SAINT: Mapping the Cybercrime

Vasileios Vlachos

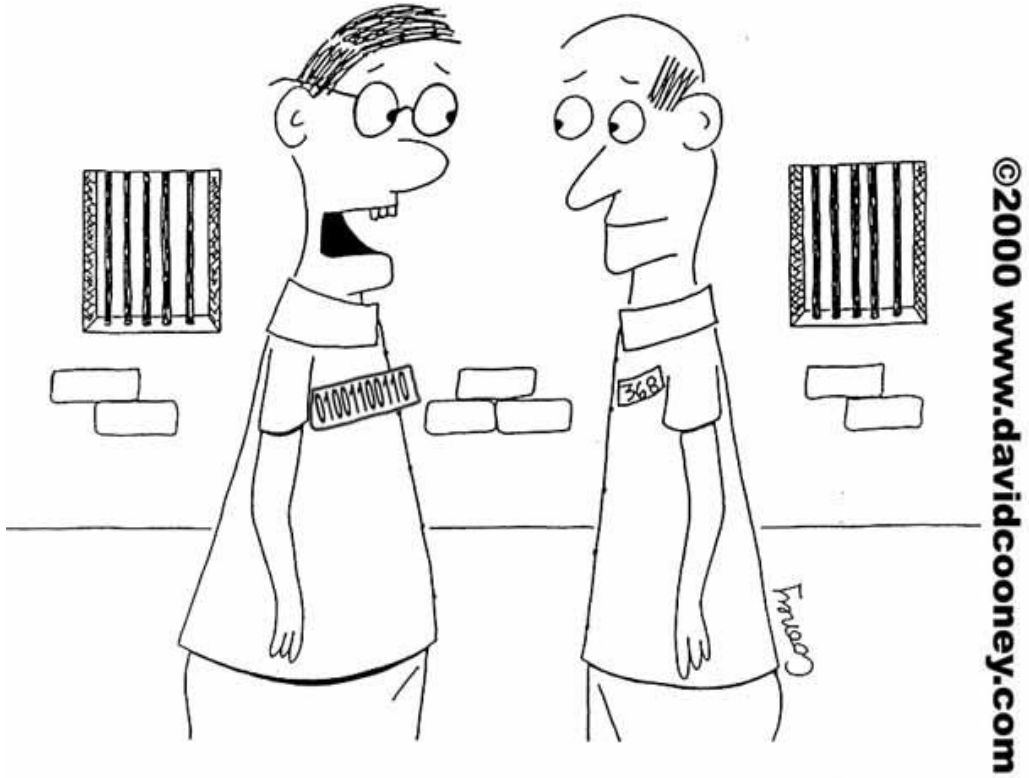
: vsvlachos :https://www.linkedin.com/in/vsvlachos/ :https://vsvlachos.blogspot.gr/

Computer Technology Institute
"DIOPHANTUS"

This work is performed within the SAINT Project (Systemic Analyser in Network Threats),
with the support of the European Commission and the Horizon 2020 Program, under Grant Agreement No 740829.

What is the Cost of Cybercrime?

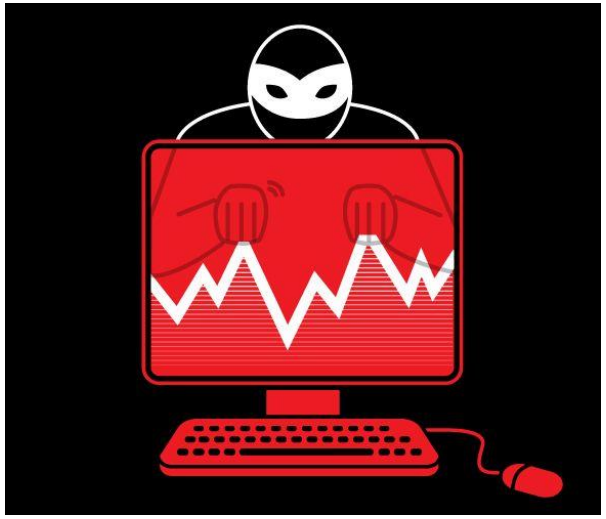
- **What is the value of our digital assets? How can we accurately measure the cost of cybercrime?**
- **After a hack most victims tend to underestimate the damage, but most security firms usually overestimate losses**
- **Estimate the strength of a security technology by learning what cybercriminals are willing to pay to bypass it and / or obtain the data**



"How'd you know I was in for cyber crime?"

SAINT CyberCrime Observatory – SCCO

- Create a pricelist – stock list of various digital goods
- Monitor price fluctuations
- Detect outliers
- Check cross-correlations and cross impacts between different indexes
- Raise alarms and provide early warning notifications
- Provide input for the economic analysis module



Deep Web

World Wide Web

A Deep Web Crawler (DWC):

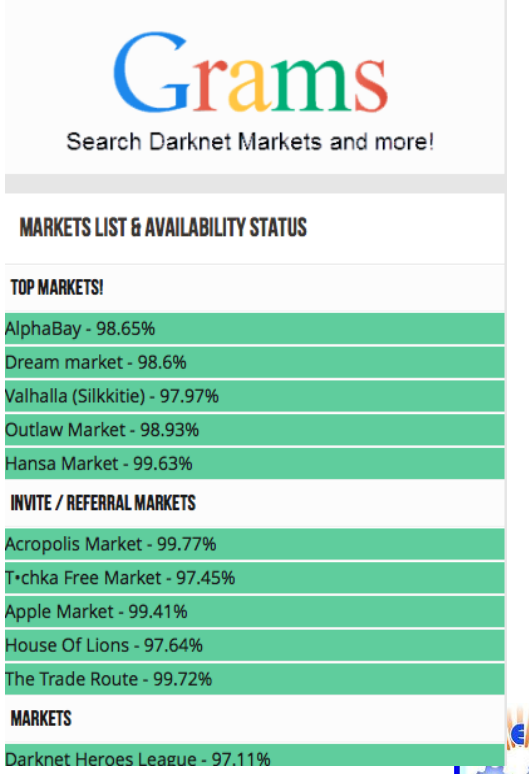
- Automatic Data Collection when possible
  - More challenging than the a simple Web Crawler

Analysis of Black Markets:

- Automatic via DWC
- Manual (Designated Researchers)
- Archives (TBs of data already available)

Open Source Intelligence (OSINT):

- Malware
- Bug Bounties
- Search Engines
- Security Updates
- Spam
- Vulnerabilities

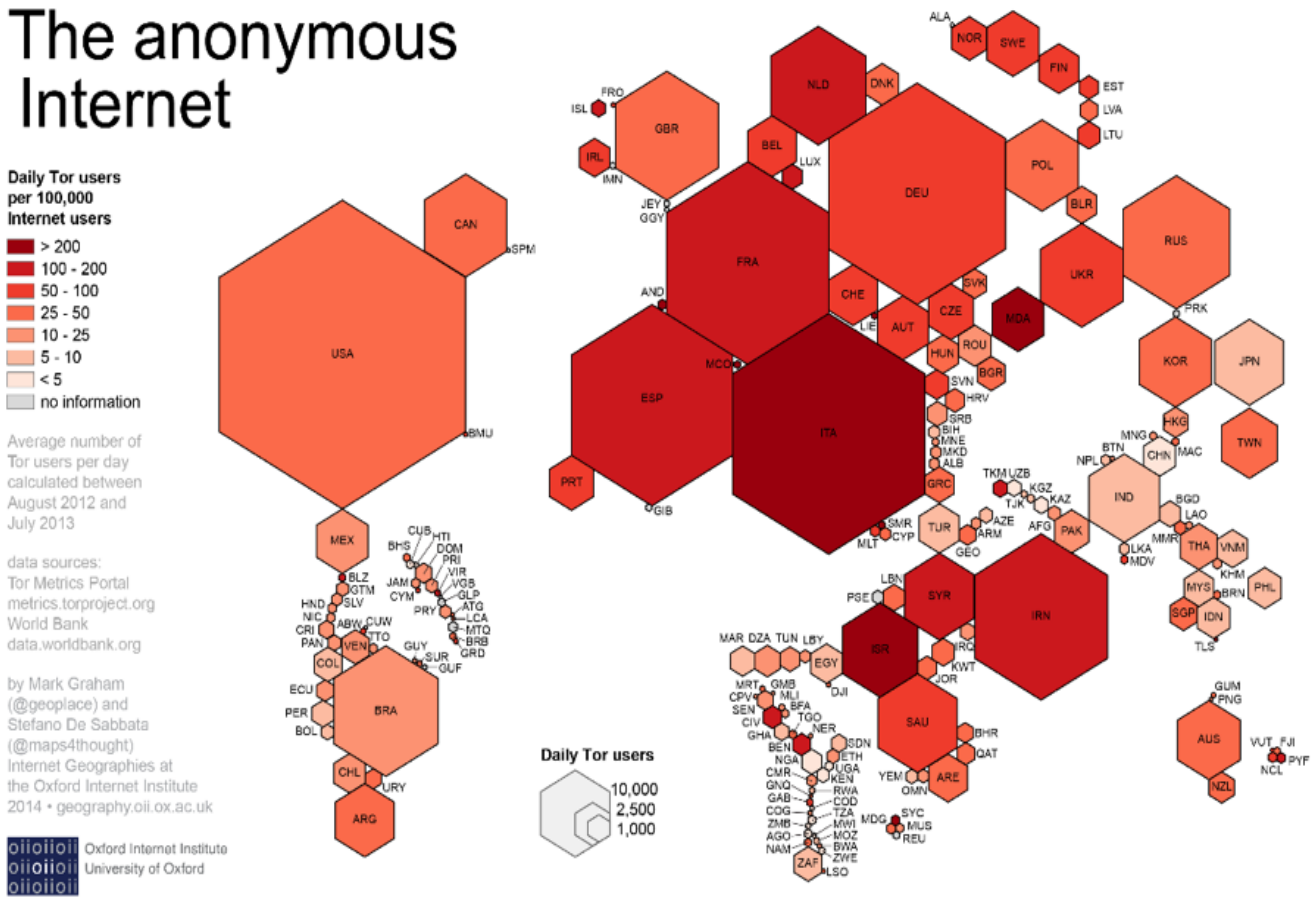


Deep Web Crawler

- Two different instances:
  - Clearnet Crawler tool
  - Deep & Dark Web Crawler tool

- Clearnet Crawler sub-instances:
  - ➢ some of the ENISA TOP 15 threats (Malware, Botnets, Spam, Phishing, DDoS, Web Based Attacks, Ransomware)
  - ➢ Bug Bounties (prices, entities)

- Deep & Dark Crawler sub-instances:
  - Vulnerability Markets
  - Cybercrime activity



Tor related usage information

SAINT CyberCrime Metrics: Underground

Deep Web Probes

Online:
- Markets
- Forums
- Vendor Shops

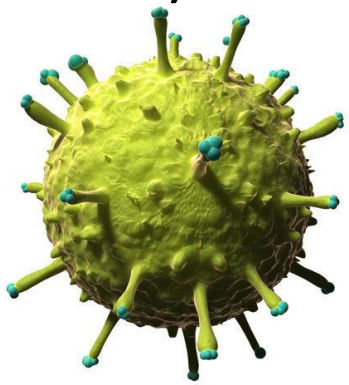
Offline:
- Cybercrime Statistical Data
- Archived of Black Markets

Dark Market Analysis

- Stolen Data:
  - Hacked Accounts
  - Credit Cards
- CaaS: Crime as a Service:
  - Botnets
  - Spam
  - Hackers for hire
  - Malware
  - Bulletproof providers
  - Pharma programs
- General Black Market Activity:
  - Posts
  - Members

SAINT CyberCrime Metrics: Malware

- New malware strains (AV effectiveness)
- Price of custom malware (AV effectiveness & OS Security)
- Number of new signatures (AV effectiveness)
- Safe Browsing blacklists (AV effectiveness & Browser Security)
- Malware hosting domains (AV effectiveness & Web Server Security)
- Top Malware lists – phylogenetic models (AV effectiveness)
- Number of AV solutions (AV effectiveness)
- Number of new IDS rules (new attacks)



SAINT CyberCrime Metrics: Spammers

- Spamlists: blocked domains / IPs (spamfilters effectiveness)
- Spam merchandise pricelist: drugs, software, replicas (anticounterfight solutions)
- Spam keywords blacklists (spamfilters effectiveness)
- Spam honeypots (spamfilters effectiveness)

SAINT CyberCrime Metrics: Search Engines

Google Hacking Results:

Automatic queries (time normalized)

"…
asslist
passlist.txt (a better way)
passwd
passwd / etc (reliable)
people.lst
psyBNC config files
pwd.db
server-dbs "intitle:index of"
signin filetype:url
spwd.db / passwd
filetype:sql "insert into" (pass|passwd|password)
filetype:sql ("values * MD5" | "values * password" | "values * encrypt")
filetype:sql +"IDENTIFIED BY" -cvs
filetype:sql password
filetype:url +inurl:"ftp://" +inurl:";@"
filetype:xls username password email
htpasswd
htpasswd / htgroup
htpasswd / htpasswd.bak
intext:"enable password 7"
intext:"enable secret 5 $" …/"

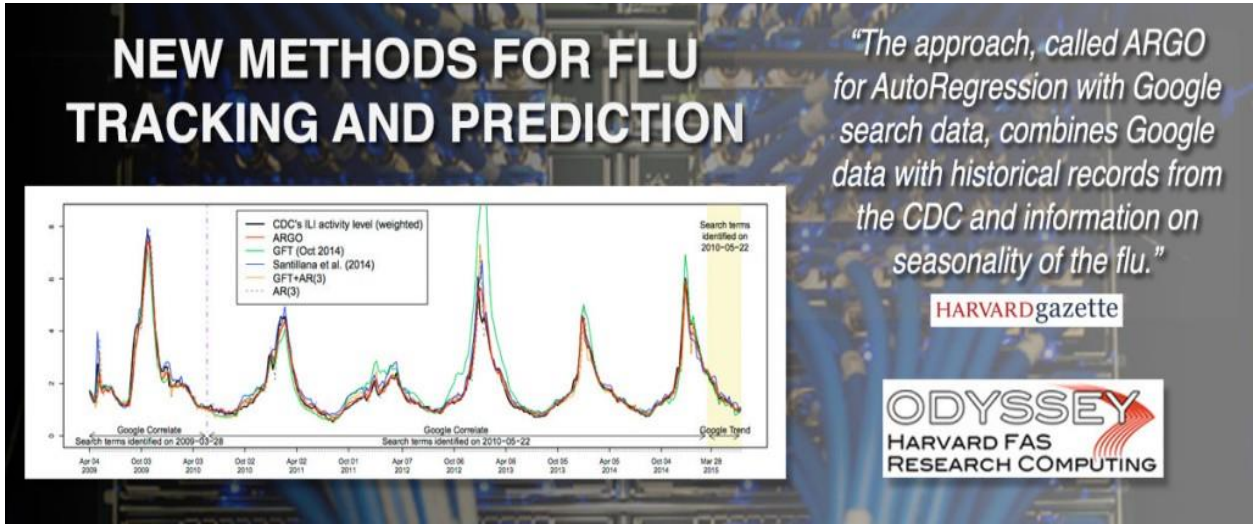
SHODAN
Computer Search Engine

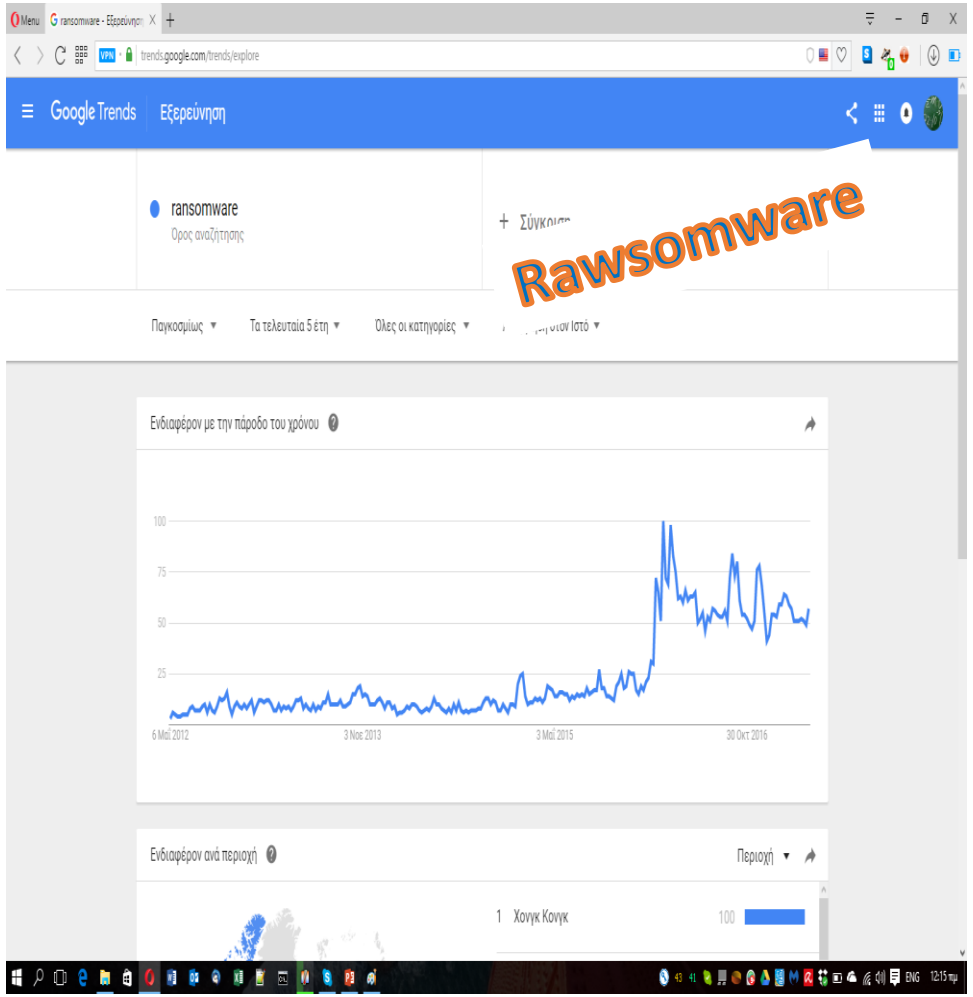
Shodan Hacking Results:

"…

- apache city:"Berlin"
- nginx country:"DE"
- Apache city:"Brussels" port:"8080" product:"Apache Tomcat/Coyote JSP engine"
- "Server: gws" hostname:"google"
- cisco net:"195.170.0.0/24"

SAINT CyberCrime Metrics: Trends





SAINT CyberCrime Metrics: Applications

- New security updates && patches && bugfixes
- Number of vulnerabilities && bugs && exploits
- Security Contests ($$$)
- Bug bounties ($$$)
- 0-days pricelist ($$$)
- Minor application versions aa.bb

ENISA Top 15 Indicators (2017)

1. Malware
2. Web-based attacks
3. Web application attacks
4. Phishing
5. Spam
6. Denial of Service
7. Ransomware
8. Botnets
9. Insider threat
10. Physical manipulation/damage/theft/loss
11. Data Breaches
12. Identity Theft
13. Information leakage
14. Exploit kits
15. Cyber-Espionage

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	Increasing	1. Malware	Stable	→
2. Web based attacks	Increasing	2. Web based attacks	Increasing	→
3. Web application attacks	Increasing	3. Web application attacks	Increasing	→
4. Denial of service	Increasing	4. Phishing	Increasing	↑
5. Botnets	Increasing	5. Spam	Increasing	↑
6. Phishing	Stable	6. Denial of service	Increasing	↓
7. Spam	Declining	7. Ransomware	Increasing	↑
8. Ransomware	Stable	8. Botnets	Increasing	↓
9. Insider threat	Stable	9. Insider threat	Stable	→
10. Physical manipulation/damage/ theft/loss	Increasing	10. Physical manipulation/damage/ theft/loss	Stable	→
11. Exploit kits	Increasing	11. Data breaches	Increasing	↑
12. Data breaches	Increasing	12. Identity theft	Increasing	↑
13. Identity theft	Declining	13. Information leakage	Increasing	↑
14. Information leakage	Increasing	14. Exploit kits	Declining	↓
15. Cyber espionage	Declining	15. Cyber espionage	Increasing	→

Legend: Trends: Declining, Stable, Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Web Based Attacks I: http://lists.blocklist.de/lists/all.txt
Web Based Attacks II: http://feeds.dshield.org/block.txt -

threats.webBasedAttacks1 — DOCUMENTS 65.7k, TOTAL SIZE 6.5MB, AVG. SIZE 103B

Documents | Schema | Explain Plan | Indexes | Validation

FILTER { field: 'value' }

INSERT DOCUMENT | VIEW | LIST | TABLE | Displaying

```
_id: ObjectId("5a82f3b8ccf9361c5c4f8137")
IP: "1.123.8.201"
TimestampUTC: 1518524312.853036
DatetimeUTC: "2018-02-13 14:18:32"

_id: ObjectId("5a82f3b8ccf9361c5c4f8138")
IP: "1.136.172.197"
TimestampUTC: 1518524312.853036
DatetimeUTC: "2018-02-13 14:18:32"

_id: ObjectId("5a82f3b8ccf9361c5c4f8139")
IP: "1.160.131.66"
TimestampUTC: 1518524312.853036
DatetimeUTC: "2018-02-13 14:18:32"

_id: ObjectId("5a82f3b8ccf9361c5c4f813a")
IP: "1.161.14.57"
TimestampUTC: 1518524312.853036
DatetimeUTC: "2018-02-13 14:18:32"
```

threats.webBasedAttacks2 — DOCUMENTS 40, TOTAL SIZE 11.1KB, AVG. SIZE 285B

Documents | Schema | Explain Plan | Indexes | Validation

FILTER { field: 'value' }

INSERT DOCUMENT | VIEW | LIST | TABLE | Displayin

```
_id: ObjectId("5a9059fca637881d2802e257")
Start: "196.52.43.0"
End: "196.52.43.255"
Netmask: 24
Attacks: 1111
Name: "LEASEWEB-NL Netherlands"
Country: "NL"
email: "abuse@nl.leaseweb.com"
Entity type: "IP"
Category: "Web Based Attacks"
TimestampUTC: 1519402460.451136
DatetimeUTC: "2018-02-23 18:14:20"

_id: ObjectId("5a9059fca637881d2802e258")
Start: "77.72.82.0"
End: "77.72.82.255"
Netmask: 24
Attacks: 1085
Name: "NETUP-AS"
Country: "RU"
email: "aospan@netup.ru"
Entity type: "IP"
Category: "Web Based Attacks"
TimestampUTC: 1519402460.451136
DatetimeUTC: "2018-02-23 18:14:20"
```

JSON formatted document objects

Index of /lists

Name	Last modified	Size	Description
Parent Directory		-	
21.txt	2018-02-28 14:30	8.6K	
22.txt	2018-02-28 14:30	113K	
25.txt	2018-02-28 14:30	248K	
80.txt	2018-02-28 14:30	137K	
110.txt	2018-02-28 14:30	29K	
143.txt	2018-02-28 14:30	29K	
443.txt	2018-02-28 14:30	137K	
993.txt	2018-02-28 14:30	29K	
all.txt	2018-02-28 14:30	396K	
all.txt.md5	2018-02-28 14:40	32	
apache.txt	2018-02-28 14:30	137K	
apache.txt.md5	2018-02-28 14:40	32	
asterisk.txt	2018-02-28 14:30	1.7K	
bots.txt	2018-02-28 14:30	1.6K	
bots.txt.md5	2018-02-28 14:40	32	
bruteforcelogin.txt	2018-02-28 14:31	9.4K	
bruteforcelogin.txt.md5	2018-02-28 14:40	32	
courierimap.txt	2018-02-28 14:30	29K	
courierpop3.txt	2018-02-28 14:30	29K	

Server content

```
1.109.90.186
1.119.43.90
1.161.70.27
1.163.48.51
1.164.50.14
1.164.54.166
1.170.167.237
1.171.181.8
1.171.208.163
1.172.116.111
1.172.49.78
1.173.121.122
1.173.158.67
1.173.164.235
1.175.60.57
1.180.145.122
1.180.158.238
1.180.64.86
1.180.70.178
1.186.113.79
1.187.240.164
1.187.249.202
1.189.131.177
1.189.206.145
1.190.175.66
1.191.139.239
1.192.240.101
1.192.240.113
1.192.240.135
1.192.240.179
1.192.240.210
1.192.240.48
1.192.240.92
```

List of IPs scraped

```
#
#   DShield.org Recommended Block List
#    (c) 2018 DShield.org
#   some rights reserved. Details http://creativecommons.org/licenses/by-nc-sa/2.5/
#   use on your own risk. No warranties implied.
#   primary URL: http://feeds.dshield.org/block.txt
#     PGP Sign.: http://feeds.dshield.org/block.txt.asc
#
#   comments: info@dshield.org
#    updated: Wed Feb 28 14:34:48 2018 UTC
#
#    This list summarizes the top 20 attacking class C (/24) subnets
#   over the last three days. The number of 'attacks' indicates the
#   number of targets reporting scans from this subnet.
#
#
#    Columns (tab delimited):
#
#    (1) start of netblock
#    (2) end of netblock
#    (3) subnet (/24 for class C)
#    (4) number of targets scanned
#    (5) name of Network
#    (6) Country
#    (7) contact email address
#
#    If a range is assigned to multiple users, the first one is listed.
#
```

page info

Start	End	Netmask	Attacks	Name	Country	email
196.52.43.0	196.52.43.255	24	1202	LEASEWEB-NL Netherlands,	NL	abuse@nl.leaseweb.com
80.82.77.0	80.82.77.255	24	1188	QUASINETWORKS , NL		abuse@quasinetworks.com
93.174.93.0	93.174.93.255	24	1186	QUASINETWORKS , NL		abuse@quasinetworks.com
66.111.41.0	66.111.41.255	24	1177	SAGO NET - Sago Networks, LLC,	US	abuse@sagonet.com
77.72.82.0	77.72.82.255	24	1161	NETUP-AS ,	RU	aospan@netup.ru
146.0.77.0	146.0.77.255	24	1155	HOSTKEY-AS ,	NL	abuse@hostkey.nl
5.188.86.0	5.188.86.255	24	1148	PIN-AS ,	RU	abuse@pinspb.ru
181.214.87.0	181.214.87.255	24	1147	WZCOM-US - WZ Communications Inc.,	US	abuse@webazilla.com
191.101.167.0	191.101.167.255	24	1143	Digital Energy Technologies Chile SpA,	CL	noc@AS61440.NET
5.188.11.0	5.188.11.255	24	1134	PIN-AS ,	RU	abuse@pinspb.ru
180.97.106.0	180.97.106.255	24	1130	CHINANET-BACKBONE No.31,Jin-rong Street,	CN	anti-spam@ns.chinanet.cn.net
60.191.38.0	60.191.38.255	24	1112	CHINANET-BACKBONE No.31,Jin-rong Street,	CN	anti-spam@ns.chinanet.cn.net
141.212.122.0	141.212.122.255	24	1112	UMICH-AS-5 - University of Michigan,	US	abuse@umich.edu
89.248.168.0	89.248.168.255	24	1101	QUASINETWORKS , NL		abuse@quasinetworks.com
71.6.146.0	71.6.146.255	24	1100	CARINET - CariNet, Inc.,	US	complaints@cari.net
58.218.213.0	58.218.213.255	24	1091	CHINANET-BACKBONE No.31,Jin-rong Street,	CN	anti-spam@ns.chinanet.cn.net
5.188.10.0	5.188.10.255	24	1085	PIN-AS ,	RU	abuse@pinspb.ru
125.212.217.0	125.212.217.255	24	1080	VIETEL-AS-AP Viettel Corporation,	VN	hm-changed@vnnic.net.vn
92.63.197.0	92.63.197.255	24	1075	ITDELUXE-AS ,	RU	support@itdeluxe.com
77.72.85.0	77.72.85.255	24	1063	NETUP-AS ,	RU	aospan@netup.ru

scraping content

SAINT Systemic Analyser In Network Threats

DDoS: https://www.exploit-db.com/google-hacking-database/12/

Phishing: https://www.phishtank.com/

Pages Containing Login Portals

main page

These are login pages for various services. Consider them the front door of a websites more sensitive functions.

Pages Containing Login Portals | Search | Search

<< prev 1 2 3 4 5 6 7 8 9 10 next >>

Date	Title	Summary
2018-02-14	inurl:/frontend/paper_lantern/index.html	inurl:/frontend/paper_lantern/index.html This Dork is useful to search and find CPANEL login...
2018-01-24	inurl:/login/index.php intitle:CentOS	inurl:/login/index.php intitle:CentOS Finds CentOS Web Panel Login Pages. See http://centos-...
2018-01-22	inurl:"/jde/E1Menu.maf"	This dork is to search for public available jd edward ERP portals. Dork: inurl:"/jde/E1...
2018-01-08	inurl:"/libs/granite/core/content/login.html&...	The following dork will give you the list of AEM Installed server. (Adobe Experience Manager) ...
2017-12-11	inurl:"https://mylogin."	Finds login pages, mostly on educational websites Dxtroyer ...
2017-12-11	inurl:"/moodle/login/index.php"	Finds Moodle Login pages Dxtroyer ...
2017-12-07	intitle:"Panel Administracyjny"	*Google Dork : intitle:"Panel Administracyjny"* *Description : Show admin panel of...
2017-11-13	inurl:"communique_detail.php?id="	*Google Dork Description*:inurl:"communique_detail.php?id=" -with this dork it is ...

inurl:/frontend/paper_lantern/index.html

« Previous GHDB

Google Dork Description: inurl:/frontend/paper_lantern/index.html	**GHDB-ID:** 4671
Google Search: inurl:/frontend/paper_lantern/index.html	**EDB-ID:** N/A
Published: 2018-02-14	**Author:** Nisankh Acharjya

```
1 inurl:/frontend/paper_lantern/index.html
2
3 This Dork is useful to search and find CPANEL login
```

scraping for further information of each threat instance

threats.exploitDataBase — DOCUMENTS 422 — TOTAL SIZE 236.0KB — AVG. SIZE 573B

Documents | Schema | Explain Plan | Indexes | Validation

FILTER { field: 'value' } — INSERT DOCUMENT — VIEW LIST TABLE — Displaying


```
_id: 4671
Category: "DDoS"
Subcategory: "Pages Containing Login Portal"
Entity Type - Google_search: "inurl:/frontend/paper_lantern/index.html"
Google Dork Description: "inurl:/frontend/paper_lantern/index.html"
Description: "inurl:/frontend/paper_lantern/index.html This Dork is useful to search..."
ENB-ID: "N/A"
TimestampUTC: 1518559200
DatetimeUTC: "2018-02-14"
TimestampUTC-CTI: 1519742800.355923
DatetimeUTC-CTI: "2018-02-27 16:46:40"
Author: "Nisankh Acharjya"

_id: 4661
Category: "DDoS"
Subcategory: "Pages Containing Login Portal"
Entity Type - Google_search: "inurl:/login/index.php intitle:CentOS"
Google Dork Description: "intitle:CentOS"
Description: "inurl:/login/index.php intitle:CentOS Finds CentOS Web Panel Login Pag..."
ENB-ID: "N/A"
TimestampUTC: 1516744800
DatetimeUTC: "2018-01-24"
TimestampUTC-CTI: 1519742801.318494
DatetimeUTC-CTI: "2018-02-27 16:46:41"
Author: "InspecterNull"
```


JSON formatted document objects

scraping for further information of each threat instance

PhishTank® Out of the Net, into the Tank.

Home | Add A Phish | Verify A Phish | Phish Search | Stats | FAQ | Developers | Mailing Lists | My Account

Submission #5503126 is currently ONLINE

Submitted Feb 28th 2018 3:32 PM by prodigyabuse (Current time: Feb 28th 2018 3:32 PM UTC)

http://meribatsuno.cf/user/Indexxatt.htm

Sign in or Register to verify this submission.

This submission needs more votes to be confirmed or denied.

Screenshot of site | View site in frame | View technical details | View site in new window

main page

PhishTank® Out of the Net, into the Tank.

Phish Search | Stats | FAQ | Developers | Mailing Lists | My Account

Verify A Phish

Showing unverified and online submissions

See all submissions in the phish archive

ID	Phish URL	Submitted	Valid?	Online?
5503124	https://scom.yolasite.com/ added on Feb 28th 2018 3:30 PM	by SWITCHCERT	Unknown	ONLINE
5503122	http://185.140.115.10/2018/home.html added on Feb 28th 2018 3:27 PM	by ShinobiPhish	Unknown	ONLINE
5503121	http://185.140.115.10/2018/home.html added on Feb 28th 2018 3:25 PM	by ShinobiPhish	Unknown	ONLINE
5503118	https://sichern.secapple2.com-ch-pyplswitz37.co.uk/... added on Feb 28th 2018 3:22 PM	by SWITCHCERT	Unknown	ONLINE
5503115	http://techsupport-team.com/ljmu.ac.html added on Feb 28th 2018 3:16 PM	by j1mb0b	Unknown	ONLINE
5503114	https://habitscr.weebly.com/ added on Feb 28th 2018 3:13 PM	by verifrom	Unknown	ONLINE
5503113	http://ec2-18-222-38-179.us-east-2.compute.amazonaws.com/NOVARICARDO20... added on Feb 28th 2018 3:12 PM	by DefesaDigital	Unknown	ONLINE
5503111	https://bizdevar.tk/catalog/view/javascript/font-awesome/fonts/it/arub... added on Feb 28th 2018 3:09 PM	by drepp85	Unknown	ONLINE
5503110	http://victoriapesca.com.ar/sec/aut.php added on Feb 28th 2018 3:07 PM	by masterblaster	Unknown	ONLINE

threats.phishtank — DOCUMENTS 3.5k — TOTAL SIZE 1.1MB — AVG. SIZE 329B

Documents | Schema | Explain Plan | Indexes | Validation

FILTER { field: 'value' } — INSERT DOCUMENT — VIEW LIST TABLE — Displaying


```
_id: "5501650"
Phish URL: "http://www.00000oooo11111111111111100000oooo.com/"
Submitted by: "PhishReporter"
Valid?: "Unknown"
Online?: "ONLINE"
DatetimeUTC: "2018-02-27 18:54:00"
TimestampUTC: 1519750440
DatetimeUTC-CTI: "2018-02-27 18:55:30"
TimestampUTC-CTI: 1519750530.102041
Entity type: "URL"
Category: "Phishing"

_id: "5501649"
Phish URL: "https://sites.google.com/site/systimrecovery48/home"
Submitted by: "leofelix"
Valid?: "Unknown"
Online?: "ONLINE"
DatetimeUTC: "2018-02-27 18:50:00"
TimestampUTC: 1519750200
DatetimeUTC-CTI: "2018-02-27 18:55:30"
TimestampUTC-CTI: 1519750530.102041
Entity type: "URL"
Category: "Phishing"
```


JSON formatted document objects

ITYE "ΔΙΟΦΑΝΤΟΣ" ινστιτουτο τεχνολογιας υπολογιστων & εκδοσεων

Malware: https://mirror.uce.edu.ec/malwaredomains/ -
Botnets: http://osint.bambenekconsultingcom/feeds/c2-ipmasterlist.txt

Espejo Público de

../malwaredomains/

filename	timestamp
../	28 Feb 2018, 08:04
20160801.txt	01 Aug 2016, 17:10
20160802.txt	02 Aug 2016, 16:53
20160803.txt	03 Aug 2016, 16:56
20160804.txt	04 Aug 2016, 16:14
20160805.txt	05 Aug 2016, 16:51
20160807.txt	07 Aug 2016, 22:59
20160808.txt	08 Aug 2016, 16:46
20160809.txt	09 Aug 2016, 16:04
20160810.txt	10 Aug 2016, 16:07
20160811.txt	11 Aug 2016, 16:32
20160812.txt	12 Aug 2016, 15:26
20160815.txt	15 Aug 2016, 16:40
20160816.txt	16 Aug 2016, 16:47
20160817.txt	17 Aug 2016, 16:06

```
floreplan.com.br        phishing        cybertracker.malwarehunte
pousadarotadaspraias.com.br     phishing        cybertracker.malw
srs-bd.com      phishing        private 20160801
s-teamworld.com predator        cybertracker.malwarehunterteam.co
validlogin.top  rat     cybertracker.malwarehunterteam.com      2
12-land.co.jp   locky   techhelplist.com        20160801
akeseverin.com  locky   techhelplist.com        20160801
krovgid.ru      locky   techhelplist.com        20160801
libertymanuals.com      locky   techhelplist.com        20160801
programistyczni.strefa.pl       locky   techhelplist.com        2
ramsayconstruction.ca   locky   techhelplist.com        20160801
steelfs.com.mx  locky   techhelplist.com        20160801
visionaero.com  locky   techhelplist.com        20160801
robtozier.com   locky   techhelplist.com        20160801
axcpbvmtj.info  pykspa  private 20160801
bothimportant.net       suppobox        private 20160801
dhllocgjklyq.com        tinba   private 20160801
doctornotice.net        suppobox        private 20160801
fellowlength.net        suppobox        private 20160801
fieldrain.net   suppobox        private 20160801
fmbaucylhdainytfyzhddqhha.com   murofet private 20160801
fvwvupqbcwpg.com        tinba   private 20160801
gainover.net    suppobox        private 20160801
gpdcrtustufu.com        tinba   private 20160801
hkleofepnyvv.com        tinba   private 20160801
hpplus.net      nymaim  private 20160801
ihkhhxsxwfev.com        tinba   private 20160801
kbfnilkoobyl.org        tinba   private 20160801
mothermodern.net        suppobox        private 20160801
nailhouse.net   suppobox        private 20160801
nayafm.com      nymaim  private 20160801
newbin.com      nymaim  private 20160801
nextfn.com      nymaim  private 20160801
otacee.com      virut   private 20160801
pgwernynwwkk.com        tinba   private 20160801
```

```
#################################################################
## Master Feed of known, active and non-sinkholed C&Cs IP
## addresses
##
## Feed generated at: 2018-03-14 12:13
##
## 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/c2-ipmasterlist.txt
##
## All times are in UTC
#################################################################
23.107.124.53,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekc
23.228.203.69,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekc
23.236.62.147,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekc
23.89.102.179,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekc
43.230.142.125,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenek
43.241.196.105,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenek
50.63.202.18,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekcon
50.63.202.28,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekcon
50.63.202.3,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekcons
50.63.202.8,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
62.149.142.219,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
62.4.17.220,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
67.231.240.114,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
67.55.92.182,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
67.55.92.183,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
69.46.71.59,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
69.64.147.249,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
74.208.236.219,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
74.220.199.8,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
74.220.207.152,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
78.24.9.52,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
78.46.156.194,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
81.169.145.159,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
81.169.145.160,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
81.169.145.161,IP used by banjori C&C,2018-03-14 12:04,http://osint.bambenekconsulting.com/manual/banjori.txt
```

```
#################################################################
## Master list feed of all current C&C IPs using DGAs
##
## Feed Provided By: John Bambenek of Bambenek Consulting
## jcb@bambenekconsulting.com // http://bambenekconsulting.com
##
#################################################################

This feed is merely an aggregate of the other feeds which list
IP addresses of active and non-sinkholed C&C servers.  The
current list of malware families that are represented in
these feeds are:

  - Cryptolocker
  - GameOver Zeus (p2p and post-Tovar)
  - tinba
  - matsnu
  - pushdo
  - qakbot

See the respecitve manual pages for how each indicator is
generated.

This feed is generated every 10 minutes.
```

JSON formatted document objects

SAINT – Threats database collections -MongoDB (NoSQL schema database &JSON Big Data)

```
Event_ID,Attribute_ID,Datetime,Category,Type
2,26,2014-03-25 09:47:42,Artifacts dropped,comment
2,27,2014-05-19 17:20:29,Artifacts dropped,filename
2,28,2014-03-25 09:45:09,Artifacts dropped,regkey|value
2,29,2014-05-19 17:20:40,Artifacts dropped,yara
2,30,2014-05-19 17:20:17,External analysis,link
2,31,2014-05-19 17:20:53,External analysis,link
2,32,2014-03-25 09:42:05,External analysis,url
2,33,2014-03-25 09:47:00,Network activity,comment
2,34,2014-03-25 09:43:40,Network activity,ip-dst
2,35,2014-03-25 09:44:10,Network activity,user-agent
2,36,2014-03-25 09:49:26,Payload delivery,vulnerability
2,37,2014-03-25 09:42:53,Payload installation,md5
2,38,2014-03-25 09:43:19,Payload installation,sha1
2,36678,2014-05-19 17:21:40,External analysis,link
3,39,2014-04-01 15:37:23,Antivirus detection,text
3,40,2014-04-01 15:37:23,Antivirus detection,text
3,41,2014-04-02 14:13:55,External analysis,link
3,42,2014-04-01 15:38:47,Payload delivery,filename|sha1
3,43,2014-04-01 15:38:47,Payload delivery,filename|sha256
3,44,2014-04-01 15:38:47,Payload delivery,malware-sample
3,45,2014-04-01 15:34:50,Payload delivery,md5
3,46,2014-04-01 15:51:55,Payload delivery,sha1
3,47,2014-04-01 15:50:34,Payload delivery,sha1
3,48,2014-04-01 15:36:11,Payload delivery,sha256
3,49,2014-04-01 15:33:13,Payload delivery,vulnerability
3,50,2014-04-01 15:36:44,Payload installation,sha1
```

Collections

CREATE COLLECTION

Collection Name	Documents	Avg. Document Size	Total Document Size	Num. Indexes	Total Index Size
exploitDataBase	422	572.7 B	236.0 KB	1	16.0 KB
ipmasterlist	20,363	375.7 B	7.3 MB	1	788.0 KB
malwaredomains	57,846	269.5 B	14.9 MB	1	564.0 KB
phishtank	6,105	303.8 B	1.8 MB	1	88.0 KB
webBasedAttacks1	65,700	103.3 B	6.5 MB	1	624.0 KB

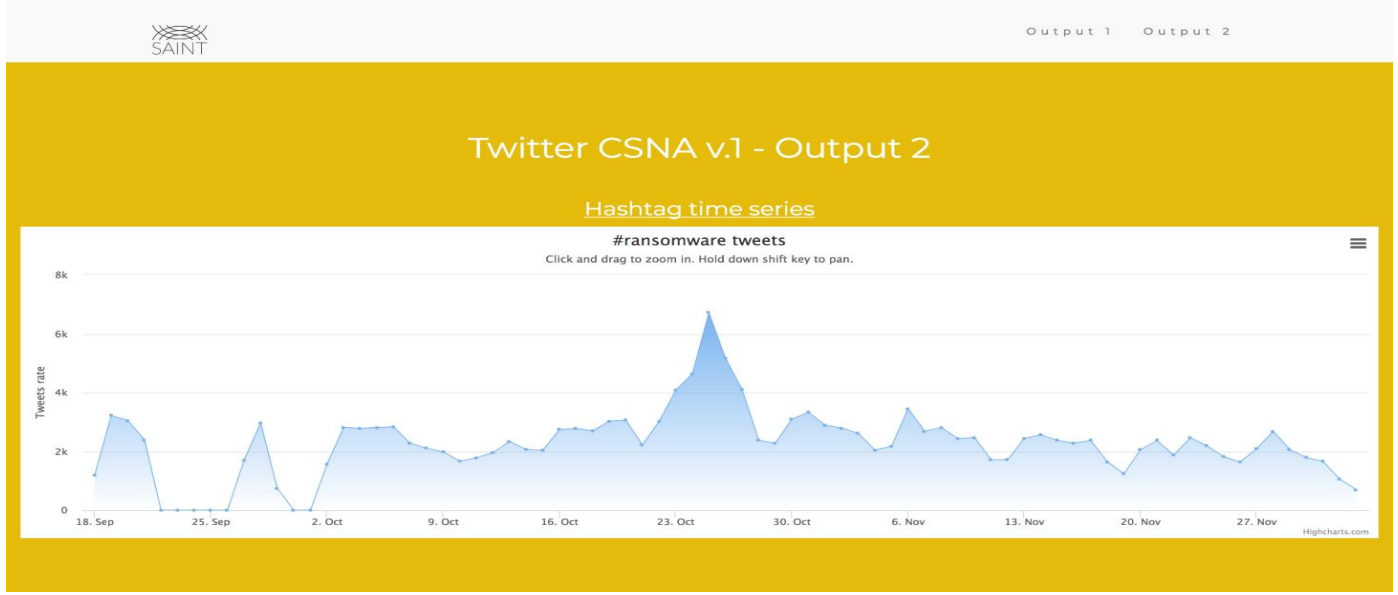
Database Name	Storage Size	Collections	Indexes
admin	68.0KB	0	3
demokritos	58.3MB	1	1
local	44.0KB	1	1
threats	6.7MB	5	5
twitter	1.2GB	2	2

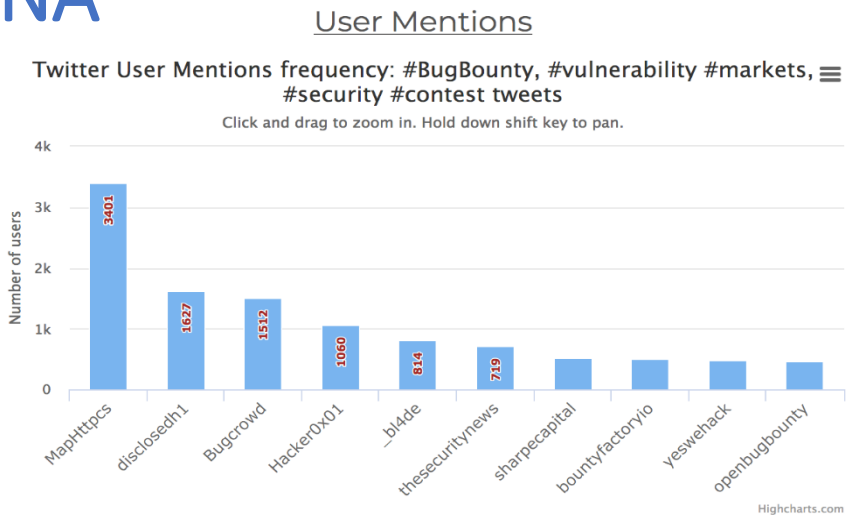
SAINT CyberCrime Metrics: Social Networks

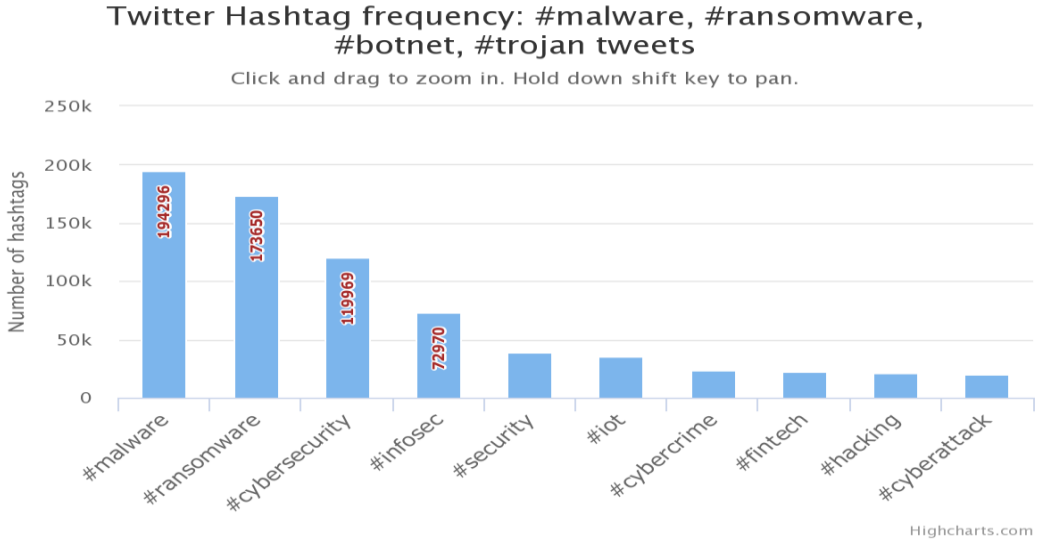
Social Network Analysis (SNA):

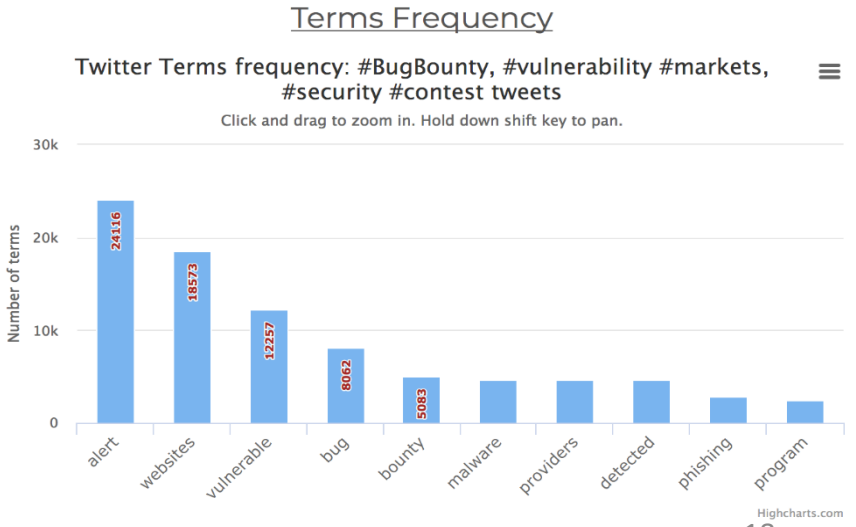
Twitter hastags frequency monitoring: #bugs #bounties #malware #hacking #spam #osint #deepweb #darkmarket #vulnerability #0day #apt #rat #bot #c&c #zombiepc #exploit #carders #phising #ddos #stressers #backfoor #logicbomb #dox #shell #blackhat #spoof #socialengineer #trojan #rawsomware #crimeware #resolver #scriptkiddie #root #rootkit #deface #XSS #SQLinjection #bufferoverflow #hactivism

Cybersecurity Social Network Analyzer - CSNA



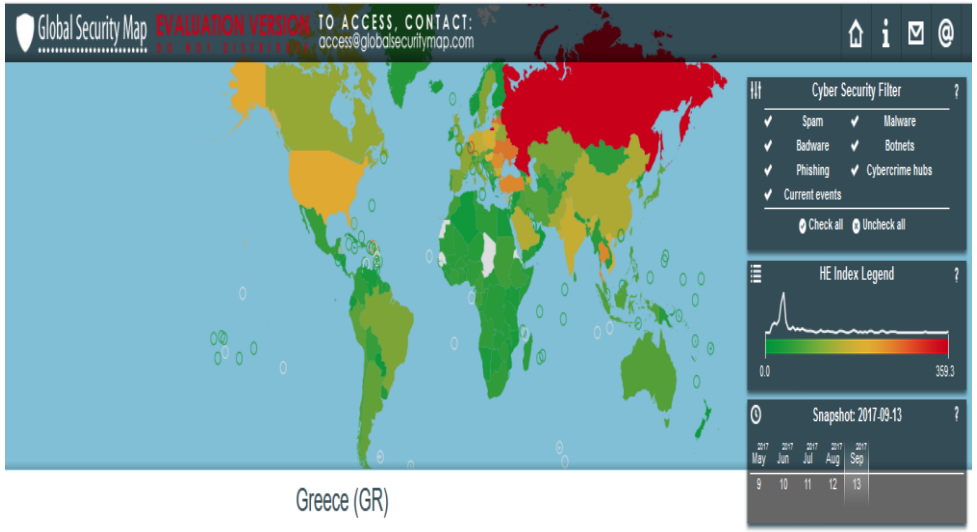






SAINT CyberCrime Metrics: Global Security Map

http://globalsecuritymap.com/#



Greece (GR)

Cyber security summary

Greece is ranked #61 out of 224 countries on the Host Exploit index for cyber security (HE-index) at 2017-09-13 (a higher rank equals worse security). The lowest ranking of Greece was 53 on 2014-09-06. The country's highest ranking was observed on 2011-12-24, where the country ranked 216.

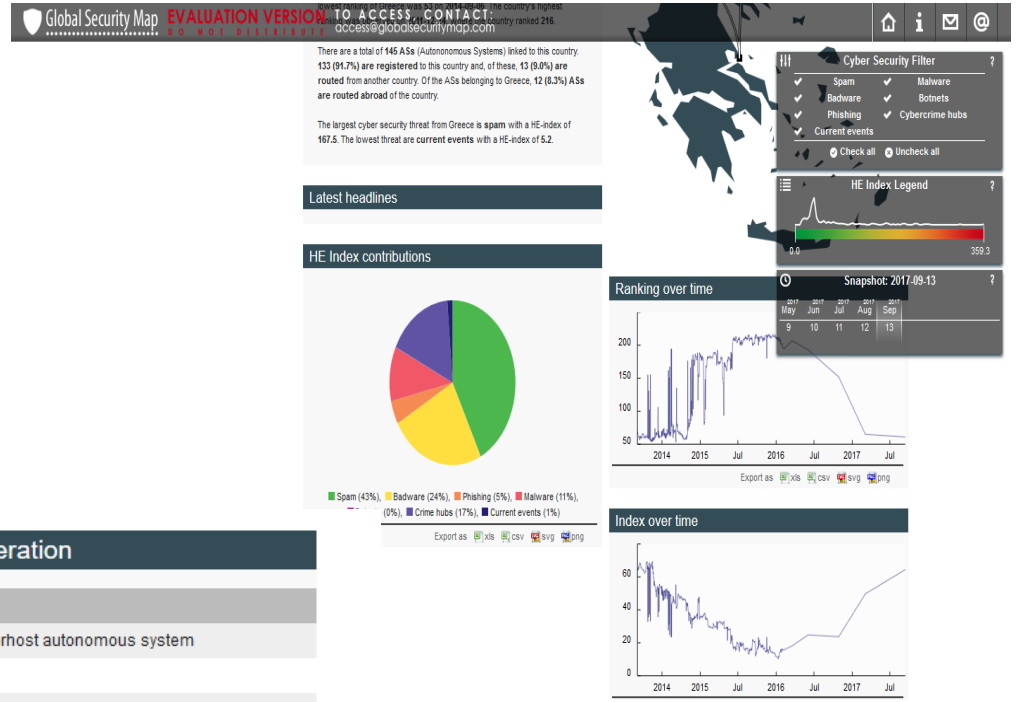
There are a total of 145 ASs (Autonomous Systems) linked to this country. 133 (91.7%) are registered to this country and, of these, 13 (9.0%) are routed from another country. Of the ASs belonging to Greece, 12 (8.3%) ASs are routed abroad of the country.

The largest cyber security threat from Greece is spam with a HE-index of 167.5. The lowest threat are current events with a HE-index of 5.2.

Latest headlines

Worst ASs of Russian Federation

HE-index	AS name
191.8	MASTERHOST-AS .masterhost autonomous system
159.5	AGAVA3 Agava Ltd.
157.0	IQHOST IQHost Ltd
147.5	ESERVER Hosting Operator eServer.ru Ltd.
140.6	CENTROHOST-AS CJSC Registrar R01
131.0	SWEB-AS SpaceWeb CJSC
129.7	CITYTELECOM-AS Filanco LTD
119.3	ASN-RUCENTER-HOSTING Autonomous Non-commercial Organization 'Regional Network Information Center'
113.7	RTCOMM-AS OJSC RTComm.RU
110.8	TIMEWEB-AS OOO TimeWeb



SAINT CyberCrime Metrics: Outcomes

- A SAINT CyberCrime Observatory for European citizens, stakeholders, legislators, security researchers, scientists and law enforcement officers
- Basic Early Warning Services for imminent threats
- A toolbox of methodologies and prototype applications to analyze IT security trends and cybercrime activity
- A set of cybercrime metrics to evaluate the financial impact of existing cybersecurity technologies

Saint EU Project Home: https://project-saint.eu/

Stay connected

https://vimeo.com/246975321

A successful workshop organized by SAINT consortium

Wednesday 28 March, 2018

The 1st SAINT workshop took place last Tuesday 20 March 2018. A highly successful event for clustering and networking for Cyber Security projects, hosted by the NCSR "Demokritos" in Athens. The objective of this workshop was achieved by bringing together several EU cyber security and privacy related projects, exchanging knowledge and ideas and promoting inter-project collaboration.

Read more

The SAINT workshop

Date: Tuesday, March 20, 2018

The H2020 SAINT project organises its 1st workshop on Tuesday, March 20th 2018 in Athens.

The main objective of this workshop is to bring together several EU cyber security and privacy related projects, to assist in the exchange of knowledge and ideas and promote inter-project collaboration.

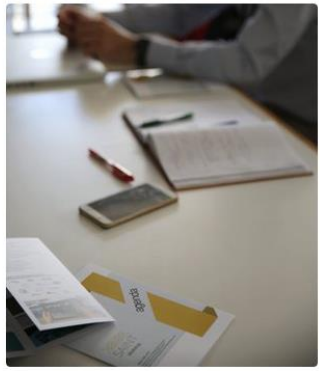
Date: 20.03.2018

Venue: NCSR "Demokritos" , Institute of Informatics & Telecommunications Building (No 26)
Patriarchou Gregoriou E & 27 Neapoleos str, Agia Paraskevi, Athens, Greece

Read more

Tweets by @saintprojecteu

saintprojecteu
@saintprojecteu
More about the #saintprojecteu workshop follow up at project-saint.eu/article/succes...



Mar 30, 2018

saintprojecteu
@saintprojecteu
Thank you all for contributing to this successful workshop! All presentations are now available on: project-saint.eu/event/saint-wo... #saintprojecteu @sissden @enisa_eu @CYBECO_project @ANASTACIA_H2020 @konfidoproject @shield_h2020 @DOGANAProject @CIPSECproject

Thank you for your attention!

Q&A

Vasileios Vlachos

Assistant Professor
Department of Computer Science and Engineering
Technological Educational Institute (TEI) of Thessaly

: vsvlachos :https://www.linkedin.com/in/vsvlachos/ :https://vsvlachos.blogspot.gr/