TLS
USE_SSL false

# SSL/TLS (private/cert) PEM file (e.g. openssl req -new -x509 -keyout server.pem -out server.pem -days 1023 -nodes)
#SSL_PEM misc/server.pem

# User entries (username:sha256(password):UID:filter_netmask(s))
# Note(s): UID >= 1000 have only rights to display results
#           filter_netmask(s) is/are used to filter results
USERS
  admin:9ab3cd9d67bf49d01f6a2e33d0bd9bc804ddbe6ce1ff5d219c42624851db5dbc:0:0.0.0.0/0 # changeme!

# Listen address of (log collecting) UDP server
#UDP_ADDRESS 0.0.0.0

# Listen port of (log collecting) UDP server
#UDP_PORT 8337

# Should server do the trail updates too (to support UPDATE_SERVER)
USE_SERVER_UPDATE_TRAILS false

# [Sensor]

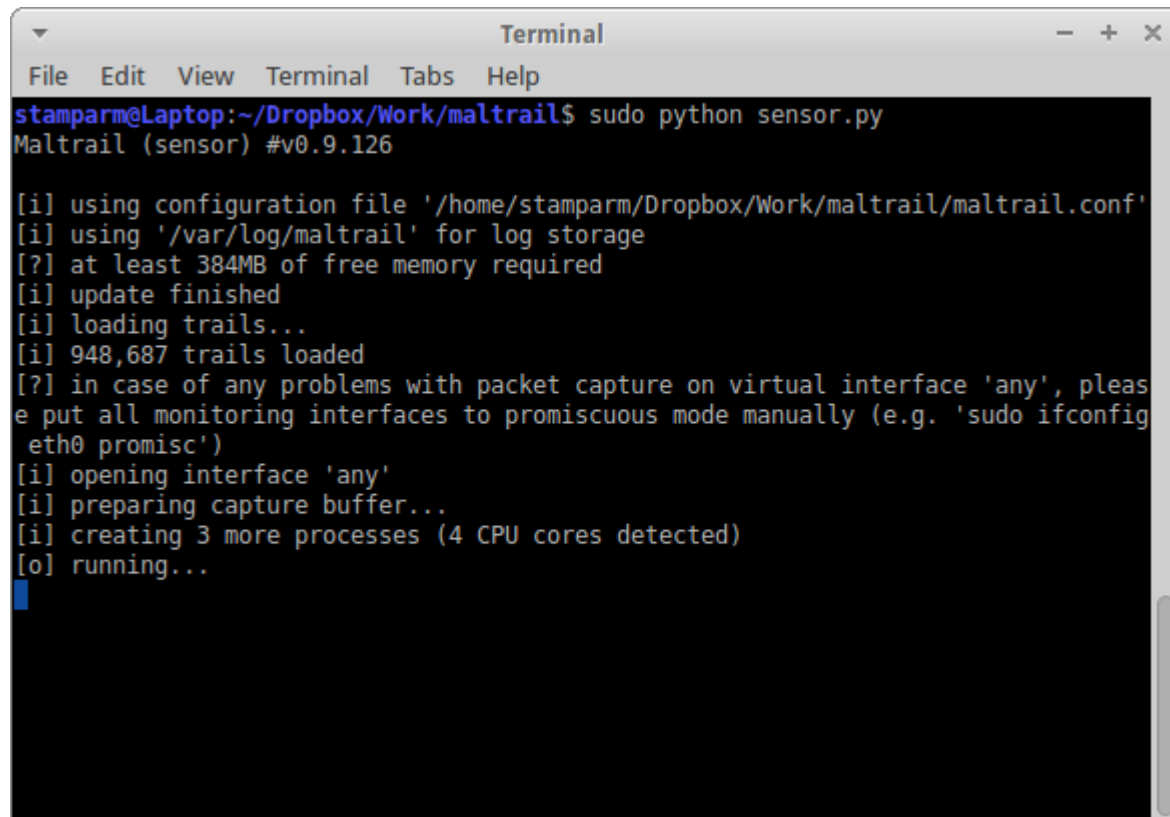
# Use multiprocessing (if possible)
USE_MULTIPROCESSING true

# Use feeds (too) in trail updates
USE_FEED_UPDATES true

# Update trails after every given period (seconds)
UPDATE_PERIOD 60
```

# Sensor (run)

- Python (2.6.x or 2.7.x)
- Pcapy (e.g. `sudo apt-get install python-pcap`)

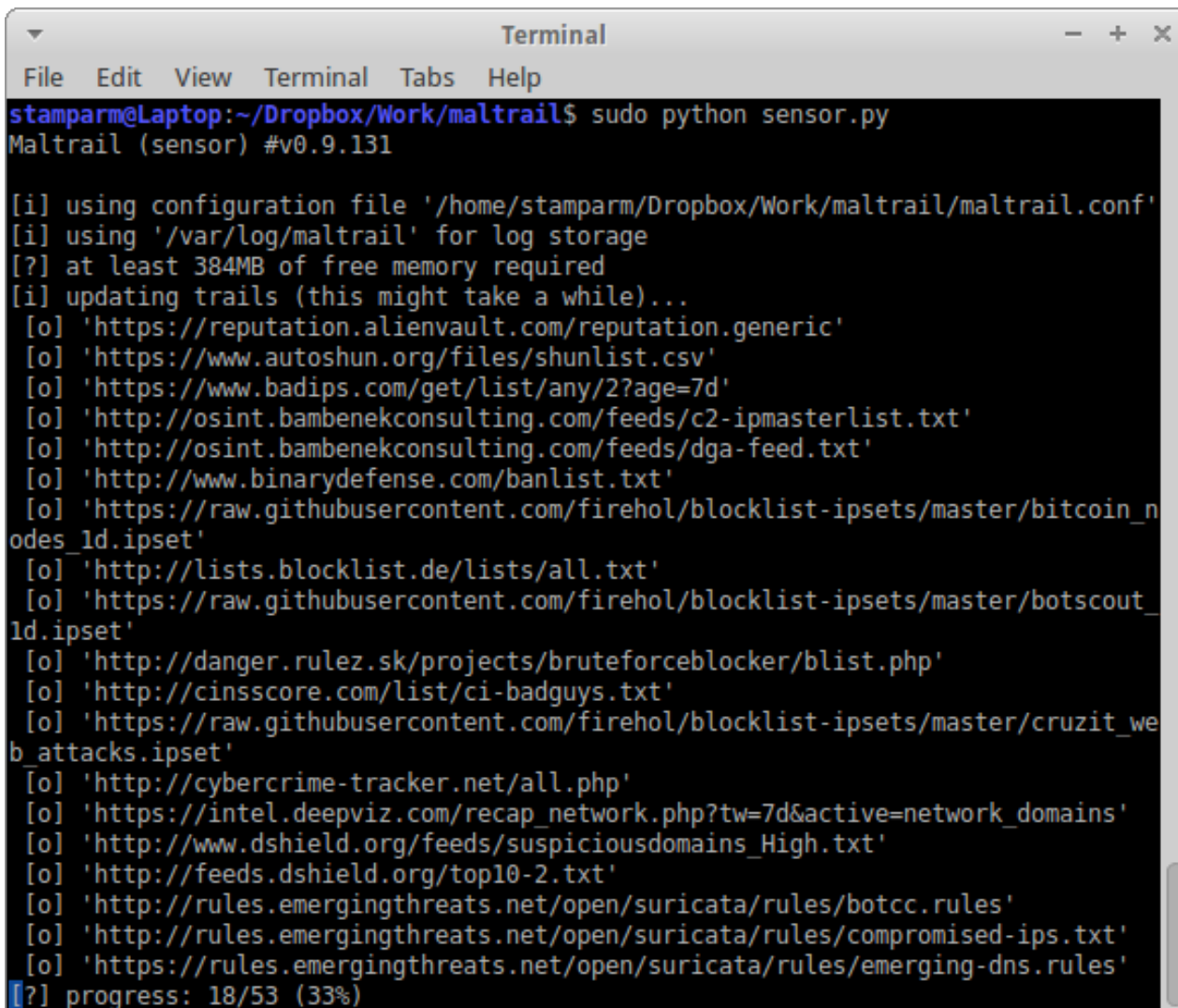


```
Terminal
File Edit View Terminal Tabs Help
stamparm@Laptop:~/Dropbox/Work/maltrail$ sudo python sensor.py
Maltrail (sensor) #v0.9.126

[i] using configuration file '/home/stamparm/Dropbox/Work/maltrail/maltrail.conf'
[i] using '/var/log/maltrail' for log storage
[?] at least 384MB of free memory required
[i] update finished
[i] loading trails...
[i] 948,687 trails loaded
[?] in case of any problems with packet capture on virtual interface 'any', please put all monitoring interfaces to promiscuous mode manually (e.g. 'sudo ifconfig eth0 promisc')
[i] opening interface 'any'
[i] preparing capture buffer...
[i] creating 3 more processes (4 CPU cores detected)
[o] running...
```



# Sensor (update)



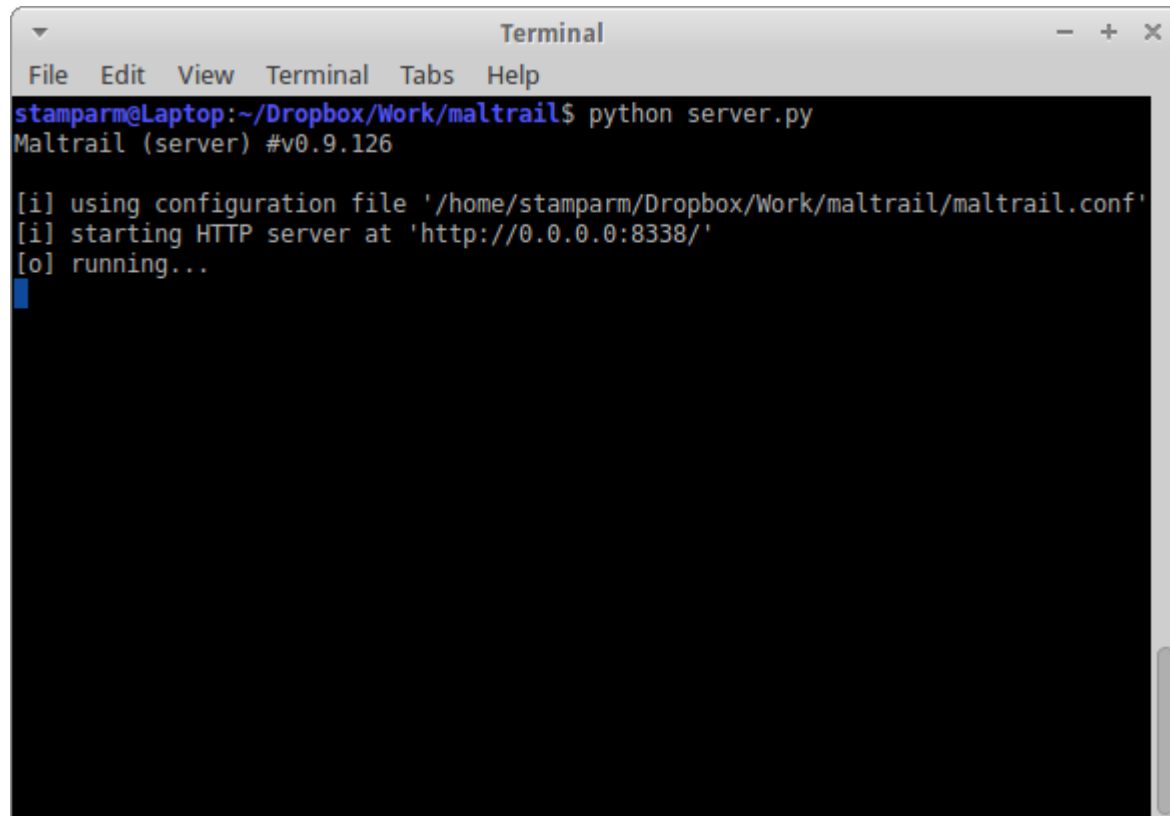
```
Terminal
File Edit View Terminal Tabs Help
stamparm@Laptop:~/Dropbox/Work/maltrail$ sudo python sensor.py
Maltrail (sensor) #v0.9.131

[i] using configuration file '/home/stamparm/Dropbox/Work/maltrail/maltrail.conf'
[i] using '/var/log/maltrail' for log storage
[?] at least 384MB of free memory required
[i] updating trails (this might take a while)...
[o] 'https://reputation.alienvault.com/reputation.generic'
[o] 'https://www.autoshun.org/files/shunlist.csv'
[o] 'https://www.badips.com/get/list/any/2?age=7d'
[o] 'http://osint.bambenekconsulting.com/feeds/c2-ipmasterlist.txt'
[o] 'http://osint.bambenekconsulting.com/feeds/dga-feed.txt'
[o] 'http://www.binarydefense.com/banlist.txt'
[o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/bitcoin_n
odes_1d.ipset'
[o] 'http://lists.blocklist.de/lists/all.txt'
[o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/botscout_
1d.ipset'
[o] 'http://danger.rulez.sk/projects/bruteforceblocker/blist.php'
[o] 'http://cinsscore.com/list/ci-badguys.txt'
[o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/cruzit_we
b_attacks.ipset'
[o] 'http://cybercrime-tracker.net/all.php'
[o] 'https://intel.deepviz.com/recap_network.php?tw=7d&active=network_domains'
[o] 'http://www.dshield.org/feeds/suspiciousdomains_High.txt'
[o] 'http://feeds.dshield.org/top10-2.txt'
[o] 'http://rules.emergingthreats.net/open/suricata/rules/botcc.rules'
[o] 'http://rules.emergingthreats.net/open/suricata/rules/compromised-ips.txt'
[o] 'https://rules.emergingthreats.net/open/suricata/rules/emerging-dns.rules'
[?] progress: 18/53 (33%)
```



# Server (run)

- Python (2.6.x or 2.7.x)

A screenshot of a terminal window titled "Terminal" with standard window controls (minimize, maximize, close). The terminal shows the command "python server.py" being executed from the directory "~/Dropbox/Work/maltrail". The output indicates that Maltrail (server) #v0.9.126 is using a configuration file at "/home/stamparm/Dropbox/Work/maltrail/maltrail.conf", starting an HTTP server at "http://0.0.0.0:8338/", and is now running. A blue cursor is visible on the line following the output.

```
Terminal
File Edit View Terminal Tabs Help
stamparm@Laptop:~/Dropbox/Work/maltrail$ python server.py
Maltrail (server) #v0.9.126

[i] using configuration file '/home/stamparm/Dropbox/Work/maltrail/maltrail.conf'
[i] starting HTTP server at 'http://0.0.0.0:8338/'
[o] running...
█
```

# Server (log storage)

```
Terminal
File Edit View Terminal Tabs Help
stamparm@Laptop:~/var/log/maltrail$ head -20 2016-01-21.log
"2016-01-21 00:00:00.002587" blitvenica 175.6.228.149 37333 1521 TCP IP 175.6.228.149 "bad reputat
ion" "alienvault.com (+blocklist.de,cinsscore.com,greensnow.co)"
"2016-01-21 00:00:00.207441" blitvenica 185.130.5.224 40710 53413 UDP IP 185.130.5.224 "known attac
ker" "badips.com (+cruzit.com,emergingthreats.net,greensnow.co,openbl.org,rulez.sk)"
"2016-01-21 00:00:00.656163" blitvenica 185.130.5.224 41309 53413 UDP IP 185.130.5.224 "known atta
cker" "badips.com (+cruzit.com,emergingthreats.net,greensnow.co,openbl.org,rulez.sk)"
"2016-01-21 00:00:00.753330" blitvenica 185.130.5.224 58322 53413 UDP IP 185.130.5.224 "known atta
cker" "badips.com (+cruzit.com,emergingthreats.net,greensnow.co,openbl.org,rulez.sk)"
"2016-01-21 00:00:00.753324" blitvenica 185.130.5.224 58322 53413 UDP IP 185.130.5.224 "known atta
cker" "badips.com (+cruzit.com,emergingthreats.net,greensnow.co,openbl.org,rulez.sk)"
"2016-01-21 00:00:00.778409" blitvenica 185.130.5.224 59779 53413 UDP IP 185.130.5.224 "known attac
ker" "badips.com (+cruzit.com,emergingthreats.net,greensnow.co,openbl.org,rulez.sk)"
"2016-01-21 00:00:01.002715" blitvenica 175.6.228.149 37333 1521 TCP IP 175.6.228.149 "bad reputat
ion" "alienvault.com (+blocklist.de,cinsscore.com,greensnow.co)"
"2016-01-21 00:00:01.303074" blitvenica 53482 54.231.50.44 80 TCP IP 54.231.50.44 "malware distrib
ution" malc0de.com
"2016-01-21 00:00:01.438555" blitvenica 51.255.65.22 41309 80 TCP IP 51.255.65.22 spammer botscout.c
om
"2016-01-21 00:00:01.885076" blitvenica 53482 54.231.50.44 80 TCP IP "54.231.50.44 (s3.amazonaws.c
om)" "malware distribution" malc0de.com
"2016-01-21 00:00:01.999955" blitvenica 175.6.228.149 37333 1521 TCP IP 175.6.228.149 "bad reputat
ion" "alienvault.com (+blocklist.de,cinsscore.com,greensnow.co)"
"2016-01-21 00:00:02.012652" blitvenica 53504 54.231.50.44 80 TCP IP 54.231.50.44 "malware distrib
ution" malc0de.com
"2016-01-21 00:00:02.166869" blitvenica 53504 54.231.50.44 80 TCP IP "54.231.50.44 (s3.amazonaws.c
om)" "malware distribution" malc0de.com
"2016-01-21 00:00:02.213851" blitvenica 223.215.30.156 3924 25 TCP IP 223.215.30.156 "bad reputati
on" snort.org
"2016-01-21 00:00:02.549213" blitvenica 125.64.93.78 41967 22 TCP IP 125.64.93.78 "known attacker"
"badips.com (+blocklist.de)"
"2016-01-21 00:00:02.820134" blitvenica 185.130.5.224 32838 53413 UDP IP 185.130.5.224 "known attac
ker" "badips.com (+cruzit.com,emergingthreats.net,greensnow.co,openbl.org,rulez.sk)"
"2016-01-21 00:00:02.925960" blitvenica 48962 8.8.8.8 53 UDP DNS (176ac04372ab418385fd2e679c5817f0
.51.3.63588931202944.updates).vidcreek.tv "long domain (suspicious)" (heuristic)
```

# Client

- Modern web browser (IE, Chrome, Firefox, etc.)
- HTML/JS (heavy usage of JavaScript – fat client)

maltrail 2016-01-20 (a day ago) Documentation | Issues | Log Out (cert)

6,945 Threats 903,708 Events medium Severity 4,498 Sources 6,402 Trails

25 threats per page Filter Q Clear Print Tools

threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
419cfec5	blitvenica	33288	low	20th 00:00:04	20th 23:59:59		175.6.228.149				TCP	IP	175.6.228.149	bad reputation	allenvault.com +3	
ba483ca0	blitvenica	4	low	20th 18:04:40	20th 23:59:59		51.255.65.22			80 (http)	TCP	IP	51.255.65.22	spammer	botscout.com	
faa569ca	blitvenica	1111	low	20th 00:00:02	20th 23:59:58		71.6.158.166					IP	71.6.158.166	bad reputation	allenvault.com	
785399cd	blitvenica	3939	low	20th 00:00:03	20th 23:59:58		71.6.135.131					IP	71.6.135.131	mass scanner	(static) +3	
cf308719	blitvenica	2808	low	20th 00:00:32	20th 23:59:58		222.186.21.34			22 (ssh)	TCP	IP	222.186.21.34	known attacker	autossh.org +3	
e11b7a7a	blitvenica	127	medium	20th 03:16:13	20th 23:59:58				54.231.50.44		TCP	IP	54.231.50.44 (s3.amazonaws.com)	malware distribution	malc0de.com	
d2923bd5	blitvenica	403	low	20th 23:40:34	20th 23:59:58		125.64.93.78			22 (ssh)	TCP	IP	125.64.93.78	known attacker	badips.com +1	
08031c3b	blitvenica	30298	low	20th 00:00:00	20th 23:59:57		185.130.5.224			53413 (netis)	UDP	IP	185.130.5.224	known attacker	badips.com +6	
e1603084	blitvenica	21	low	20th 01:46:09	20th 23:59:57		91.200.12.106			80 (http)	TCP	IP	91.200.12.106	known attacker	blocklist.de +2	
4b185819	blitvenica	137	medium	20th 03:24:55	20th 23:59:57			53 (dns)			UDP	DNS	info	consonant threshold no such domain (suspicious)	(heuristic)	
aeb2ba46	blitvenica	7082	low	20th 00:00:32	20th 23:59:55		198.20.99.130					IP	198.20.99.130	mass scanner	(static) +1	
9ef1ca13	blitvenica	2837	low	20th 00:00:50	20th 23:59:55		94.102.48.195	43905			TCP	IP	94.102.48.195	bad reputation	allenvault.com +3	
a996e144	blitvenica	627	low	20th 08:37:38	20th 23:59:54		141.212.122.194				TCP	IP	141.212.122.194	mass scanner	(static)	
f18c67d5	blitvenica	564	low	20th 08:39:29	20th 23:59:54		141.212.122.193				TCP	IP	141.212.122.193	mass scanner	(static) +2	
975cac1d	blitvenica	55	medium	20th 01:07:21	20th 23:59:53				8.8.8.8	53 (dns)	UDP	DNS	.sx	domain (suspicious)	(static)	
01b94405	blitvenica	801	low	20th 08:45:14	20th 23:59:53		141.212.122.207				TCP	IP	141.212.122.207	mass scanner	(static)	
7a84b346	blitvenica	413	low	20th 09:05:22	20th 23:59:53		141.212.122.206				TCP	IP	141.212.122.206	mass scanner	(static) +2	
4fcfd17d	blitvenica	4828	low	20th 00:00:10	20th 23:59:50		149.202.238.216			8080 (http-alt)	TCP	IP	149.202.238.216	bad reputation	allenvault.com +1	
de7d3a3c	blitvenica	101	low	20th 00:03:52	20th 23:59:50		141.212.121.40			443 (https)	TCP	IP	141.212.121.40	mass scanner	(static)	
8d8b2642	blitvenica	3999	low	20th 00:00:05	20th 23:59:49		71.6.165.200					IP	71.6.165.200	mass scanner	(static) +3	
07420f9f	blitvenica	967	low	20th 00:00:45	20th 23:59:49		82.221.105.7					IP	82.221.105.7	mass scanner	(static) +2	
db858271	blitvenica	5	medium	20th 07:04:43	20th 23:59:49		8.8.8.8	53 (dns)			UDP	DNS	amsnrelojy.ru	excessive no such domain (suspicious)	(heuristic)	
569aba30	blitvenica	1	low	20th 23:59:48	20th 23:59:48		67.21.35.231	43025		53 (dns)	UDP	IP	67.21.35.231	http spammer	sblam.com	
81e04040	blitvenica	1875	low	20th 00:00:04	20th 23:59:47		188.138.17.205					IP	188.138.17.205	bad reputation	allenvault.com	
2cc6e6d8	blitvenica	43	medium	20th 00:21:23	20th 23:59:47		8.8.8.8	53 (dns)			UDP	DNS	.eease.com	excessive no such domain (suspicious)	(heuristic)	

Showing 1 to 25 of 6,945 threats

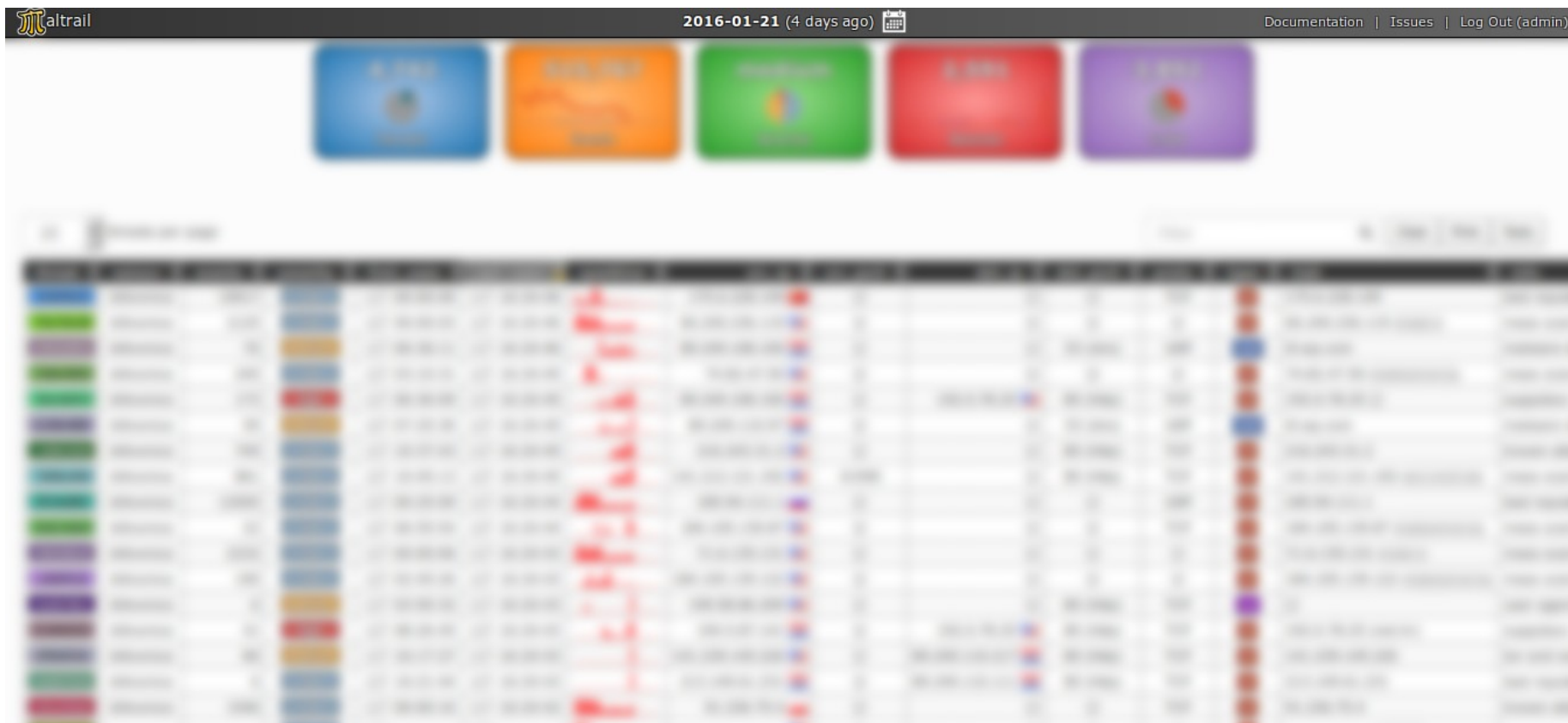
Previous 1 2 3 4 5 ... 278 Next

# Client (authentication)

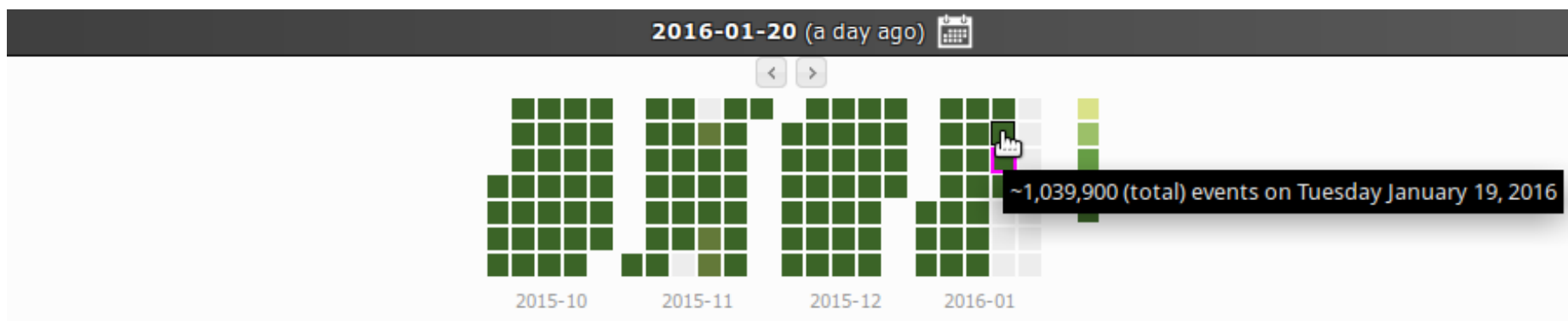
The screenshot displays the Altrail web application interface. At the top, the browser address bar shows 'localhost:8338'. The Altrail logo is on the left, and the date '2016-01-25 (today)' is in the center. On the right, there are links for 'Documentation', 'Issues', and 'Log In'. Below the header, there are five large colored buttons: 'Threats' (blue), 'Events' (orange), 'Severity' (green), 'Sources' (red), and 'Trails' (purple). Each button has a small minus icon at the top. Below these buttons, there is a '25 threats per page' dropdown menu and a 'Filter' search bar with 'Clear', 'Print', and 'Tools' buttons. A table header is visible with columns: 'threat', 'sensor', 'events', 'severity', 'first\_seen', 'last\_seen', 'sparkline', 'src\_ip', 'src\_port', 'dst\_ip', 'dst\_port', 'proto', 'type', and 'tr'. The table content shows 'No matching threats found'. Below the table, it says 'Showing 0 to 0 of 0 total threats'. An 'Authentication' dialog box is open in the center, containing 'Username:' and 'Password:' input fields, and 'Cancel' and 'Log In' buttons. 'Previous' and 'Next' buttons are also visible on the right side of the table area.

# Client (header)

- Timeline, documentation, issues, log in/out



# Client (timeline)





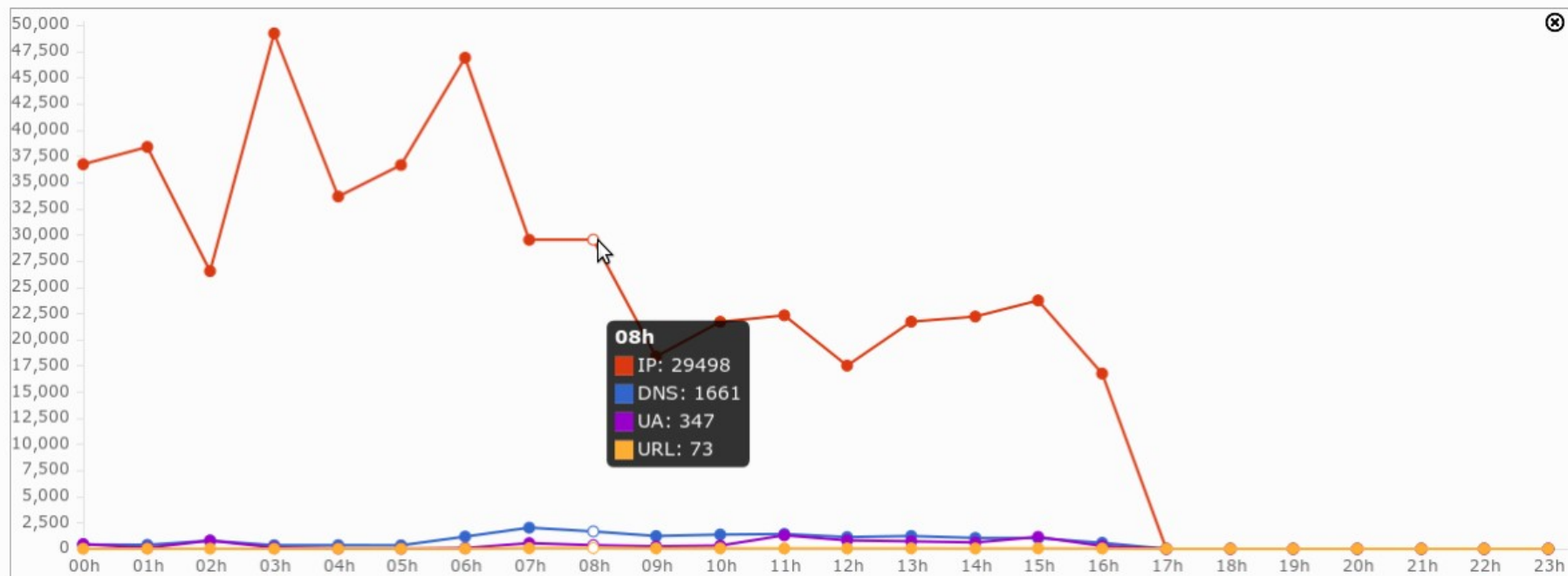
# Client (status buttons)

- Threats, events, severity, sources, trails



The image shows a blurred screenshot of a data table. The table has multiple columns and rows, with some cells containing red text. The table is likely a list of threats or events, as indicated by the context of the slide.






# Client (status graphs)
















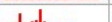





# Client (details table)

## ■ Details for each (detected) threat

25 threats per page

Filter

threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info
419cfec5	blitvenica	19017	low	21 <sup>st</sup> 00:00:00	21 <sup>st</sup> 16:24:46		175.6.228.149				TCP	IP	175.6.228.149	bad reputa
75e70a38	blitvenica	2125	low	21 <sup>st</sup> 00:00:03	21 <sup>st</sup> 16:24:46		66.240.236.119					IP	66.240.236.119 shodan.io	mass scanr
946e8db4	blitvenica	76	medium	21 <sup>st</sup> 06:36:11	21 <sup>st</sup> 16:24:46					53 (dns)	UDP	DNS	i0.wp.com	malware di
73be4992	blitvenica	245	low	21 <sup>st</sup> 03:10:31	21 <sup>st</sup> 16:24:45		74.82.47.50					IP	74.82.47.50 shadowserver.org	mass scanr
46ee8d44	blitvenica	173	high	21 <sup>st</sup> 06:36:09	21 <sup>st</sup> 16:24:45				192.0.78.25	80 (http)	TCP	IP	192.0.78.25	suppobox (
a19bcd86	blitvenica	59	medium	21 <sup>st</sup> 07:25:30	21 <sup>st</sup> 16:24:45					53 (dns)	UDP	DNS	i0.wp.com	malware di
12661925	blitvenica	749	low	21 <sup>st</sup> 10:37:43	21 <sup>st</sup> 16:24:45		216.243.31.2			80 (http)	TCP	IP	216.243.31.2	known atta
79dbe500	blitvenica	861	low	21 <sup>st</sup> 10:45:13	21 <sup>st</sup> 16:24:45		141.212.121.192	41590		80 (http)	TCP	IP	141.212.121.192 eecs.umich.edu	mass scanr
2fc4ad82	blitvenica	12505	low	21 <sup>st</sup> 00:25:09	21 <sup>st</sup> 16:24:44		185.94.111.1				UDP	IP	185.94.111.1	bad reputa
63d14de0	blitvenica	22	low	21 <sup>st</sup> 06:55:54	21 <sup>st</sup> 16:24:44		184.105.139.87				TCP	IP	184.105.139.87 shadowserver.org	mass scanr
785399cd	blitvenica	2232	low	21 <sup>st</sup> 00:00:06	21 <sup>st</sup> 16:24:43		71.6.135.131					IP	71.6.135.131 shodan.io	mass scanr
c386fb26	blitvenica	190	low	21 <sup>st</sup> 02:45:26	21 <sup>st</sup> 16:24:43		184.105.139.122					IP	184.105.139.122 shadowserver.org	mass scanr
3e097851	blitvenica	6	medium	21 <sup>st</sup> 03:50:32	21 <sup>st</sup> 16:24:43		199.58.86.209			80 (http)	TCP	UA		user agent
b1809554	blitvenica	41	high	21 <sup>st</sup> 08:26:45	21 <sup>st</sup> 16:24:43				192.0.78.25	80 (http)	TCP	IP	192.0.78.25 (net.hr)	suppobox (
afb0d34e	blitvenica	80	medium	21 <sup>st</sup> 16:17:27	21 <sup>st</sup> 16:24:43		141.239.145.226			80 (http)	TCP	IP	141.239.145.226	tor exit noc
4a9d7525	blitvenica	6	low	21 <sup>st</sup> 16:21:44	21 <sup>st</sup> 16:24:43					80 (http)	TCP	IP	213.149.61.231	bad reputa
c91e42a6	blitvenica	1546	low	21 <sup>st</sup> 00:00:16	21 <sup>st</sup> 16:24:42		91.236.75.4				TCP	IP	91.236.75.4	known atta

# Client (threat details)

threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port
946e8db4	blitvenica	76	medium	21 <sup>st</sup> 06:36:11	21 <sup>st</sup> 16:24:46		 	

src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
		53 (dns)	UDP	DNS	i0.wp.com	malware distribution	hosts-file.net	watchout

# Client (high severity threats)

25▼ threats per page

highClearPrintTools

threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
46ec8d44	blitvenica	173	high	21 <sup>st</sup> 06:36:09	21 <sup>st</sup> 16:24:45				192.0.78.25	80 (http)	TCP	IP	192.0.78.25	suppobox (malware)	bambenekconsulting.com	
b1809554	blitvenica	41	high	21 <sup>st</sup> 08:26:45	21 <sup>st</sup> 16:24:43				192.0.78.25	80 (http)	TCP	IP	192.0.78.25 (net.hr)	suppobox (malware)	bambenekconsulting.com	
d9d9ea6d	blitvenica	8064	high	21 <sup>st</sup> 00:01:52	21 <sup>st</sup> 16:24:42				192.0.78.25		TCP	IP	192.0.78.25	suppobox (malware)	bambenekconsulting.com	
b871a810	blitvenica	4790	high	21 <sup>st</sup> 06:43:56	21 <sup>st</sup> 16:24:40				192.0.78.25	80 (http)	TCP	IP	192.0.78.25	suppobox (malware)	bambenekconsulting.com	
3caad1e6	blitvenica	180	high	21 <sup>st</sup> 00:32:55	21 <sup>st</sup> 16:24:31				50.56.218.189	25 (smtp)	TCP	IP	50.56.218.189 rackspace	suppobox (malware)	bambenekconsulting.com	
f56cadcb	blitvenica	7800	high	21 <sup>st</sup> 00:00:50	21 <sup>st</sup> 16:24:28				192.0.78.24	80 (http)	TCP	IP	192.0.78.24	suppobox (malware)	bambenekconsulting.com	
113fe6de	blitvenica	313	high	21 <sup>st</sup> 08:04:41	21 <sup>st</sup> 16:24:21				192.0.78.24	80 (http)	TCP	IP	192.0.78.24	suppobox (malware)	bambenekconsulting.com	
afa98222	blitvenica	52	high	21 <sup>st</sup> 07:35:21	21 <sup>st</sup> 16:24:09				192.0.78.25	80 (http)	TCP	IP	192.0.78.25	suppobox (malware)	bambenekconsulting.com	
07d40810	blitvenica	896	high	21 <sup>st</sup> 00:49:25	21 <sup>st</sup> 16:24:08				192.0.78.24		TCP	IP	192.0.78.24	suppobox (malware)	bambenekconsulting.com	
fce21cd7	blitvenica	17	high	21 <sup>st</sup> 16:22:59	21 <sup>st</sup> 16:23:50				198.232.124.226	80 (http)	TCP	IP	198.232.124.226 (assets.croportal.net)	malware	malwaredomainlist.com	
d2517cf0	blitvenica	1163	high	21 <sup>st</sup> 00:01:11	21 <sup>st</sup> 16:23:46				192.0.78.24		TCP	IP	192.0.78.24	suppobox (malware)	bambenekconsulting.com	
03568b7c	blitvenica	1120	high	21 <sup>st</sup> 00:00:50	21 <sup>st</sup> 16:23:25				192.0.78.25		TCP	IP	192.0.78.25	suppobox (malware)	bambenekconsulting.com	
03d1cfde	blitvenica	97	high	21 <sup>st</sup> 08:08:49	21 <sup>st</sup> 16:23:25				213.186.33.16	80 (http)	TCP	IP	213.186.33.16 ovh	malware	malwaredomainlist.com +2	
11765bb0	blitvenica	854	high	21 <sup>st</sup> 01:08:43	21 <sup>st</sup> 16:23:10				5.9.18.114	80 (http)	TCP	IP	5.9.18.114 hetzner	simda (malware)	bambenekconsulting.com	
691cb083	blitvenica	1868	high	21 <sup>st</sup> 02:24:23	21 <sup>st</sup> 16:22:57				192.0.78.24	80 (http)	TCP	IP	192.0.78.24	suppobox (malware)	bambenekconsulting.com	
af79784e	blitvenica	1783	high	21 <sup>st</sup> 02:24:24	21 <sup>st</sup> 16:22:57				192.0.78.25	80 (http)	TCP	IP	192.0.78.25	suppobox (malware)	bambenekconsulting.com	
e1d606f0	blitvenica	680	high	21 <sup>st</sup> 06:58:56	21 <sup>st</sup> 16:22:07				192.0.78.24	80 (http)	TCP	IP	192.0.78.24	suppobox (malware)	bambenekconsulting.com	
0209725a	bliti	31886	91.199.77.50		80 (http)	TCP	IP	91.199.77.50		simda (malware)						
f74044ec	bliti															
fc37cd31	bliti	16588	72.52.4.90		80 (http)	TCP	IP	72.52.4.90		tinba (malware)						
4fbbd77a	bliti															
05575172	bliti	25249	8.8.8.8		53 (dns)	UDP	DNS	cfddtxywxvnm.com		tinba dga (malware)						
c0dbcc43	bliti															
2d517bdf	bliti	39051	8.8.8.8		53 (dns)	UDP	DNS	rkcrurk1bstr.com		tinba dga (malware)						
e611949d	bliti															
		25249	198.232.124.226		80 (http)	TCP	IP	198.232.124.226		malware						
		25249	5.9.18.114		25 (smtp)	TCP	IP	5.9.18.114 hetzner		simda (malware)						
		25249	192.0.78.24		80 (http)	TCP	IP	192.0.78.24		suppobox (malware)						
		25249	192.0.78.24		80 (http)	TCP	IP	192.0.78.24 (net.hr)		suppobox (malware)						
		25249	192.0.78.24		80 (http)	TCP	IP	192.0.78.24 (net.hr)		suppobox (malware)						
		25249	8.8.8.8		53 (dns)	UDP	DNS	.nk-slaven-belupo.hr		malware						
		25249	66.6.44.4		80 (http)	TCP	IP	66.6.44.4		suppobox (malware)						
		25249			25 (smtp)	TCP	IP	5.9.18.114 hetzner		simda (malware)						
		25249	213.186.33.5		80 (http)	TCP	IP	213.186.33.5 ovh		simda (malware)						
		25249	66.147.244.51		80 (http)	TCP	IP	66.147.244.51 (urbanfestival.blok.hr)		malware						

Showing 1 to 25 of 25 items

14Next



# Client (medium severity threats)

25 threats per page

medium

Clear

Print

Tools

threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
0c0a1e4f	blitvenica	17	medium	21 <sup>st</sup> 08:31:06	21 <sup>st</sup> 16:23:00					53 (dns)	UDP	DNS	d.agkn.com	malware distribution	hosts-file.net	
1f364b4c	blitvenica	63	medium	21 <sup>st</sup> 01:18:25	21 <sup>st</sup> 16:22:59				205.185.216.42	80 (http)	TCP	IP	205.185.216.42	malware distribution	malcode.com +1	
be416bc3	blitvenica	293	medium	21 <sup>st</sup> 00:10:48	21 <sup>st</sup> 16:22:56		8.8.4.4	53 (dns)			UDP	DNS	amnsreluoju.ru	excessive no such domain (suspicious)	(heuristic)	
b9a3932a	blitvenica	146	medium	21 <sup>st</sup> 00:38:59	21 <sup>st</sup> 16:22:52				8.8.8.8	53 (dns)	UDP	DNS	i0.wp.com	malware distribution	hosts-file.net	
8ccc3342	blitvenica	4	medium	21 <sup>st</sup> 08:55:16	21 <sup>st</sup> 16:22:51				8.8.8.8	53 (dns)	UDP	DNS	filesor.com	malware distribution	hosts-file.net	
53cc002e	blitvenica	1	medium	21 <sup>st</sup> 16:22:50	21 <sup>st</sup> 16:22:50			53 (dns)		58309	UDP	DNS	mullenfitzmaurice.com	consonant threshold no such domain (suspicious)	(heuristic)	
8afe3469	blitvenica	1	medium	21 <sup>st</sup> 16:22:50	21 <sup>st</sup> 16:22:50			32315	8.8.8.8	53 (dns)	UDP	DNS	ist1-1.filesor.com	malware distribution	hosts-file.net	
68942672	blitvenica	973	medium	21 <sup>st</sup> 06:48:42	21 <sup>st</sup> 16:22:45			53 (dns)			UDP	DNS	miz.hr	consonant threshold no such domain (suspicious)	(heuristic)	
3f73f227	blitvenica	219	medium	21 <sup>st</sup> 06:34:32	21 <sup>st</sup> 16:22:44				69.16.175.42	80 (http)	TCP	IP	69.16.175.42	malware distribution	malcode.com +1	
0f7b1f89	blitvenica	45	medium	21 <sup>st</sup> 00:03:49	21 <sup>st</sup> 16:22:42			53 (dns)			UDP	DNS	co.nz	consonant threshold no such domain (suspicious)	(heuristic)	
b04ae6b3	blitvenica	619	medium	21 <sup>st</sup> 06:48:31	21 <sup>st</sup> 16:22:39			53 (dns)			UDP	DNS	mzss.hr	consonant threshold no such domain (suspicious)	(heuristic)	
75137f32	blitvenica	75	medium	21 <sup>st</sup> 00:12:59	21 <sup>st</sup> 16:22:29				8.8.8.8	53 (dns)	UDP	DNS	(extensions).ftalkconnect.com	malware distribution	hosts-file.net	
1b0d3e8a	blitvenica	105	medium	21 <sup>st</sup> 05:11:07	21 <sup>st</sup> 16:22:23				8.8.8.8	53 (dns)	UDP	DNS	cdn.vicardf.com	malware distribution	hosts-file.net	
5327972e	blitvenica	45									UDP	DNS	.biz	consonant threshold no such domain (suspicious)	(heuristic)	
1ce0a875	blitvenica	102									UDP	DNS	.co.nz	consonant threshold no such domain (suspicious)	hosts-file.net	
0f403b5b	blitvenica	21									UDP	DNS	.ertelecom.ru	entropy threshold no such domain (suspicious)	(heuristic)	
275d7f82	blitvenica	24									UDP	DNS	.vidcreek.tv	entropy threshold no such domain (suspicious)	malcode.com +1	
5ff49ca8	blitvenica	34									UDP	DNS	.vidcreek.tv	long domain (suspicious)	(heuristic)	
0c095bd8	blitvenica	18									UDP	DNS	.vidcreek.tv	long domain (suspicious)	(static)	
3ef40722	blitvenica	181					8.8.8.8	53 (dns)			UDP	DNS	.vidcreek.tv	long domain (suspicious)	(static)	
989863f3	blitvenica	337						80 (http)			TCP	UA	Snoopy	user agent (suspicious)	(heuristic)	
263f43f1	blitvenica	380									TCP			user agent (suspicious)	(heuristic)	
f8fce5b8	blitvenica	50					8.8.8.8	53 (dns)			UDP	DNS	.pw	domain (suspicious)	(heuristic)	
c4a31e48	blitvenica	152									UDP	DNS	.vidcreek.tv	entropy threshold no such domain (suspicious)	malcode.com +1	
156f8ab	blitvenica	50									UDP	DNS	.vidcreek.tv	entropy threshold no such domain (suspicious)	malcode.com +1	
Showing 26 to 50 of 1,938 threats (filter)																
									443 (https)		TCP	IP	213.186.7.232	tor exit node (suspicious)		
							8.8.8.8	53 (dns)			UDP	DNS	.sx	domain (suspicious)		
							205.185.216.10	80 (http)			TCP	IP	205.185.216.10	malware distribution		
								80 (http)			TCP	DNS	.ws	domain (suspicious)		
											UDP	DNS	.biz	consonant threshold no such domain (suspicious)		
											UDP	DNS	.info	consonant threshold no such domain (suspicious)		
											UDP	DNS	.org	consonant threshold no such domain (suspicious)		
											UDP	DNS	.in	consonant threshold no such domain (suspicious)		
											UDP	DNS	i0.wp.com	malware distribution		
							8.8.8.8	53 (dns)			UDP	DNS	.jotzey.net	malware distribution		
											TCP	IP	83.110.195.146	malicious		

Showing 26 to 50 of 1,938 threats (filter)

2 3 4 5 ... 78 Next

# Client (low severity threats)

25

threats per page

low

Clear

Print









Tools

threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags									
419dfc5	blitvenica	19017	low	21 <sup>st</sup> 00:00:00	21 <sup>st</sup> 16:24:46		175.6.228.149				TCP	IP	175.6.228.149	bad reputation	alienvault.com +3										
75e70a38	blitvenica	2125	low	21 <sup>st</sup> 00:00:03	21 <sup>st</sup> 16:24:46		66.240.236.119					IP	66.240.236.119 shodan.io	mass scanner	(static) +6										
73bc4992	blitvenica	245	low	21 <sup>st</sup> 03:10:31	21 <sup>st</sup> 16:24:45		74.82.47.50					IP	74.82.47.50 shadowserver.org	mass scanner	(static) +1										
12661925	blitvenica	749	low	21 <sup>st</sup> 10:37:43	21 <sup>st</sup> 16:24:45		216.243.31.2			80 (http)	TCP	IP	216.243.31.2	known attacker	dshield.org										
79dbec500	blitvenica	861	low	21 <sup>st</sup> 10:45:13	21 <sup>st</sup> 16:24:45		141.212.121.192	41590		80 (http)	TCP	IP	141.212.121.192 eecs.umich.edu	mass scanner	(static)										
2fc4ad82	blitvenica	12505	low	21 <sup>st</sup> 00:25:09	21 <sup>st</sup> 16:24:44		185.94.111.1				UDP	IP	185.94.111.1	bad reputation	alienvault.com +2										
63d14de0	blitvenica	22	low	21 <sup>st</sup> 06:55:54	21 <sup>st</sup> 16:24:44		184.105.139.87				TCP	IP	184.105.139.87 shadowserver.org	mass scanner	(static) +1										
70539pcc	blitvenica	2232	low	21 <sup>st</sup> 00:00:06	21 <sup>st</sup> 16:24:43		71.6.135.131					IP	71.6.135.131 shodan.io	mass scanner	(static) +3										
c386fb26	blitvenica	190	low	21 <sup>st</sup> 02:45:26	21 <sup>st</sup> 16:24:43		184.105.139.122					IP	184.105.139.122 shadowserver.org	mass scanner	(static) +2										
4a9d7525	blitvenica	6	low	21 <sup>st</sup> 16:21:44	21 <sup>st</sup> 16:24:43		213.149.61.231		89.249.110.111	80 (http)	TCP	IP	213.149.61.231	bad reputation	snort.org										
c91c42a6	blitvenica	1546	low	21 <sup>st</sup> 00:00:16	21 <sup>st</sup> 16:24:42		91.236.75.4				TCP	IP	91.236.75.4	known attacker	dshield.org										
8d8b2642	blitvenica	2053	low	21 <sup>st</sup> 00:01:02	21 <sup>st</sup> 16:24:42		71.6.165.200					IP	71.6.165.200 shodan.io	mass scanner	(static) +3										
fb28b88c	blitvenica	281	low	21 <sup>st</sup> 11:25:59	21 <sup>st</sup> 16:24:42		169.38.65.251	27019			UDP	IP	169.38.65.251	bad reputation	alienvault.com										
f56c0ab1	blitvenica	262	low	21 <sup>st</sup> 00:01:09	21 <sup>st</sup> 16:24:41		129.82.138.44	-		-	ICMP	IP	129.82.138.44 netsec.colostate.edu	mass scanner	(static)										
57124026	blitvenica	253	low	21 <sup>st</sup> 00:02:31	21 <sup>st</sup> 16:24:41		146.185.239.102	65026			TCP	IP	146.185.239.102	bad reputation	alienvault.com										
46ec3a31	blitvenica	630	low	21 <sup>st</sup> 11:12:03	21 <sup>st</sup> 16:24:40		80.82.70.198			2404	TCP	IP	80.82.70.198	bad reputation	alienvault.com										
4d09da52	blitvenica	602	low	21 <sup>st</sup> 12:56:28	21 <sup>st</sup> 16:24:40		185.40.4.43	59678			UDP	IP	185.40.4.43 hostgrad	bad reputation	alienvault.com +2										
cbe030a0	blitvenica	387	low	21 <sup>st</sup> 02:12:41	21 <sup>st</sup> 16:24:39		216.218.206.87					IP	216.218.206.87 shadowserver.org	mass scanner	(static) +1										
cb17420d	blitvenica	3423	low																						
18c71f02	blitvenica	763	low					80 (http)			TCP	IP	216.243.31.2	known attacker	ult.com										
84aa5e73	blitvenica	127	low																						
22d510a3	blitvenica	3594	low					80 (http)			TCP	IP	141.212.121.192 eecs.umich.edu	mass scanner	+1										
076b5895	blitvenica	3520	low																						
72abdec1	blitvenica	73	low								UDP	IP	185.94.111.1	bad reputation	+3										
09930438	blitvenica	290	low								TCP	IP	184.105.139.87 shadowserver.org	mass scanner	+1										
Showing 1 to 25 of 2,475 threats (filtered from																		1	2	3	4	5	...	99	Next
												IP	71.6.135.131 shodan.io	mass scanner											
												IP	184.105.139.122 shadowserver.org	mass scanner											
								80 (http)			TCP	IP	213.149.61.231	bad reputation											
											TCP	IP	91.236.75.4	known attacker											
												IP	71.6.165.200 shodan.io	mass scanner											
											UDP	IP	169.38.65.251	bad reputation											
								-			ICMP	IP	129.82.138.44 netsec.colostate.edu	mass scanner											
											TCP	IP	146.185.239.102	bad reputation											
								2404			TCP	IP	80.82.70.198	bad reputation											
											UDP	IP	185.40.4.43 hostgrad	bad reputation											

# Client (detail condensed form)

			IP	66.240.236.119 shodan.io	mass scanner	(static) +6
	53 (doc)	UDP	dns	id.wg.com	malware distribution	hosts file.net
				7 (echo), 11 (sysstat), 13 (daytime), 15 (netstat), 17 (qotd), 19 (chargen), 21 (ftp), 22 (ssh), 23 (telnet), 25 (smtp), 26, 37 (time), 49 (tacacs), 53 (dns), 67 (bootps), 79 (finger), 80 (http), 81, 82, 83, 84, 88 (kerberos), 102 (iso-tsap), 110 (pop3), 111 (sunrpc), 119 (nntp), 123 (ntp), 129 (pwdgen), 137 (netbios-ns), 143 (imap2), 161 (snmp), 175, 179 (bgp), 195, 311, 389 (ldap), 443 (https), 444 (snpp), 445 (microsoft-ds), 465 (urd), 500 (isakmp), 502 (modbus), 503, 515 (printer), 520 (route), 523, 554 (rtsp), 587 (submission), 623 (ipmi), 626, 631 (ipp), 666, 771, 789, 873 (rsync), 902, 992 (telnets), 993 (imaps), 995 (pop3s), 1010, 1023, 1025, 1099 (rmiregistry), 1177, 1200, 1234, 1311, 1434 (ms-sql-m), 1471, 1604, 1723 (pptp), 1883, 1911, 1962, 1991, 2000 (cisco-sccp), 2067, 2082, 2083, 2086 (gnunet), 2087, 2123, 2152, 2222, 2323, 2332, 2375, 2376, 2404, 2455, 2480, 2628 (dict), 3000, 3128 (squid), 3306 (mysql), 3386, 3388, 3389 (rdesktop), 3460, 3541, 3542, 3689 (daap), 3749, 3780, 3784, 3790, 4000, 4022, 4040, 4063, 4064, 4369 (epmd), 4443, 4444, 4500 (ipsec-nat-t), 4567, 4848, 4911, 4949 (munin), 5000, 5001, 5006, 5007, 5008, 5009, 5060 (sip), 5094, 5222 (xmpp-client), 5269 (xmpp-server), 5353 (mdns), 5357 (wsdapi), 5432 (postgresql), 5555 (rplay), 5560, 5577, 5632, 5672 (amqp), 5901 (vnc-1), 5984, 5985, 5986, 6000 (x11), 6379 (redis), 6664, 6666, 6667 (ircd), 6881, 6969, 7071, 7218, 7474, 7547 (cwmp), 7548, 7657, 7777, 7779, 8000, 8010, 8060, 8069, 8080 (http-alt), 8081 (tproxy), 8086, 8087, 8089, 8090, 8098, 8099, 8112, 8139, 8140, 8181, 8333, 8334, 8443 (https-alt), 8554, 8649, 8834, 8880, 8888, 8889, 9000, 9001, 9002, 9051, 9080, 9100, 9151, 9160, 9191, 9200 (wap-wsp), 9443, 9595, 9600, 9943, 9944, 9981, 9999, 10000 (webmin), 10001, 10243, 11211 (memcached), 12345, 13579, 14147, 16010, 18245, 20000, 20547, 21025, 21379, 23023, 23424, 25105, 25565, 27015, 27017 (mongo), 28017, 30718, 32400, 32764, 37777, 44818, 47808, 49152, 49153, 50070, 50100, 51106, 55553, 55554, 62078, 64738		

# Client (reverse DNS and WHOIS)




src_ip	
185.40.4.48	
216.218.206.87	
	
	
180.97.106.36	
184.105.247.199	
	
	

**hosted-by.hostgrad.ru**  
inetnum: 185.40.4.0/24  
org: ORG-HL100-RIPE  
netname: Hostgrad  
descr: Hostgrad  
country: RU  
admin-c: EH3355-RIPE  
tech-c: EH3355-RIPE  
status: ASSIGNED PA  
mnt-by: HOSTGRAD-MNT  
created: 2015-07-03T11:55:45Z  
last-modified: 2015-07-03T11:55:45Z  
source: RIPE




# Client (trail dorking)

TCP	IP	168.62.238.153
💬	IP	68.116.5.134
💬	IP	68.116.5.134
TCP	IP	95.65.34.177
TCP	UA	M
UDP	DNS	utorrent.com
TCP	IP	93.174.93.218 e
TCP	IP	192.0.78.25 💬
TCP	IP	77.222.197.13
TCP	IP	213.186.33.16 o
💬	IP	46.166.186.236
UDP	DNS	net.mx
💬	IP	66.240.192.138



Answer | Images Videos

**cluster005.ovh.net**  
Owner: OVH SAS Shared Hosting Servers <http://www.ovh.com> (France)  
 More at RobTex

WHOIS - 213.186.33.16

Previous | 1 | 2 | 3 | **4** | 5 | ...



# Real-life cases (mass scans)

	216.243.31.2			80 (http)	TCP		216.243.31.2	known attacker
	141.212.121.192	41590		80 (http)	TCP		141.212.121.192 <a href="#">eecs.umich.edu</a>	mass scanner
	185.94.111.1				UDP		185.94.111.1	bad reputation
	184.105.139.87				TCP		184.105.139.87 <a href="#">shadowserver.org</a>	mass scanner
	71.6.135.131						71.6.135.131 <a href="#">shodan.io</a>	mass scanner
	184.105.139.122						184.105.139.122 <a href="#">shadowserver.org</a>	mass scanner
			192.0.78.25	80 (http)	TCP		192.0.78.25 <a href="#">suppobox</a>	suppobox (malware)
	141.239.145.226			80	80 (http), 123 (ntp), 443 (https), 9200 (wap-wsp), 11211 (memcached), 27017 (mongo)			e (suspicious)
				80				ion
	199.58.86.209			80 (http)	TCP		MJ12bot	user agent (suspicious)
	91.236.75.4				TCP		91.236.75.4	known attacker
	71.6.165.200						71.6.165.200 <a href="#">shodan.io</a>	mass scanner
			192.0.78.25		TCP		192.0.78.25	suppobox (malware)
	169.38.65.251	27019			UDP		169.38.65.251	bad reputation
	129.82.138.44	-		-	ICMP		129.82.138.44 <a href="#">netsec.colostate.edu</a>	mass scanner
	146.185.239.102	65026			TCP		146.185.239.102	bad reputation

# Real-life cases (known attackers)

	221.167.66.8 🇰🇷	🗨️	🗨️	23 (telnet)	TCP		221.167.66.8	known attacker	<a href="#">blocklist.de</a>
	91.201.236.113 🇲🇩	🗨️	🗨️	22 (ssh)	TCP		91.201.236.113	known attacker	<a href="#">badips.com</a> +4
	186.120.170.149 🇧🇪	🗨️		53 (dns)	UDP		186.120.170.149	known attacker	<a href="#">badips.com</a> +1
	203.156.121.22 🇷🇺	🗨️		25 (smtp)	TCP		203.156.121.22	known attacker	<a href="#">blocklist.de</a>
	216.195.72.27 🇺🇸	🗨️	🗨️	25 (smtp)	TCP		216.195.72.27	known attacker	<a href="#">blocklist.de</a>
	183.87.59.158 🇮🇳	41088		37370	UDP		183.87.59.158	known attacker	<a href="#">blocklist.de</a>
	106.38.216.210 🇨🇳	6413		21 (ftp)	TCP		106.38.216.210	known attacker	<a href="#">greensnow.co</a>
	50.23.96.210 🇺🇸	7499	🗨️	22 (ssh)	TCP		50.23.96.210 <small>softlayer</small>	known attacker	<a href="#">autoshun.org</a> +5
	155.133.82.40 🇨🇳	🗨️	🗨️	25 (smtp)	TCP		155.133.82.40	known attacker	<a href="#">blocklist.de</a> +1
	65.60.171.205 🇺🇸	🗨️		25 (smtp)	TCP		65.60.171.205	known attacker	<a href="#">blocklist.de</a>
		41736	157.56.52.45 🇺🇸	40016	UDP		157.56.52.45	known attacker	<a href="#">blocklist.de</a>
	83.15.99.121 🇨🇳	53916		53 (dns)	UDP		83.15.99.121	known attacker	<a href="#">badips.com</a> +1
	121.168.217.191 🇰🇷	58131		23 (telnet)	TCP		121.168.217.191	known attacker	<a href="#">greensnow.co</a>
	65.181.125.199 🇺🇸	47745		25 (smtp)	TCP		65.181.125.199	known attacker	<a href="#">blocklist.de</a>
	200.94.115.114 🇲🇩	🗨️	🗨️	🗨️	🗨️		200.94.115.114	known attacker	<a href="#">badips.com</a>
	59.31.159.20 🇰🇷	2221		23 (telnet)	TCP		59.31.159.20	known attacker	<a href="#">greensnow.co</a>
	118.175.13.246 🇷🇺	🗨️		22 (ssh)	TCP		118.175.13.246	known attacker	<a href="#">badips.com</a> +1
	189.112.42.157 🇧🇷	-	🗨️	-	ICMP		189.112.42.157	known attacker	<a href="#">greensnow.co</a>
	185.63.252.55 🇷🇺	🗨️	🗨️	53 (dns)	UDP		185.63.252.55	known attacker	<a href="#">cruzit.com</a>
	211.149.169.75 🇨🇳	🗨️	🗨️	25 (smtp)	TCP		211.149.169.75	known attacker	<a href="#">blocklist.de</a> +1
	83.12.0.246 🇨🇳	🗨️		25 (smtp)	TCP		83.12.0.246	known attacker	<a href="#">blocklist.de</a>
	64.94.1.143 🇺🇸	🗨️	🗨️	🗨️	UDP		64.94.1.143	known attacker	<a href="#">greensnow.co</a>

# Real-life cases (Tor)

		37370	46.166.188.206	8307	UDP		46.166.188.206 santrex	tor exit node (suspicious)
	5.196.1.129			80 (http)	TCP		5.196.1.129 ovh	tor exit node (suspicious)
	197.231.221.211				TCP		197.231.221.211	tor exit node (suspicious)
	142.4.206.84	37655		23165	TCP		142.4.206.84 ovh	tor exit node (suspicious)
	77.247.181.162				TCP		77.247.181.162	tor exit node (suspicious)
	77.247.181.165				TCP		77.247.181.165	tor exit node (suspicious)
	78.46.220.130			443	80 (http), 443 (https)		78.46.220.130 hetzner	tor exit node (suspicious)
			109.201.154.201				109.201.154.201	tor exit node (suspicious)
		49994	144.76.185.42	80 (http)	TCP		144.76.185.42 hetzner	tor exit node (suspicious)
				443 (https)	TCP		212.92.219.15	tor exit node (suspicious)
	185.60.144.31			80 (http)	TCP		185.60.144.31	tor exit node (suspicious)
			46.166.190.176	23605			46.166.190.176 santrex	tor exit node (suspicious)
	46.183.222.171				TCP		46.183.222.171	tor exit node (suspicious)
	176.10.104.243				TCP		176.10.104.243	tor exit node (suspicious)
	193.90.12.87				TCP		193.90.12.87	tor exit node (suspicious)
	37.59.47.27				UDP		37.59.47.27 ovh	tor exit node (suspicious)
	171.25.193.131				TCP		171.25.193.131	tor exit node (suspicious)
	84.19.190.106			80 (http)	TCP		84.19.190.106	tor exit node (suspicious)
	193.90.12.86				TCP		193.90.12.86	tor exit node (suspicious)

# Real-life cases (service attackers)

	123.252.166.79			3389 (rdesktop)	TCP		123.252.166.79	bad reputation
	93.126.34.162	4935		3389 (rdesktop)	TCP		93.126.34.162	known attacker
	71.42.131.94			3389 (rdesktop)	TCP		71.42.131.94	bad reputation
	190.100.136.205	4935		3389 (rdesktop)	TCP		190.100.136.205	bad reputation
	89.248.172.98	11022		3389 (rdesktop)	TCP		89.248.172.98	bad reputation
	198.74.113.189	4935		3389 (rdesktop)	TCP		198.74.113.189	bad reputation
	115.111.114.249			3389 (rdesktop)	TCP		115.111.114.249	bad reputation
	50.240.184.154			3389 (rdesktop)	TCP		50.240.184.154	bad reputation
	173.11.128.1	4935		3389 (rdesktop)	TCP		173.11.128.1	known attacker
	212.179.227.181			3389 (rdesktop)	TCP		212.179.227.181	bad reputation
	124.219.3.65			3389 (rdesktop)	TCP		124.219.3.65	bad reputation
	200.42.62.100	4935		3389 (rdesktop)	TCP		200.42.62.100	bad reputation
	125.209.97.62	4935		3389 (rdesktop)	TCP		125.209.97.62	bad reputation
	200.47.55.2			3389 (rdesktop)	TCP		200.47.55.2	bad reputation
	164.39.47.244			3389 (rdesktop)	TCP		164.39.47.244	bad reputation
	1.34.4.54	4935		3389 (rdesktop)	TCP		1.34.4.54	bad reputation
	222.81.23.34			3389 (rdesktop)	TCP		222.81.23.34	bad reputation
	89.212.7.18			3389 (rdesktop)	TCP		89.212.7.18	known attacker
	219.141.248.222			3389 (rdesktop)	TCP		219.141.248.222	known attacker
	212.181.5.109	4935		3389 (rdesktop)	TCP		212.181.5.109	bad reputation
	113.189.226.198	59197		3389 (rdesktop)	TCP		113.189.226.198	known attacker



# Real-life cases (known DGA)

			8.8.8.8	53 (dns)	UDP			tinba dga (malware)
			8.8.8.8	53 (dns)	UDP		counter.yadro.ru	zeroaccess (malware)
<div>b410n0l2k4j3a.cc, bdfehmqrstcps.com, btwjyfooplju.com, cfddtxywxvnm.com, diuyeeloptdk.com, djhifghxltif.com, eeotkktlxkpw.com, fdiykspxbeee.com, fedlixcgvlgw.com, fnrjmmbccxul.com, fqpyiuwgwgnb.com, hefjgghbrddw.com, heknbuuxhxdd.com, hgwwwqmnmpsp.com, ihgunmevihtb.com, iunrcxddomfs.com, jiqfgcbevkjq.com, jixxuvuexcmv.com, jjeejrbsteyi.com, jybrspkjyphc.com, nvbdmneewtuf.com, nvgchhhxhmlo.com, oognqnoxdeyv.com, rkcrurklbstr.com, skxokuxpqrjq.com, ulpmrcfxssk.com, upvbhcofiqqm.com, uyqponmmotts.com, vwwwnkrkxphx.com, vwiuiuxyufih.com, wkhlkqwlidgd.com, ynbjwnvuteju.com, yuexdyngcuyi.com, yyckjwlweqmd.com</div>								
			192.0.78.24	80 (http)	TCP		192.0.78.24	suppobox (malware)
				53 (dns)	UDP		pica.banjalucke-ljepotice.ru	palevo (malware)
			213.186.33.2	80 (http)	TCP		213.186.33.2  ovh	malware
			192.0.78.25	80 (http)	TCP		192.0.78.25 (net.hr)	suppobox (malware)
			198.232.124.226	80 (http)	TCP		198.232.124.226	malware

# Real-life cases (unknown DGA)

				443 (https)	TCP		212.92.219.15	tor exit node (suspicious)
			69.16.175.10	80 (http)	TCP		69.16.175.10	malware distribution
		53 (dns)			UDP		.biz	consonant threshold no such domain (suspicious)
		53 (dns)	80.240.110.241		UDP		.co.nz	consonant threshold no such domain (suspicious)
	cknnqwksv, drnffefbxzs, dttibyhkny, fltsnphki, hdfbygaofdkd, jxzqyqxm, ksselpgfyxv, mktpkgwci, ndfpwkr, nrcpwuzpti, nrfdtmgqbfe, nunhtcxryr, snddxhyrc, uhwvecfyy, vbmcvsspf, wtpkflcc, wzaiqlfbokb, xhqwrmtm, zcgsistfrqx						ertelecom.ru	entropy threshold no such domain (suspicious)
							vidcreek.tv	long domain (suspicious)
							shoopy	user agent (suspicious)
			8.8.8.8	53 (dns)	UDP		.pw	domain (suspicious)
	8.8.8.8	53 (dns)			UDP		.vidcreek.tv	entropy threshold no such domain (suspicious)
				443 (https)	TCP		213.186.7.232	tor exit node (suspicious)
			8.8.8.8	53 (dns)	UDP		.sx	domain (suspicious)
			205.185.216.10	80 (http)	TCP		205.185.216.10	malware distribution
				80 (http)	TCP		.ws	domain (suspicious)
			104.18.42.146	80 (http)	TCP			user agent (suspicious)
		53 (dns)			UDP		.biz	consonant threshold no such domain (suspicious)
		53 (dns)			UDP		.info	consonant threshold no such domain (suspicious)
		53 (dns)			UDP		.org	consonant threshold no such domain (suspicious)
		53 (dns)			UDP		.in	consonant threshold no such domain (suspicious)

# Real-life cases (known malware)

ramnit

Q

Clear

Print

Tools



sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	
			209.99.40.223	80 (http)	TCP		209.99.40.223 <a href="#">data</a>	ramnit (malware)	
			209.99.40.222	80 (http)	TCP		209.99.40.222 <a href="#">data</a>	ramnit (malware)	
			30397	209.99.40.222	80 (http)	TCP		209.99.40.222 (www.mcorner.net) <a href="#">data</a>	ramnit (malware)
				209.99.40.222	80 (http)	TCP		209.99.40.222 (www.bullstuff.net) <a href="#">data</a>	ramnit (malware)
			56691	209.99.40.222	80 (http)	TCP		209.99.40.222 <a href="#">data</a>	ramnit (malware)

Previous

1

Next

# Real-life cases (ipinfo)

				8.8.8.8 	53 (dns)	UDP		checkip.dyndns.org	ipinfo (suspicious)
					53 (dns)	UDP		checkip.dyndns.org	ipinfo (suspicious)
					53 (dns)	UDP		 .whatismyip.com	ipinfo (suspicious)
					53 (dns)	UDP		 .getmyip.org	ipinfo (suspicious)
					53 (dns)	UDP		ipinfo.io	ipinfo (suspicious)
				8.8.8.8 	53 (dns)	UDP		 .icanhazip.com	ipinfo (suspicious)
				8.8.8.8 	53 (dns)	UDP		ipinfo.io	ipinfo (suspicious)
				8.8.8.8 	53 (dns)	UDP		 .ip-adress.com	ipinfo (suspicious)
				8.8.8.8 	53 (dns)	UDP		ip-api.com	ipinfo (suspicious)
			19210	8.8.8.8 	53 (dns)	UDP		ip-api.com	ipinfo (suspicious)
			38587	8.8.8.8 	53 (dns)	UDP		 .ip-adress.com	ipinfo (suspicious)
				8.8.8.8 	53 (dns)	UDP		 .ipaddress.com	ipinfo (suspicious)
			23754		80 (http)	TCP		 .ipaddress.com	ipinfo (suspicious)
			56025		53 (dns)	UDP		ipinfo.io	ipinfo (suspicious)



# Real-life cases (dynamic domain)

						53 (dns)	UDP		.dyndns-ip.com	dynamic domain (suspicious)
						53 (dns)	UDP		.zaproto.org	dynamic domain (suspicious)
				8.8.8.8		53 (dns)	UDP		.dyndns.org	dynamic domain (suspicious)
						53 (dns)	UDP		.no-ip.biz	dynamic domain (suspicious)
				8.8.8.8		53 (dns)	UDP		.mine.nu	dynamic domain (suspicious)
			20151			53 (dns)	UDP		.dyndns.org	dynamic domain (suspicious)
			54273			53 (dns)	UDP		.no-ip.biz	dynamic domain (suspicious)
						53 (dns)	UDP		.no-ip.org	dynamic domain (suspicious)
			4346	8.8.8.8		53 (dns)	UDP		.mine.nu	dynamic domain (suspicious)
			19909	8.8.8.8		53 (dns)	UDP		madh0use8	dynamic domain (suspicious)
			16026	8.8.8.8		53 (dns)	UDP		.no-ip.org	dynamic domain (suspicious)
			37568	8.8.8.8		53 (dns)	UDP		.sytes.net	dynamic domain (suspicious)
			20587	8.8.8.8		53 (dns)	UDP		.dyndns.org	dynamic domain (suspicious)
			21362	8.8.8.8		53 (dns)	UDP		.servegame.com	dynamic domain (suspicious)
			21266	8.8.8.8		53 (dns)	UDP		.dynu.com	dynamic domain (suspicious)

# Real-life cases (Host:)

		53 (dns)			UDP		.122-airtelbroadband.in	consonant threshold no such domain (suspicious)
	188.138.1.218						188.138.1.218 plusserver.de	bad reputation
	216.218.206.110				TCP		216.218.206.110 shadowserver.org	mass scanner
			8.8.8.8	53 (dns)	UDP		search.mlstat.com	malware distribution
			190.119.255.182				190.119.255.182	proxy (suspicious)
			192.0.78.24	80 (http)	TCP		192.0.78.24	suppobox (malware)
				53 (dns)	UDP		(ham)er-dat.net	malware distribution

bakingwithsibella.com, net.hr, ninakuhinja.com, qpq.net.hr, tankandafvnews.com, www.net.hr

... 190 Next



























# Real-life cases (sqlmap)

224	medium	28 <sup>th</sup> 23:27:06	28 <sup>th</sup> 23:27:08			8000	TCP	UA	sqlmap	suspicious user agent	(heuristic)
207	medium	28 <sup>th</sup> 23:27:07	28 <sup>th</sup> 23:27:08			8000	TCP	URL	:8000	suspicious http request	(heuristic)
33	low	28 <sup>th</sup> 23:35:07	28 <sup>th</sup> 23:44:09							potential port scanning	(heuristic)

(POST) id=(SELECT (CASE WHEN (5999=4965) THEN 5999 ELSE 5999\*(SELECT 5999 FROM INFORMATION\_SCHEMA.CHARACTER\_SETS END)), (POST) id=(SELECT (CASE WHEN (7293=7293) THEN 7293 ELSE 7293\*(SELECT 7293 FROM INFORMATION\_SCHEMA.CHARACTER\_SETS END)), (POST) id=(SELECT (CHR(113)||CHR(122)||CHR(118)||CHR(112)||CHR(113)) ||(SELECT (CASE WHEN (3058=3058) THEN 1 ELSE 0 END))::text|| (CHR(113)||CHR(122)||CHR(113)||CHR(12 2)||CHR(113))), (POST) id=(SELECT 5269 FROM(SELECT COUNT(\*),CONCAT(0x717a767071, (SELECT (ELT(5269=5269,1))),0x717a717a71,FLOOR(RAND(0)\*2)) x FROM INFORMATION\_SCHEMA.CHARACTER\_SETS GROUP BY x)a), (POST) id=(SELECT CHAR(113)+CHAR(122)+CHAR(118)+CHAR(112)+CHAR(113)+ (SELECT (CASE WHEN (6592=6592) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(122)+CHAR(113)+CHAR(122)+CHAR (113)), (POST) id=1 AND (SELECT \* FROM (SELECT(SLEEP(5)))VMQv), (POST) id=1 AND (SELECT \* FROM (SELECT(SLEEP(5)))VMQv)-- NBeC, (POST) id=1 AND (SELECT 3650 FROM(SELECT COUNT(\*),CONCAT(0x717a767071,(SELECT (ELT(3650=3650,1))),0x717a717a71,FLOOR(RAND(0)\*2)) x FROM INFORMATION\_SCHEMA.CHARACTER\_SETS GROUP BY x)a), (POST) id=1 AND (SELECT 3650 FROM(SELECT COUNT(\*),CONCAT(0x717a767071,(SELECT

Previous 1 Next

# Real-life cases (direct .exe download)

185.65.135.227 			443 (https)	TCP		185.65.135.227	tor exit node (suspicious)
69.30.201.98 	57124		80 (http)	TCP			user agent (suspicious)
122.152.160.161 	61622		80 (http)	TCP		 .hr 	suspicious http request
151.20.106.172 	61424		80 (http)	TCP			user agent (suspicious)
			80 (http)	TCP		download.yourfileinfo.com 	direct .exe download (suspicious)
158.69.214.111 	51696		80 (http)	TCP		158.69.214.111 ovh 	tor exit node (suspicious)

Previous 1 ... 4 **5** 6 ... 2

/amnis  
/installer.exe

## Real-life cases (?)

[illegible]

# Questions?

