Maltrail

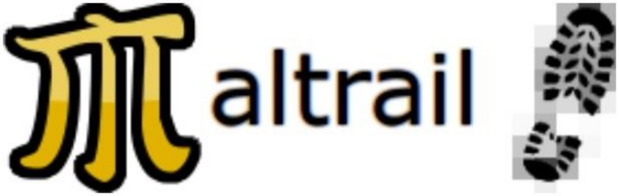
Information Security Inc.

Contents

- About Maltrail
- Testing Environment
- Blacklists utilized
- Architecture
- Installing Maltrail
- Running Maltrail
- References

About Maltrail

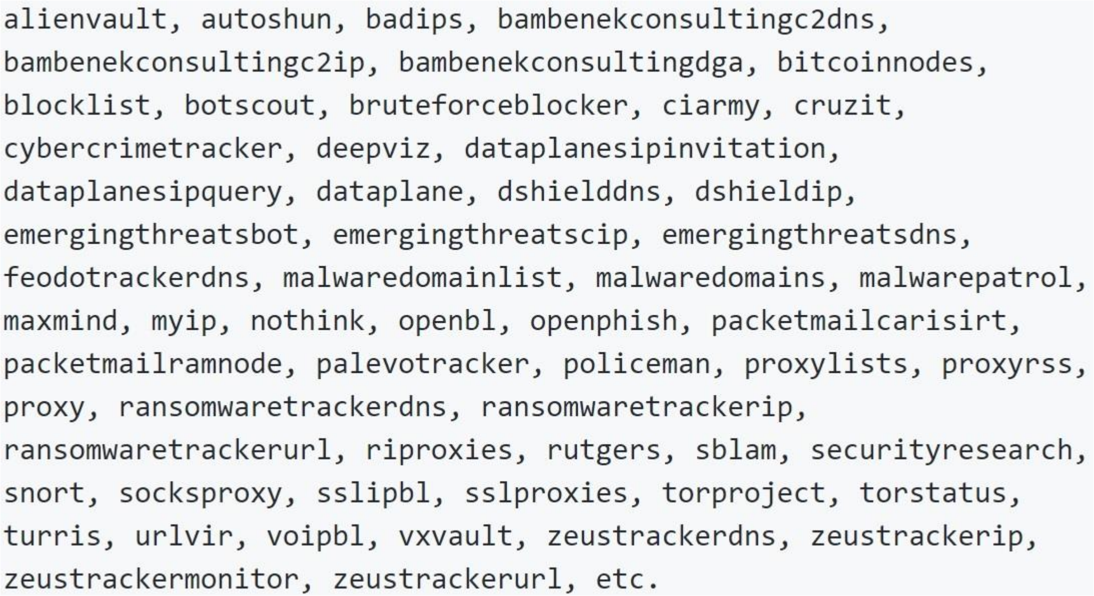
- Maltrail is a malicious traffic detection system, utilizing publicly available (black)lists containing malicious and/or generally suspicious trails, along with static trails compiled from various AV reports and custom user defined lists



About Maltrail

- Where trail can be anything from domain name (e.g. zvpprsensinaix.com for Banjori malware), URL (e.g. http://109.162.38.120/harsh02.exe for known malicious executable), IP address (e.g. 185.130.5.231 for known attacker) or HTTP User-Agent header value (e.g. sqlmap for automatic SQL injection and database takeover tool)

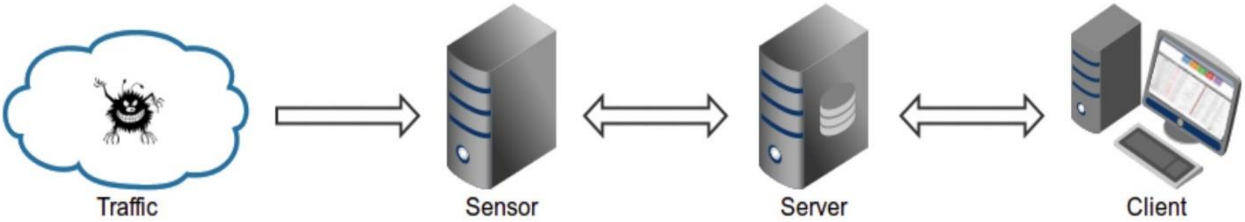
Blacklists utilized



```
alienvault, autoshun, badips, bambenekconsultingc2dns,
bambenekconsultingc2ip, bambenekconsultingdga, bitcoinnodes,
blocklist, botscout, bruteforceblocker, ciarmy, cruzit,
cybercrimetracker, deepviz, dataplanesipinvitation,
dataplanesipquery, dataplane, dshielddns, dshieldip,
emergingthreatsbot, emergingthreatscip, emergingthreatsdns,
feodotrackerdns, malwaredomainlist, malwaredomains, malwarepatrol,
maxmind, myip, nothink, openbl, openphish, packetmailcarisirt,
packetmailramnode, palevotracker, policeman, proxylists, proxyrss,
proxy, ransomwaretrackerdns, ransomwaretrackerip,
ransomwaretrackerurl, riproxies, rutgers, sblam, securityresearch,
snort, socksproxy, sslipbl, sslproxies, torproject, torstatus,
turris, urlvir, voipbl, vxvault, zeustrackerdns, zeustrackerip,
zeustrackermonitor, zeustrackerurl, etc.
```

Architecture

- Maltrail is based on the **Traffic** -> **Sensor** <-> **Server** <-> **Client** architecture

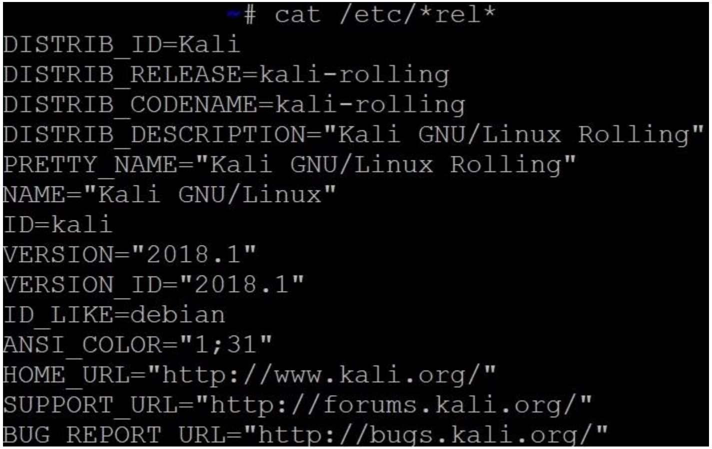


Architecture

- Sensor(s) is a standalone component running on the monitoring node (e.g. Linux platform connected passively to the SPAN/mirroring port or transparently inline on a Linux bridge) or at the standalone machine (e.g. Honeypot) where it "monitors" the passing Traffic for blacklisted items/trails
- **Server**'s primary role is to store the event details and provide back-end support for the reporting web application
- Events for the chosen period are transferred to the **Client**, where the reporting web application is solely responsible for the presentation part

Testing Environment

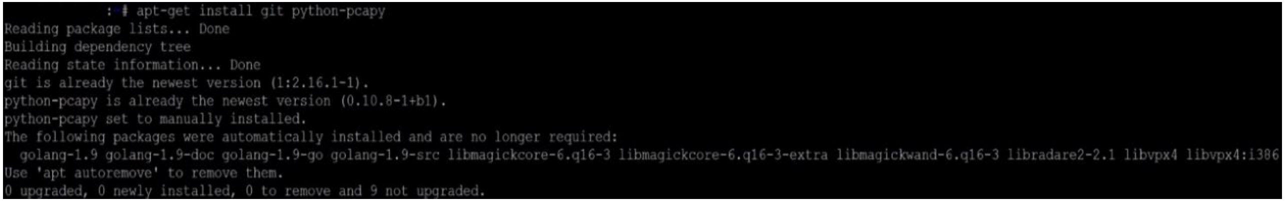
- Kali Linux 2018.1



```
~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2018.1"
VERSION_ID="2018.1"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing Maltrail

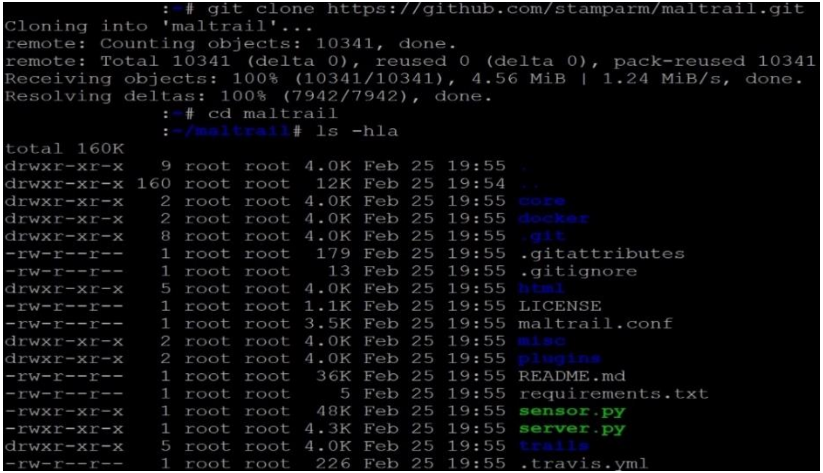
- apt-get install git python-pcapy



```
            :~# apt-get install git python-pcapy
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.16.1-1).
python-pcapy is already the newest version (0.10.8-1+b1).
python-pcapy set to manually installed.
The following packages were automatically installed and are no longer required:
  golang-1.9 golang-1.9-doc golang-1.9-go golang-1.9-src libmagickcore-6.q16-3 libmagickcore-6.q16-3-extra libmagickwand-6.q16-3 libradare2-2.1 libvpx4 libvpx4:i386
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
```

Installing Maltrail

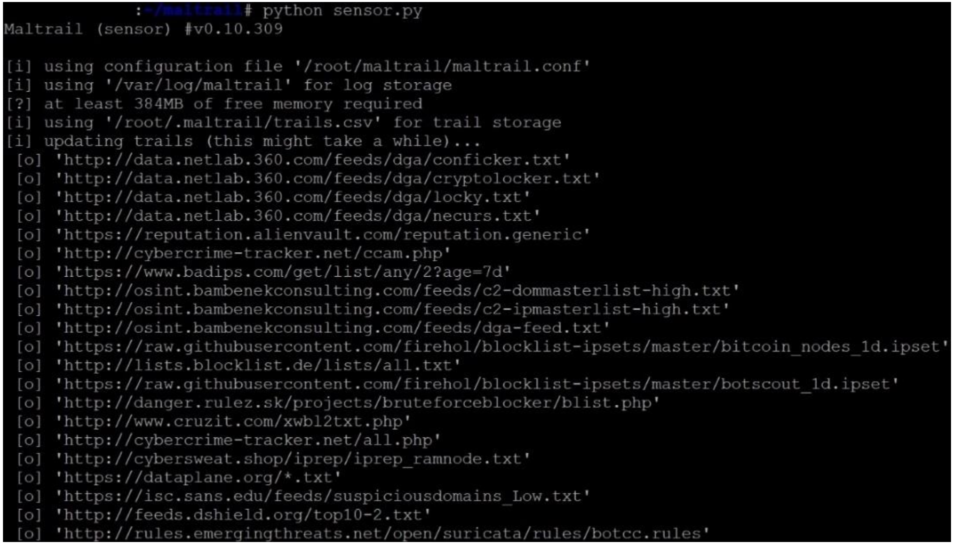
- git clone https://github.com/stamparm/maltrail.git



```
[redacted]:~# git clone https://github.com/stamparm/maltrail.git
Cloning into 'maltrail'...
remote: Counting objects: 10341, done.
remote: Total 10341 (delta 0), reused 0 (delta 0), pack-reused 10341
Receiving objects: 100% (10341/10341), 4.56 MiB | 1.24 MiB/s, done.
Resolving deltas: 100% (7942/7942), done.
[redacted]:~# cd maltrail
[redacted]:~/maltrail# ls -hla
total 160K
drwxr-xr-x   9 root root 4.0K Feb 25 19:55 .
drwxr-xr-x 160 root root  12K Feb 25 19:54 ..
drwxr-xr-x   2 root root 4.0K Feb 25 19:55 core
drwxr-xr-x   2 root root 4.0K Feb 25 19:55 docker
drwxr-xr-x   8 root root 4.0K Feb 25 19:55 .git
-rw-r--r--   1 root root  179 Feb 25 19:55 .gitattributes
-rw-r--r--   1 root root   13 Feb 25 19:55 .gitignore
drwxr-xr-x   5 root root 4.0K Feb 25 19:55 html
-rw-r--r--   1 root root 1.1K Feb 25 19:55 LICENSE
-rw-r--r--   1 root root 3.5K Feb 25 19:55 maltrail.conf
drwxr-xr-x   2 root root 4.0K Feb 25 19:55 misc
drwxr-xr-x   2 root root 4.0K Feb 25 19:55 plugins
-rw-r--r--   1 root root  36K Feb 25 19:55 README.md
-rw-r--r--   1 root root    5 Feb 25 19:55 requirements.txt
-rwxr-xr-x   1 root root  48K Feb 25 19:55 sensor.py
-rwxr-xr-x   1 root root 4.3K Feb 25 19:55 server.py
drwxr-xr-x   5 root root 4.0K Feb 25 19:55 trails
-rw-r--r--   1 root root  226 Feb 25 19:55 .travis.yml
```

Running Maltrail

- Starting the sensor

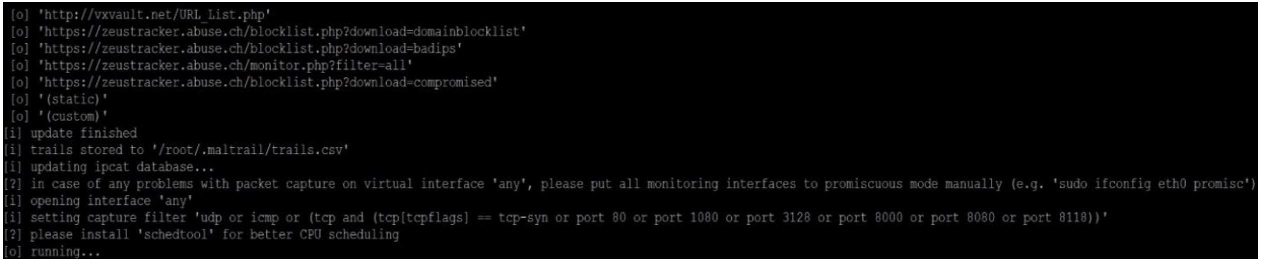


```
[redacted]:~/maltrail# python sensor.py
Maltrail (sensor) #v0.10.309

[i] using configuration file '/root/maltrail/maltrail.conf'
[i] using '/var/log/maltrail' for log storage
[?] at least 384MB of free memory required
[i] using '/root/.maltrail/trails.csv' for trail storage
[i] updating trails (this might take a while)...
 [o] 'http://data.netlab.360.com/feeds/dga/conficker.txt'
 [o] 'http://data.netlab.360.com/feeds/dga/cryptolocker.txt'
 [o] 'http://data.netlab.360.com/feeds/dga/locky.txt'
 [o] 'http://data.netlab.360.com/feeds/dga/necurs.txt'
 [o] 'https://reputation.alienvault.com/reputation.generic'
 [o] 'http://cybercrime-tracker.net/ccam.php'
 [o] 'https://www.badips.com/get/list/any/2?age=7d'
 [o] 'http://osint.bambenekconsulting.com/feeds/c2-dommasterlist-high.txt'
 [o] 'http://osint.bambenekconsulting.com/feeds/c2-ipmasterlist-high.txt'
 [o] 'http://osint.bambenekconsulting.com/feeds/dga-feed.txt'
 [o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/bitcoin_nodes_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://www.cruzit.com/xwbl2txt.php'
 [o] 'http://cybercrime-tracker.net/all.php'
 [o] 'http://cybersweat.shop/iprep/iprep_ramnode.txt'
 [o] 'https://dataplane.org/*.txt'
 [o] 'https://isc.sans.edu/feeds/suspiciousdomains_Low.txt'
 [o] 'http://feeds.dshield.org/top10-2.txt'
 [o] 'http://rules.emergingthreats.net/open/suricata/rules/botcc.rules'
```

Running Maltrail

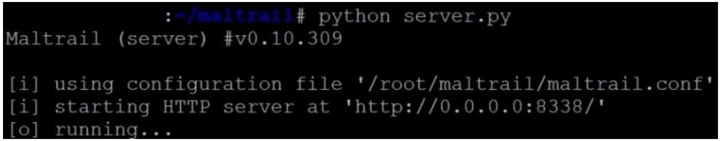
- Starting the sensor



```
 [o] 'http://vxvault.net/URL_List.php'
 [o] 'https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist'
 [o] 'https://zeustracker.abuse.ch/blocklist.php?download=badips'
 [o] 'https://zeustracker.abuse.ch/monitor.php?filter=all'
 [o] 'https://zeustracker.abuse.ch/blocklist.php?download=compromised'
 [o] '(static)'
 [o] '(custom)'
[i] update finished
[i] trails stored to '/root/.maltrail/trails.csv'
[i] updating ipcat database...
[?] 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] setting capture filter 'udp or icmp or (tcp and (tcp[tcpflags] == tcp-syn or port 80 or port 1080 or port 3128 or port 8000 or port 8080 or port 8118))'
[?] please install 'schedtool' for better CPU scheduling
[o] running...
```

Running Maltrail

- Starting the server

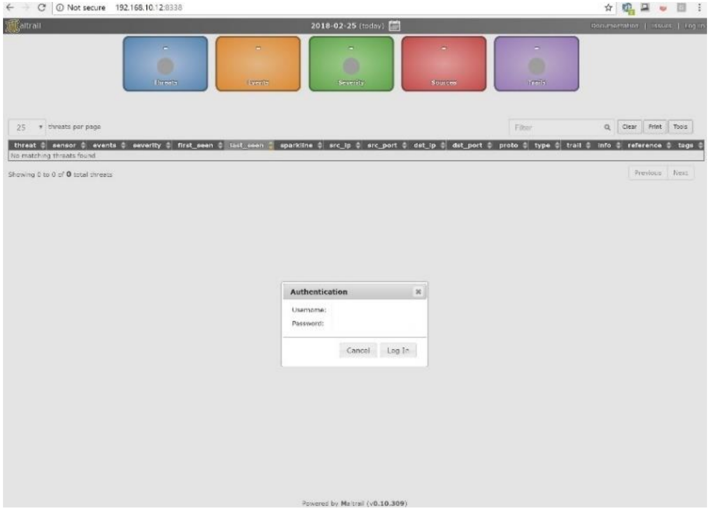


```
             :~/maltrail# python server.py
Maltrail (server) #v0.10.309

[i] using configuration file '/root/maltrail/maltrail.conf'
[i] starting HTTP server at 'http://0.0.0.0:8338/'
[o] running...
```

Running Maltrail

- Access the reporting interface (i.e. Client) by visiting the http://192.168.10.12:8338 (default credentials: admin:changeme!) from your web browser



threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
No matching threats found																

Showing 0 to 0 of **0** total threats

Authentication

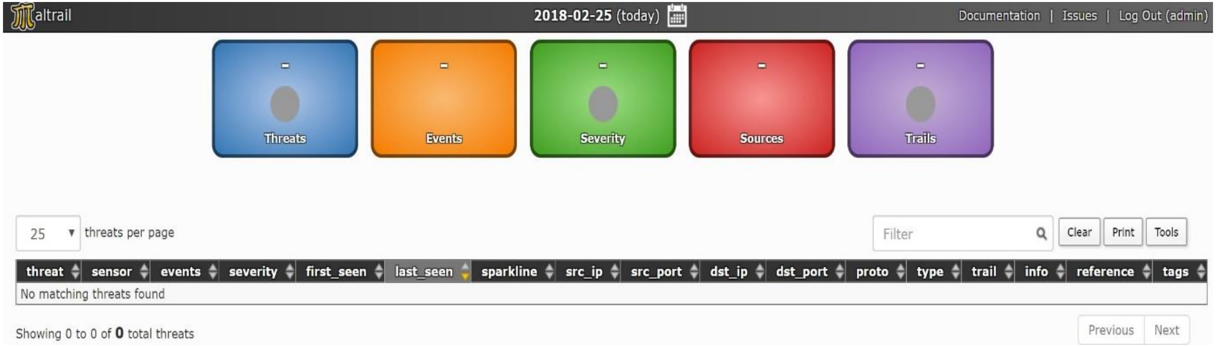
Username:

Password:

Powered by Maltrail (v0.10.309)

Running Maltrail

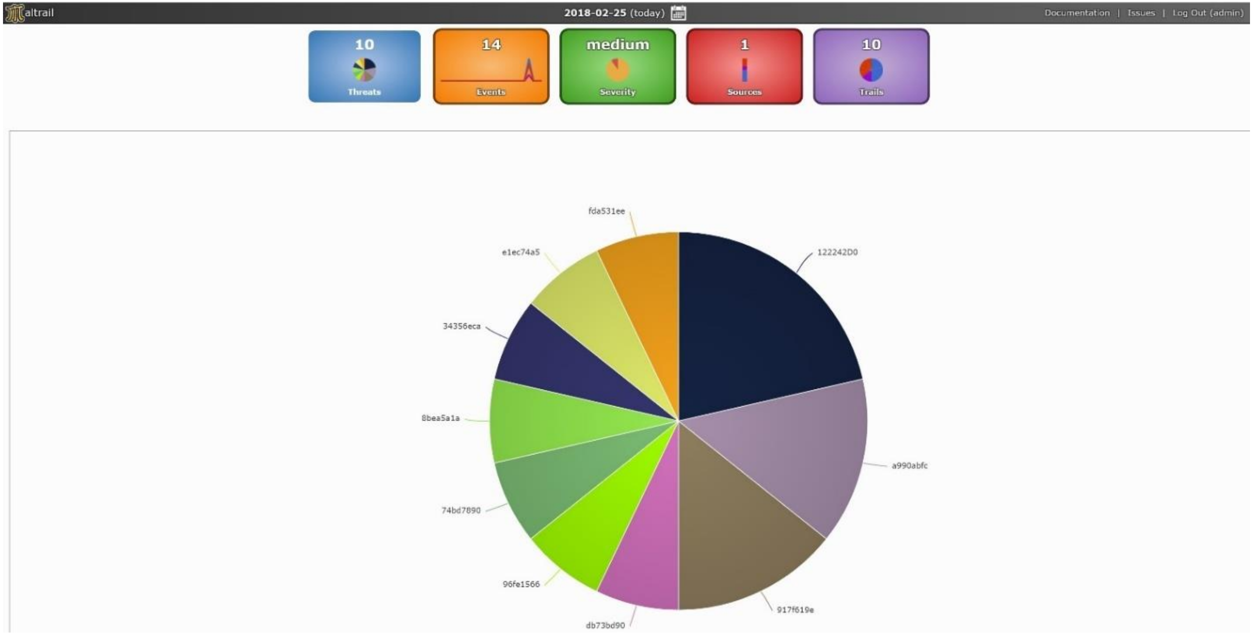
- Access the reporting interface (i.e. Client) by visiting the http://192.168.10.12:8338 (default credentials: admin:changeme!) from your web browser



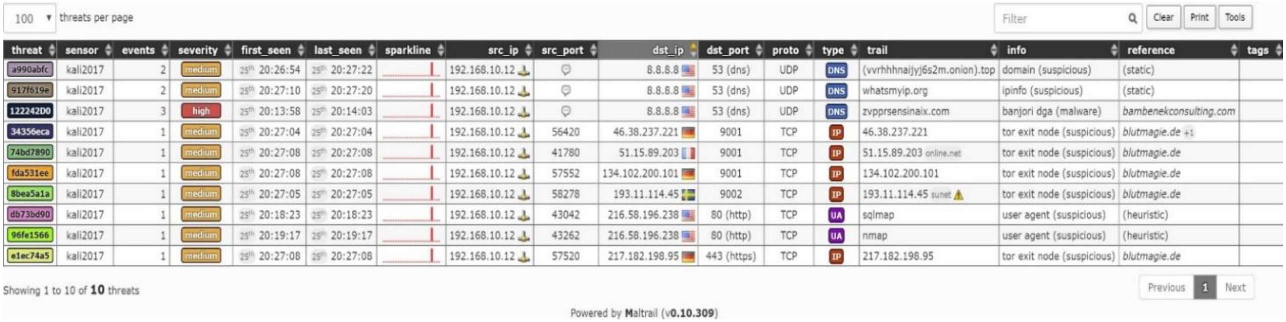
threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
No matching threats found																

Showing 0 to 0 of **0** total threats

Running Maltrail



Running Maltrail



threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
a990abfc	kali2017	2	medium	25th 20:26:54	25th 20:27:22		192.168.10.12		8.8.8.8	53 (dns)	UDP	DNS	(vvrhhhnaijyj6s2m.onion).top	domain (suspicious)	(static)	
917f619e	kali2017	2	medium	25th 20:27:10	25th 20:27:20		192.168.10.12		8.8.8.8	53 (dns)	UDP	DNS	whatsmyip.org	ipinfo (suspicious)	(static)	
122242D0	kali2017	3	high	25th 20:13:58	25th 20:14:03		192.168.10.12		8.8.8.8	53 (dns)	UDP	DNS	zvpprsensinaix.com	banjori dga (malware)	*bambenekconsulting.com*	
34356eca	kali2017	1	medium	25th 20:27:04	25th 20:27:04		192.168.10.12	56420	46.38.237.221	9001	TCP	IP	46.38.237.221	tor exit node (suspicious)	*blutmagie.de* +1	
74bd7890	kali2017	1	medium	25th 20:27:08	25th 20:27:08		192.168.10.12	41780	51.15.89.203	9001	TCP	IP	51.15.89.203 online.net	tor exit node (suspicious)	*blutmagie.de*	
fda531ee	kali2017	1	medium	25th 20:27:08	25th 20:27:08		192.168.10.12	57552	134.102.200.101	9001	TCP	IP	134.102.200.101	tor exit node (suspicious)	*blutmagie.de*	
8bea5a1a	kali2017	1	medium	25th 20:27:05	25th 20:27:05		192.168.10.12	58278	193.11.114.45	9002	TCP	IP	193.11.114.45 sunet ⚠	tor exit node (suspicious)	*blutmagie.de*	
db73bd90	kali2017	1	medium	25th 20:18:23	25th 20:18:23		192.168.10.12	43042	216.58.196.238	80 (http)	TCP	UA	sqlmap	user agent (suspicious)	(heuristic)	
96fe1566	kali2017	1	medium	25th 20:19:17	25th 20:19:17		192.168.10.12	43262	216.58.196.238	80 (http)	TCP	UA	nmap	user agent (suspicious)	(heuristic)	
e1ec74a5	kali2017	1	medium	25th 20:27:08	25th 20:27:08		192.168.10.12	57520	217.182.198.95	443 (https)	TCP	IP	217.182.198.95	tor exit node (suspicious)	*blutmagie.de*	

Showing 1 to 10 of **10** threats

Powered by **M**altrail (v**0.10.309**)

References

- Github

https://github.com/stamparm/maltrail