

RiskBased SECURITY

"Cyber" Who Done It?! Attribution Analysis Through Arrest History

Jake Kouns, CISO
jake@riskbasedsecurity.com
@jkouns

Lee Johnstone
Security Researcher
@83leej

August 2016

Cyber? Drink!

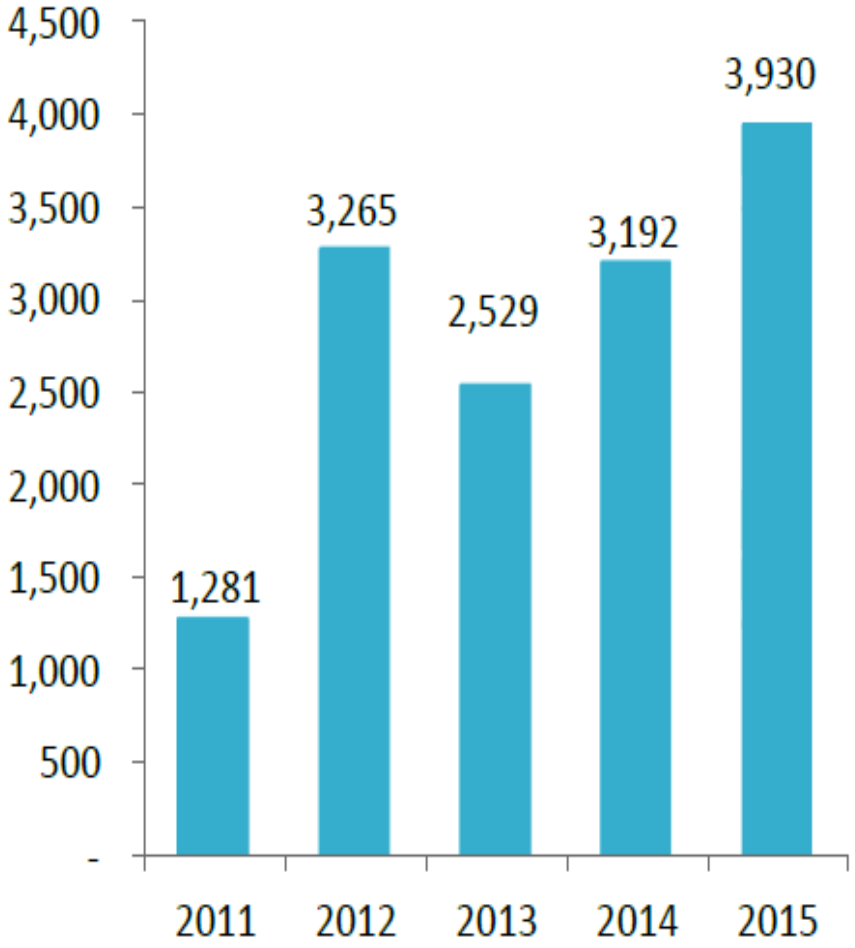

SAY CYBER
ONE MORE TIME
memegenerator.net



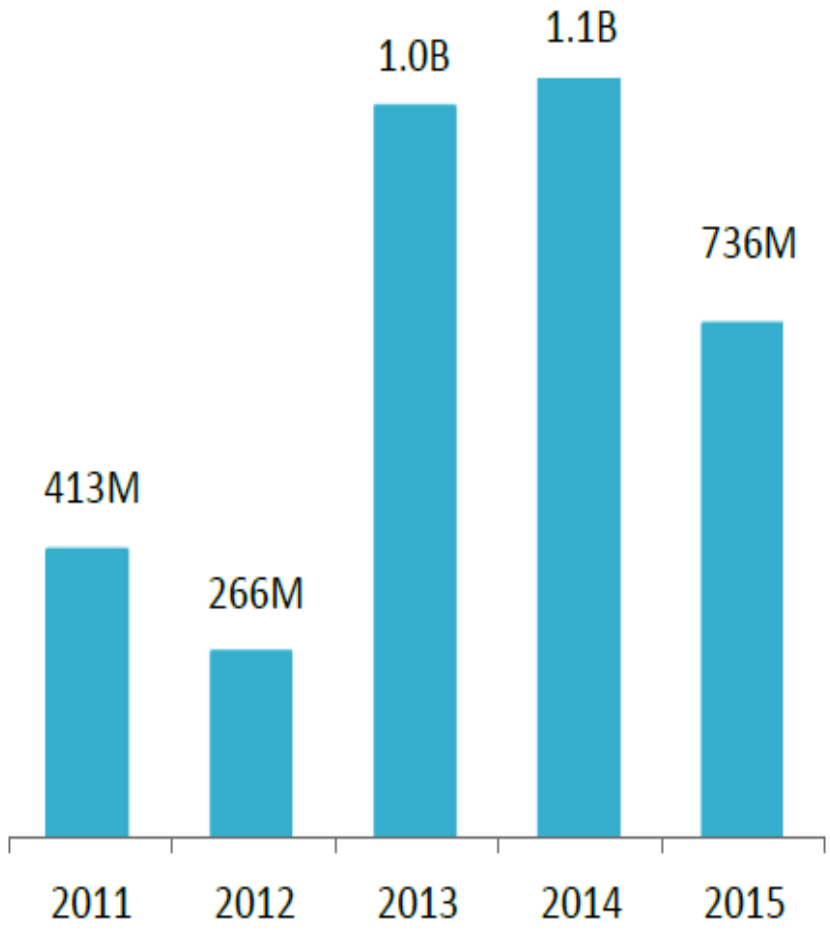

MUG
ROOT BEER
Root Beer
Stewart's
Barq's
A&W
ROOT BEER

Looking Back At The Last Five Years

Number of Incidents

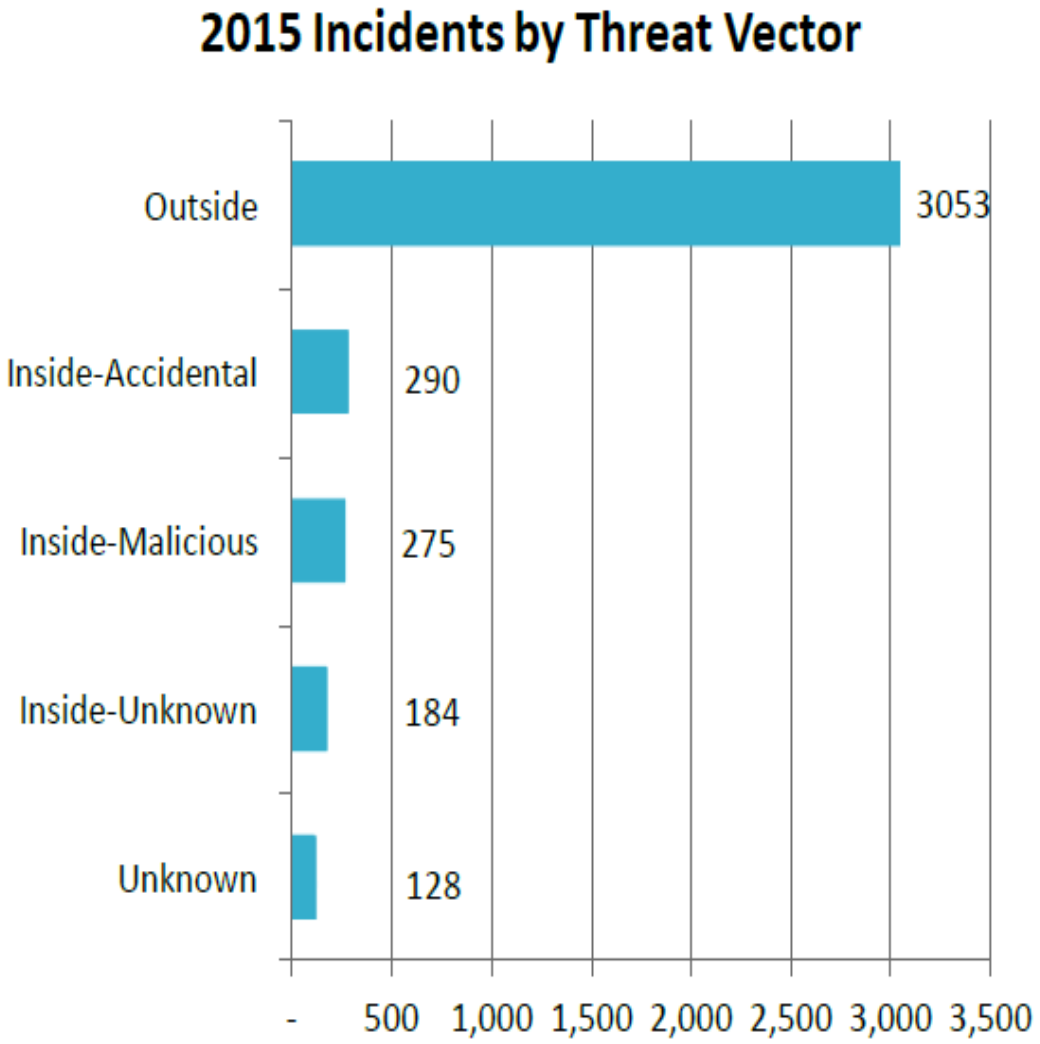


Number of Records Exposed



Source: CyberRiskAnalytics.com

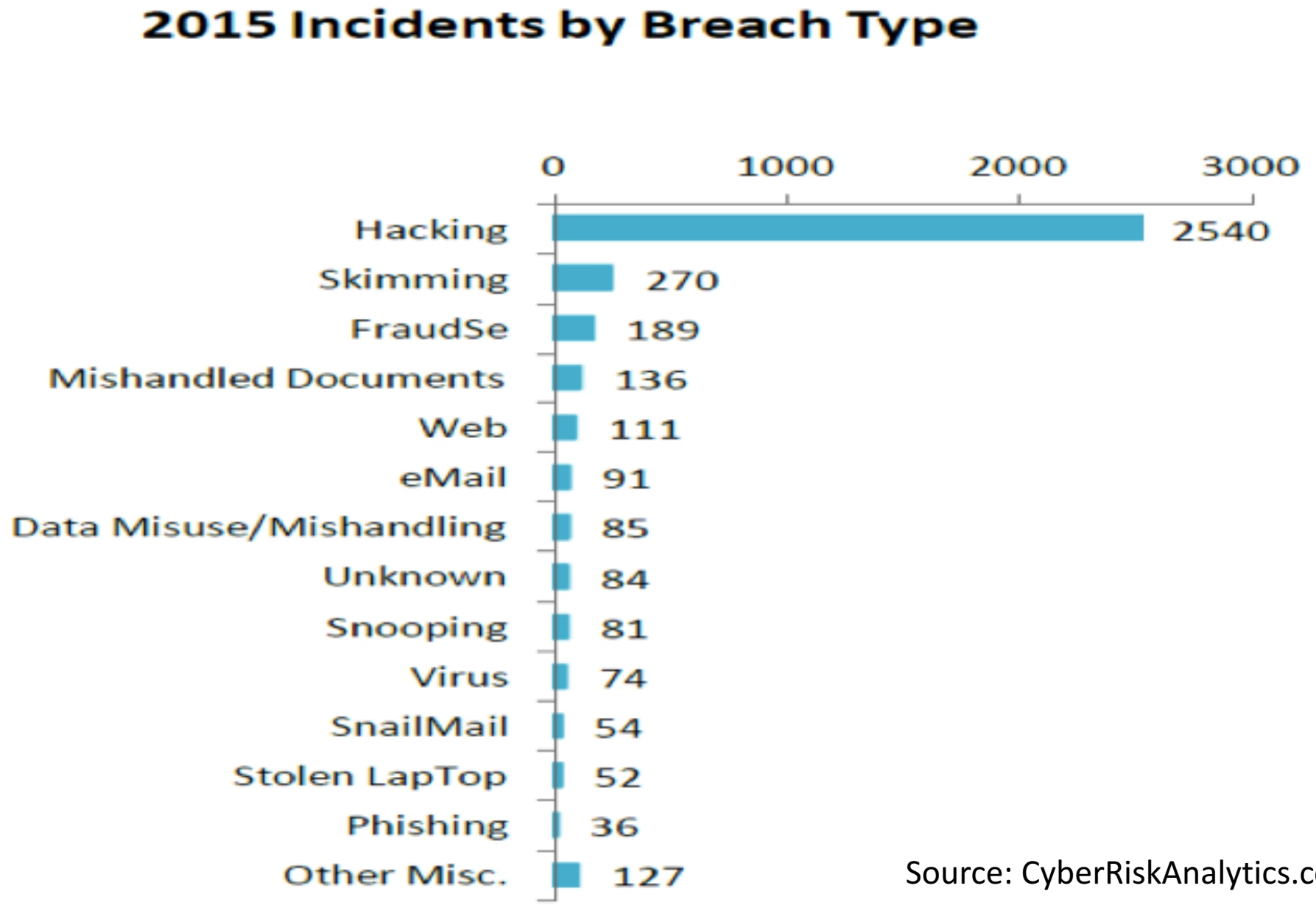
2015 – Threat Vector



77.7% of incidents involved outside the organization activity.

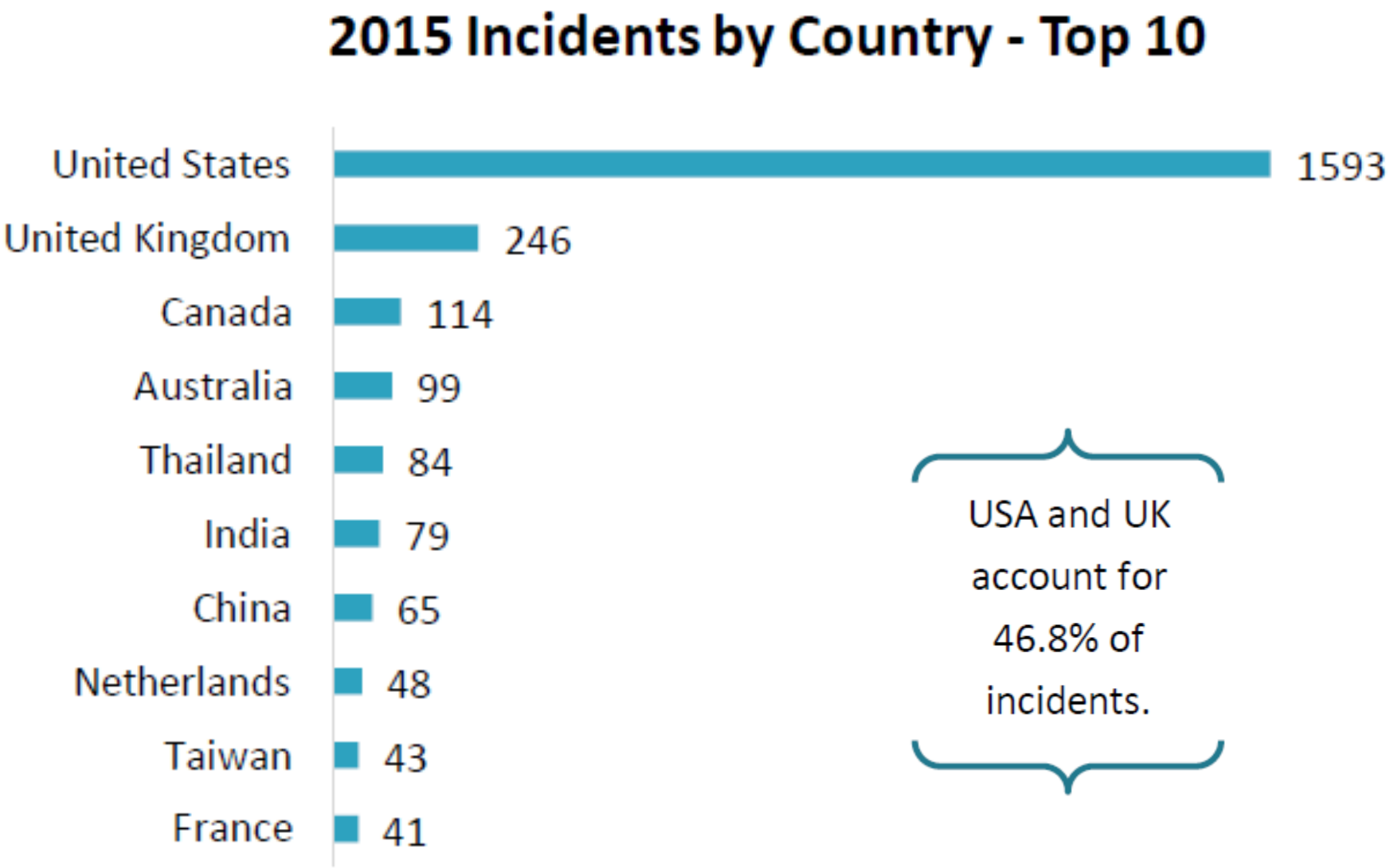
Source: CyberRiskAnalytics.com

2015 - Breach Types



Source: CyberRiskAnalytics.com

2015 Analysis – Country By Records



Source: CyberRiskAnalytics.com

2016 Year To Date

RiskBased SECURITY

2,000+

reported data breaches

1.1+ Billion

exposed records

Who is behind all of these data breaches?

Attribution

What Does This Really Mean?



What is Attribution?

- In social psychology, **attribution** is the process by which individuals explain the causes of behavior and events.
- **Attribution** in copyright law, is acknowledgement as credit to the copyright holder of a work.
- The **attribution** of information to its Source (journalism)

Source: Wikipedia

Cyber Attribution



Cyber Attribution



Cyber Attribution



Why Do People Care About Attribution?

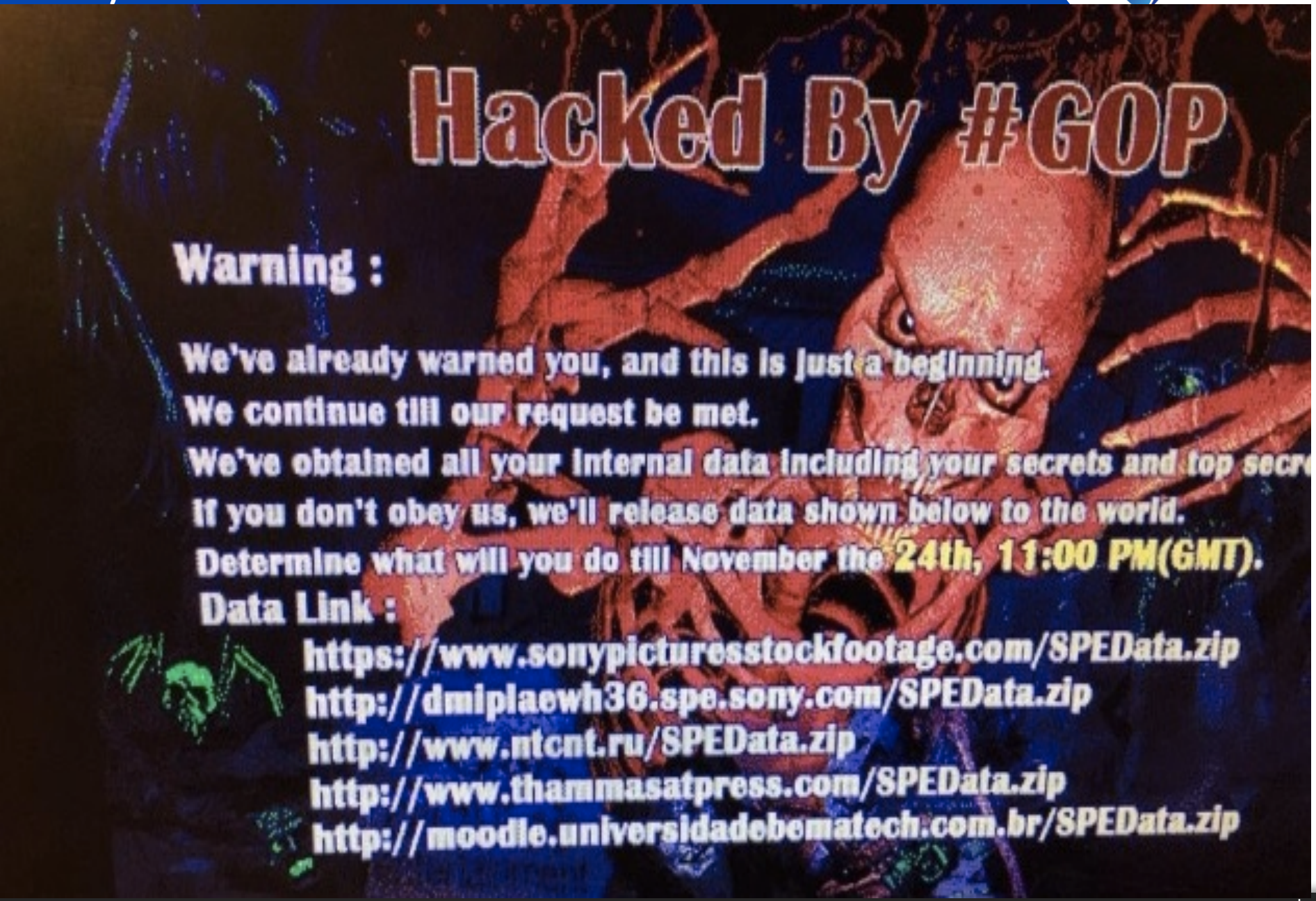


Why Do People Care About Attribution?

Attribution is power.

Jeff Rich

Sony Pictures - The Interview



Cyber War Attribution

Tweet

Attribution is hard, but playing Cyber War Attribution bingo is fun and easy!

Want to generate your own? Click Here!

Stay up to date by reading A Breakdown and Analysis of the December, 2014 Sony Hack.

Check out the Sony Hack Attribution Generator.

We would love to see some more versions (with flags instead of the country names) of the cyber war attribution cards!

Submit your version of a bingo card to cyberwar@riskbasedsecurity.com

Attribution Bingo

Vietnam	France	Saudi Arabia	Corp HackBack	Germany
Canada	Iraq	Poland	Script Kiddies	Russia
United Kingdom	Turkey	RiskBased SECURITY Free Space	Insider Threat	Dreaded APT
Japan	Ukraine	North Korea	USA	Kazakhstan
Third Party	Romania	Brazil	China	Hacktivists

Cyber War Attribution by Risk Based Security.

RiskBased SECURITY

Sony Hack Attribution Generator

RiskBased SECURITY

sony.attributed.to

TLP: White

Sony breach linked to Sony manager

Executive Summary

On November 24, 2014, personally identifiable information about Sony Pictures Entertainment (SPE) employees and their dependents, e-mails between employee executive salaries at the company, copies of unreleased Sony films, and other information, was obtained and released by a hacker group going under the monike Peace" or "GOP".

Although the motives for the hack have yet to be revealed, the hack has been tied to the planned release of the film The Interview, which depicts an assassination Korean leader Kim Jong-un, with the hackers threatening acts of terrorism if the film were to be released.

Recently, a team of 10 researchers from McAfee, Secunia, Mandiant/FireEye, Fortinet, Microsoft, iSIGHT Partners, Norse, Dell SecureWorks, Qualys, and Veracod evidence left behind by the attackers. This research has provided insight into the likely source of these attacks. Though not definitive, our analysis provides a muc suggests a Sony manager operating out of the People's Republic of China is responsible for the data breach impacting Sony Pictures Entertainment. This diclosu doubt on the FBI's assertion that the attack was carried out by state-sponsored actors under the control of North Korea, a theory that has been all but discredited security professionals since the attack became public, including White House security consultant August Alberty.

> Regardless of what my employer may say, this cannot be the work of North Korea.
>
> — August Alberty, White House security consultant

The research team is quite certain, however, that the Guardians of Peace hacker group played no role in this attack. The clues left behind confirm that the group c were a fabrication to throw investigators off the trail and to mask the true source.

Links to China

The research team was able to reconstruct the attack from the ground up and discovered a number of IP addresses that are linked to other attacks that have bee in China as well as the presence of Chinese text in the comment strings of the malware that was recovered during the forensic investigation. Some of these malw also been used in Chinese attacks.

Additional signals intelligence acquired by the research team has also implicated an actor based in China. This intelligence is highly classified and cannot be relea

Sony Hack Attribution Generator

RiskBased SECURITY

sony.attributed.to

TLP: White

Sony breach linked to Romanian organized criminal group

Executive Summary

On November 24, 2014, personally identifiable information about Sony Pictures Entertainment (SPE) employees and their dependents, e-mails between employ executive salaries at the company, copies of unreleased Sony films, and other information, was obtained and released by a hacker group going under the monik Peace" or "GOP".

Although the motives for the hack have yet to be revealed, the hack has been tied to the planned release of the film The Interview, which depicts an assassinati Korean leader Kim Jong-un, with the hackers threatening acts of terrorism if the film were to be released.

Recently, a team of 10 researchers from Norse, Cyphort, Arbor Networks, Palo Alto Networks, Qualys, and Kaspersky Labs examined the evidence left behind b research has provided insight into the likely source of these attacks. Though not definitive, our analysis provides a much clearer picture and suggests an organi operating out of Romania is responsible for the data breach impacting Sony Pictures Entertainment. This diclosure casts further doubt on the FBI's assertion th carried out by state-sponsored actors under the control of North Korea, a theory that has been all but discredited by a host of security professionals since the a including well-known Wired columnist Kim Zetter.

> I have statements from anonymous official sources stating that the evidence linking this attack to North Korea are dubious at best another source is behind the attack.
>
> — Kim Zetter, well-known Wired columnist

The research team is quite certain, however, that the Guardians of Peace hacker group played no role in this attack. The clues left behind confirm that the group were a fabrication to throw investigators off the trail and to mask the true source.

Links to Romania

The research team was able to reconstruct the attack from the ground up and discovered a number of IP addresses that are linked to other attacks that have be in Romania as well as the presence of Romanian text in the comment strings of the malware that was recovered during the forensic investigation. Some of thes have also been used in Romanian attacks.

Sony Hack Attribution Generator

RiskBased SECURITY

sony.attributed.to

load this page

TLP: White

Sony breach linked to North Korean organized criminal group

Executive Summary

On November 24, 2014, personally identifiable information about Sony Pictures Entertainment (SPE) employees and their dependents, e-mails between employees, executive salaries at the company, copies of unreleased Sony films, and other information, was obtained and released by a hacker group going under the moniker "G Peace" or "GOP".

Although the motives for the hack have yet to be revealed, the hack has been tied to the planned release of the film The Interview, which depicts an assassination at Korean leader Kim Jong-un, with the hackers threatening acts of terrorism if the film were to be released.

Recently, a team of 9 researchers from RSA, Adallom, Arbor Networks, iDefense, and Proofpoint examined the evidence left behind by the attackers. This research h insight into the likely source of these attacks. Though not definitive, our analysis provides a much clearer picture and suggests an organized criminal group operatin Democratic People's Republic of Korea is responsible for the data breach impacting Sony Pictures Entertainment. This diclosure casts further doubt on the FBI's ass attack was carried out by state-sponsored actors under the control of North Korea, a theory that has been all but discredited by a host of security professionals sinc became public, including noted security consultant Dan Tentler.

> So far all I'm seeing is 'it's gotta be NK because', and not like 'oh look, legit evidence indicating NK'. Just lots of arm waving.
>
> — Dan Tentler, noted security consultant

The research team is quite certain, however, that the Guardians of Peace hacker group played no role in this attack. The clues left behind confirm that the group clai were a fabrication to throw investigators off the trail and to mask the true source.

Links to North Korea

The research team was able to reconstruct the attack from the ground up and discovered a number of IP addresses that are linked to other attacks that have been a in North Korea as well as the presence of North Korean text in the comment strings of the malware that was recovered during the forensic investigation. Some of the samples have also been used in North Korean attacks.

Additional signals intelligence acquired by the research team has also implicated an actor based in North Korea. This intelligence is highly classified and cannot be r

WhoHackedUs.com

RiskBased SECURITY

whohackedus.com

RENDITION INFOSEC

Cyber Attack Attribution Report

Country: China
APT Group Name: CROUCHING PANDA HIDDEN DRAGON



Attack Vector: Wordpress
Malware Used: Cryptlocker!g43
Data lost in the breach: Customer Records
Who's to blame? Management
Who's getting fired? Board of directors
Contributing factors/excuses: Budget Reduction
Will Fox News call it "Cyber Terrorism?" No, bigger news to air that day.
Will we be targeted again? Yes
Cost of the data loss: $100,001.01
How much did you save using this tool for attribution? You saved a puppy, a real live puppy
Click here for permalink to these results (Export to PDF available from permalinked page)

Share 24 | Share 4 | Tweet | Follow @RenditionSec

RiskBased SECURITY

Cyber Attribution

"Don't waste money on high priced forensic investigations.... Just roll the dice!"

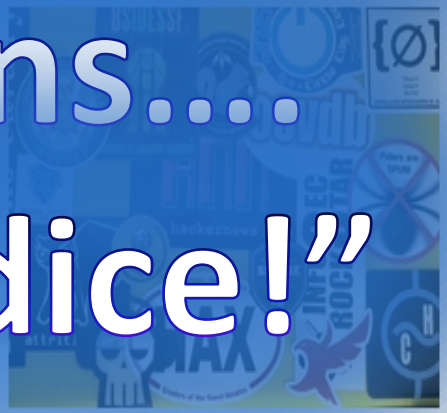
Dice

Stickers

Shopping Bag
Drag & Drop Products Here
Open Bag



Dice



Stickers

Cyber Attribution Dice



Matt Harvey
@packetdude

Follow

Cyber attack attribution dice.
cyberattribution.com/#!/Country-Att ... - This needs to be done as a "magic 8 ball"



8:55 PM - 16 Mar 2015

Attribution 8 Ball



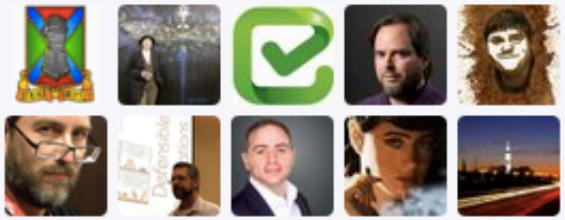
Attribution 8 Ball
@InfoSec8Ball

Got a breach that needs attribution? Got you covered!

Joined February 2015

Tweet to Attribution 8 Ball

10 Followers you know



TWEETS 83 | FOLLOWING 764 | FOLLOWERS 194 | LIKES 4

Tweets | Tweets & replies



Attribution 8 Ball @InfoSec8Ball · 5 Jun 2015
Attention, I have an announcement....China!
1 2



Attribution 8 Ball @InfoSec8Ball · 16 Apr 2015
I foresee a breach announcement coming soon. Seeing too many new CCs numbers. My guess is hospitality industry this time.



Attribution 8 Ball @InfoSec8Ball · 15 Apr 2015
You guys haven't seen anything yet. It's about to get real.
1

Attribution 8 Ball - Duo



Attribution 8 Ball - SecuriTay



Attribution 8 Ball - Threatbutt



Sony Pictures - The Interview



Sony Pictures - The Interview – Who?





CROWDSTRIKE

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY

NORSE





Norse - Sony

- While Norse is not involved in the Sony case, it has done its own investigation, and stated "We are very confident that this was not an attack sponsored by North Korea and that insiders were key to the implementation of one of the most devastating attacks in history." Stamminberger says Norse data is pointing towards a woman who calls herself "Lena" and claims to be affiliated with the "Guardians of Peace" hacking group. Norse believes it has identified this woman as someone who worked at Sony in Los Angeles for ten years until leaving the company in May.

"We are very confident that this was not an attack master-minded by North Korea."





Marc Rogers

Why attribution of North Korea in the Sony case worries me.

Attribution is hard. Out of all the digital forensic disciplines, it is probably the hardest. Digital forensics is nothing like what you see on TV – on so-called cyber-CSI shows, the investigator types in a few magical keystrokes and evidence comes flooding out of the completely unlocked computer. A few more keystrokes and a magical [...]

8

Why I *still* dont think it's likely that North Korea hacked Sony.

So the FBI has come out and said it. North Korea was behind the Sony hack. With some pretty strongly worded rhetoric, they lay out exactly why they feel confident enough to lay the blame for this criminal act at the doorstep of a foreign nation. Finally, they express their deep concern about how these [...]

19

Why the Sony hack is unlikely to be the work of North Korea.

Everyone seems to be eager to pin the blame for the Sony hack on North Korea. However, I think it's unlikely. Here's why:1. The broken English looks deliberately bad and doesn't exhibit any of the classic comprehension mistakes you actually expect to see in "Konglish". i.e it reads to me like an English speaker pretending [...]

112

http://marcrogers.org/2014/12/18/why-the-sony-hack-is-unlikely-to-be-the-work-of-north-korea/

Kim Zetter – Sony

KIM ZETTER SECURITY 12.17.14 5:32 PM

THE EVIDENCE THAT NORTH KOREA HACKED SONY IS FLIMSY



How should the U.S. government respond to North Korea's attack on Sony?

December 19, 2014 at 6:40 PM EDT



President Obama told the White House Press Corps that Sony was wrong to withdraw its film, "The Interview," and that the U.S. would react "proportionally" to the damaging cyber-attack by North Korea. Judy Woodruff turns to Dmitri Alperovitch of CrowdStrike and Jack Pritchard, the former U.S. special envoy for negotiations

SUPPORT FOR PBS NEWSHOU
shop PBS
15% OFF
Mystery Tit
SHOP NOW
INSPECTOR LEWIS
Grantchester
Your purchase supports PBS p

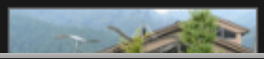
MORE VIDEO



News Wr
throat-sl
priest



How Ven
economi
environn



News Wr

PBS - Cyber Attribution Debate Live!



FBI - Sony

RiskBased SECURITY

> NEWS > PRESS RELEASES > PRESS RELEASES

FBI

Search FBI

NEWS

Stories | Videos | Press Releases

Washington, D.C.
FBI National Press Office
(202) 324-3691

Email

December 19, 2014

Update on Sony Investigation

Today, the FBI would like to provide an update on the status of our investigation into the cyber attack targeting Sony Pictures Entertainment (SPE). In late November, SPE confirmed that it was the victim of a cyber attack that destroyed systems and stole large quantities of personal and commercial data. Shortly thereafter, a self-proclaimed group of individuals calling themselves the "Guardians of Peace" claimed responsibility for the attack and issued threats against SPE, its employees, and theaters that distribute its movies.

The FBI has determined that the intrusion into SPE's network consisted of the deployment of destructive malware and the theft of proprietary information as well as employees' personally identifiable information and other data from SPE's servers. The attacks also rendered thousands of SPE's computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company's business operations.

After discovering the intrusion into its network, SPE requested the FBI's assistance. Since then, the FBI has been working closely with the company throughout the investigation. Sony has been a great partner in the investigation, and continues to work closely with the FBI. Sony reported this incident within hours, which is what the FBI hopes all companies will do when facing a cyber attack. Sony's quick reporting facilitated the investigators' ability to do their jobs, and ultimately to identify the source of these attacks.

"… the FBI now has enough information to conclude that the North Korean government is responsible.."

Lots of Debate – Main Two Players!







Who Is Right? Who Is Wrong?

If evidence ends up being released, and there is clear attribution, how will this impact companies like Norse and Crowdstrike that have made such bold statements? If a company making this statement is blatantly wrong, does that suggest threat intelligence they sell can't be trusted or relied on by corporations?

If a company making this statement is blatantly wrong, does that suggest threat intelligence they sell can't be trusted?



A Breakdown and Analysis of the December, 2014 Sony Hack

The Beginning (November 24)
Second Round of Leaks (December 3)
The Analysis Continues (December 7)
Fifteen Days Under Siege (December 8)
Reality and the Blame Game (December 9)
My Life At The Company, Part 1 (December 10)
Another Day, Another Email Spool (December 10)

FBI Defends Sony Hack Attribution

N. Korean Hackers 'Got Sloppy' During Attack, FBI Director Says

Jeffrey Roman (gen_sec) • January 7, 2015 0 Comments

Twitter Facebook LinkedIn Credit Eligible Get Permission



FBI Director James Comey

In a Jan. 7 speech, FBI Director **James Comey** highlighted a bit of evidence to defend his agency's conclusion that North Korea was behind the cyber-attack on **Sony Pictures Entertainment**.

Krebs on Norse Imploding

RiskBased SECURITY

KrebsonSecurity
In-depth security news and investigation



BLOG ADVERT

30 Sources: Security Firm Norse Corp. Imploding

JAN 16

Norse Corp., a Foster City, Calif. based cybersecurity firm that has attracted much attention from the news media and investors alike this past year, fired its chief executive officer this week amid a major shakeup that could spell the end of the company. The move comes just weeks after the company laid off almost 30 percent of its staff.

Sources close to the matter say **Norse CEO Sam Glines** was asked to step down by the company's board of directors, with board member **Howard Bain** stepping in as interim CEO. Those sources say the company's investors have told employees that they can show up for work on Monday but that there is no guarantee they will get paid if they do.



Advertisement



My New



Norse @ RSA



Iftach Ian Amit
@iiamit

Following

Sadness defined: how can we spend the least about of money on the premium both space we already paid for? @NorseCorp



RETWEETS 14 LIKES 8

12:23 PM - 2 Mar 2016

Norse – Attack Map



Threatbutt Hacking Attack Attribution Map

RiskBased SECURITY

Threatbutt Internet Hacking Attack Attribution Map

About Threatbutt Internet Hacking Attack Attribution Map



By leveraging our patented **Clown Strike** technology we are able to harness the raw power of private, hybrid, public and cumulus cloud system to bring Viking grade threat intelligence to any enterprise.

And we made it into a map.

(Powered by pewpew, even though we made it more accurate because we are a company that does the best threat stuff.)

sa (136.140.115.34) uses Bad BIOS against usa (163.176.101.255) -- UPGRADE TO PREMIUM FOR MORE INFO$
us (115.42.252.204) uses PRE-PATCH HYPE against can (222.21.208.182) -- We'll just call it a "glitch"
sa (71.21.0.175) uses WordPress plugins against sau (221.95.232.28) -- IT'S CYBER POMPEII !
pn (18.207.206.70) uses QUANTUM LEAP against rus (13.69.25.122) -- it didn't work so good

Cyber Attribution

Why Is It So Hard?



Attribution Is Hard

- Cyberspace does have some unique attributes which are not mirrored in the real world.
  - Typical CSI forensic / investigation work not possible
- Easy to "spoof" evidence
- Easy to use or embed others work (tools, exploits, malware)
  - Just because it was used doesn't mean that it was same people
  - It could easily be used by different people/groups
- Nonexistence of physical "territory"
  - Some attribution markers used in other areas such as warfare are missing.
  - Hackers typically don't need an 'assembly zone' that can be detected and watched.
  - No ground boundary needs to be crossed
  - No way to track back a "missile" launch without question

DNC Hack



Give Hillary Money For Cybersecurity

RiskBased SECURITY

Hillary Act Issues Shop More Español Donate

WED, AUG 3, 2016, 6:00PM - 8:00PM

Hillary for America Cybersecurity Fundraiser at Black Hat with Jeff Moss, Michael Sulmeyer, and Jake Braun

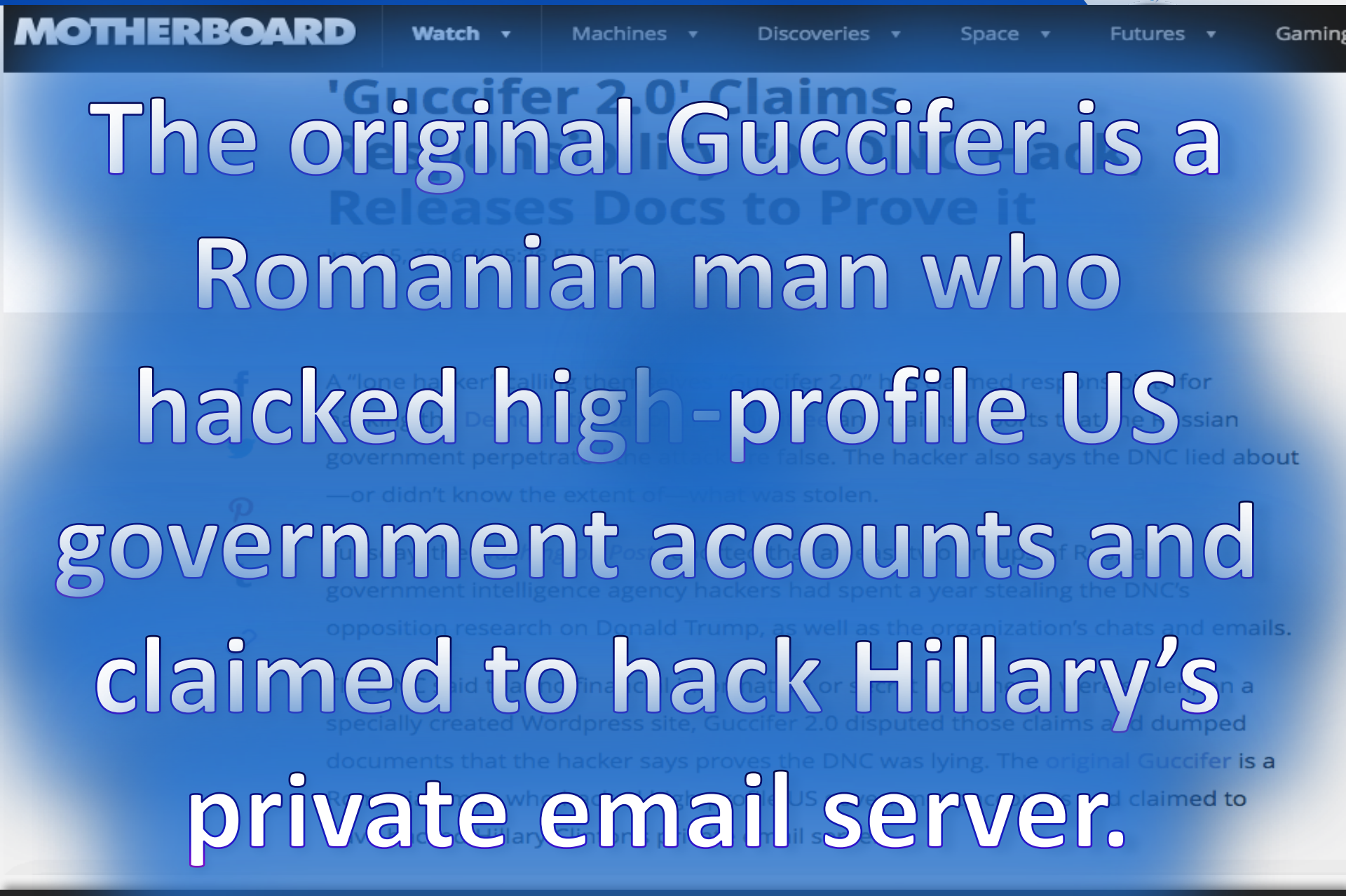
See more details

1 2 3 TICKET SELECTION SECURE

First name Last name



DNC – Attribution – Guccifer

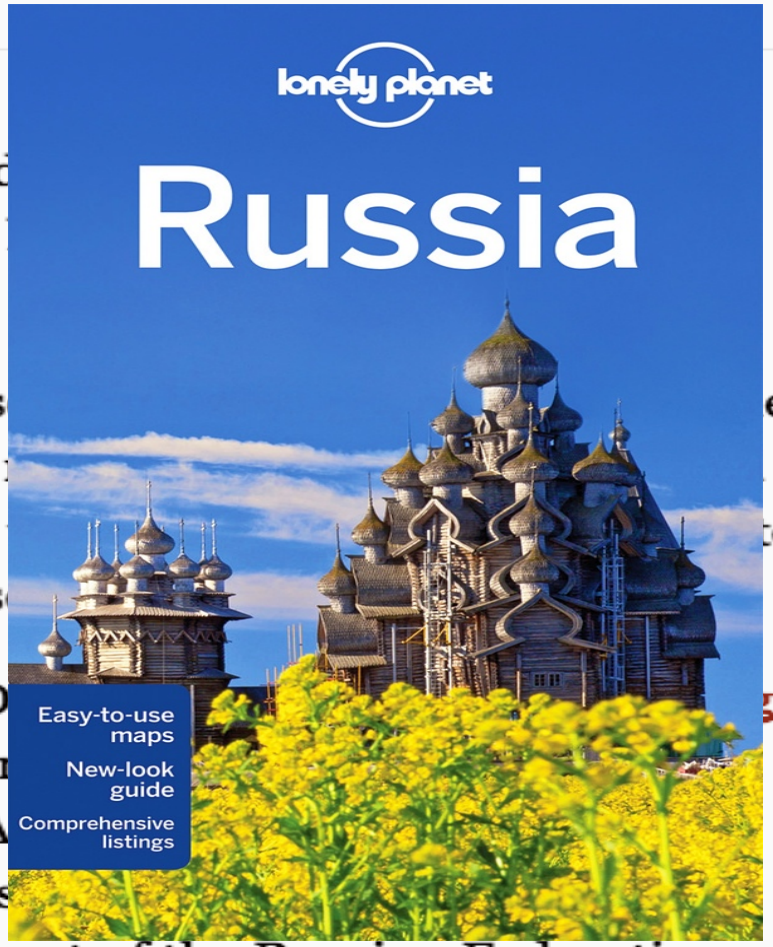


The original Guccifer is a Romanian man who hacked high-profile US government accounts and claimed to hack Hillary's private email server.

DNC – Attribution - Russia

DNC hack raises questions about cyber attribution methods





by M

The ted
Rus er
cybe

The t s e
Den C)
Cro te ter
that rs

Dmi TO
post der
adv EA
that ens

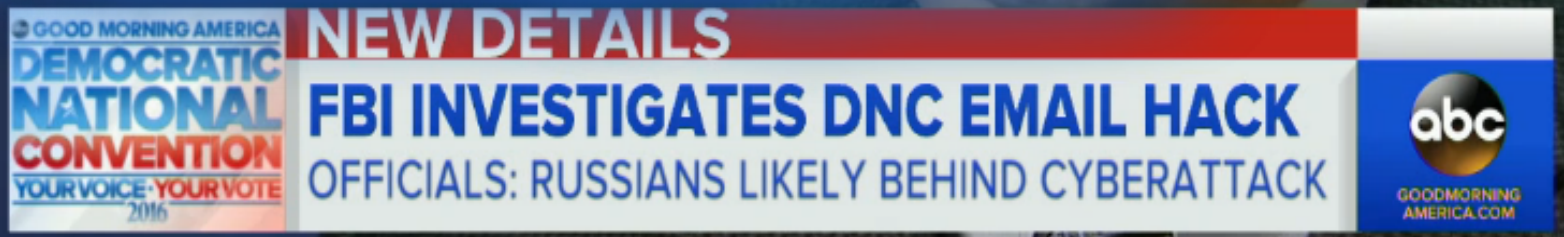
espionage for the benefit of the government of the Russian Federation and are believed to be closely linked to the Russian government's powerful and highly capable intelligence services."

Who's Behind Massive DNC Email Hack?

More

Fidelis is also very confident it is Russian actions due to:

- They looked at code
- Use of Russian Alphabet keyboard
- Timezones complied in



DNC – Attribution – Person or Russia?

RiskBased SECURITY

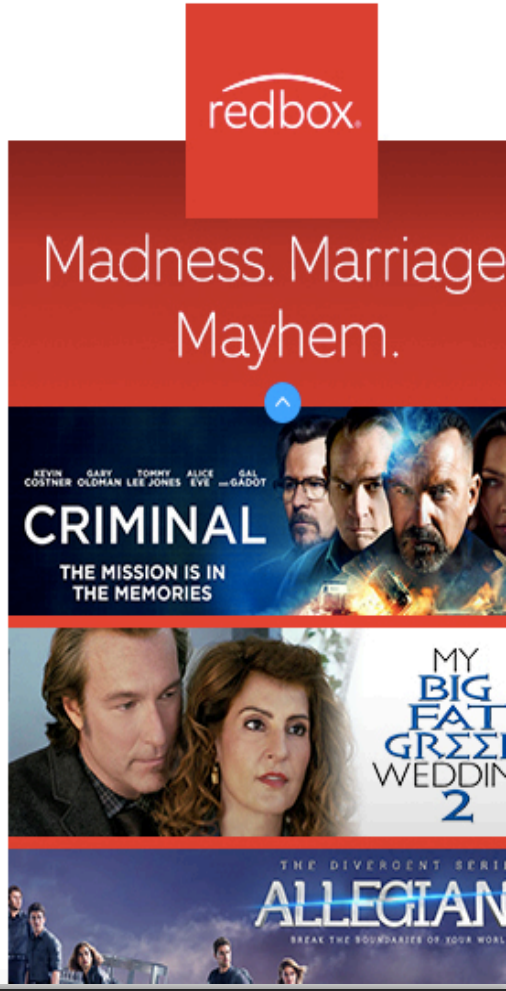
Is D.N.C. Email Hacker a Person or a Russian Front? Experts Aren't Sure

By CHARLIE SAVAGE and NICOLE PERLROTH JULY 27, 2016

WASHINGTON — Who is Guccifer 2.0, the self-proclaimed Romanian "lone hacker" responsible for copying thousands of emails and other files from the Democratic National Committee — a real person, or a front created by Russian intelligence officials?

Technology specialists have been debating that question since June 15, when CrowdStrike, a cybersecurity firm hired by the Democratic National Committee, announced that sophisticated hacker groups with Russian links were responsible for breaching the committee's computer servers. Within hours of the announcement, someone using the moniker Guccifer 2.0 started a blog to mock that finding, posting several of the stolen documents and claiming sole credit.

But the publication by WikiLeaks of an archive of the committee's internal emails — and the uproar they caused on the eve of the Democratic National Convention — have focused wider attention on who, or what, is operating behind that name. While WikiLeaks has not said how it obtained the emails, Guccifer 2.0 claimed in a blog post last month to have sent them to WikiLeaks.



DNC – Russia – Hack Back

Clinton says Russia behind DNC hacking, draws line to Trump

WASHINGTON | BY DOINA CHIACU AND ROBERTA RAMPTON



Democratic presidential candidate Hillary Clinton speaks at the David L. Lawrence Convention Center in Pittsburgh, Pennsylvania, July 30, 2016.
REUTERS/AARON P. BERNSTEIN

BREAKINGVIEWS



Chinese investors placing huge bet online games



Russia cyber attack: Large hack 'hits government'

30 July 2016 | Europe

Share



The hack reportedly targeted a number of government bodies

A "professional" cyber attack has hit Russian government bodies, the country's intelligence service says.

A "cyber-spying virus" was found in the networks of about 20 organisations, the Federal Security Service (FSB) said.

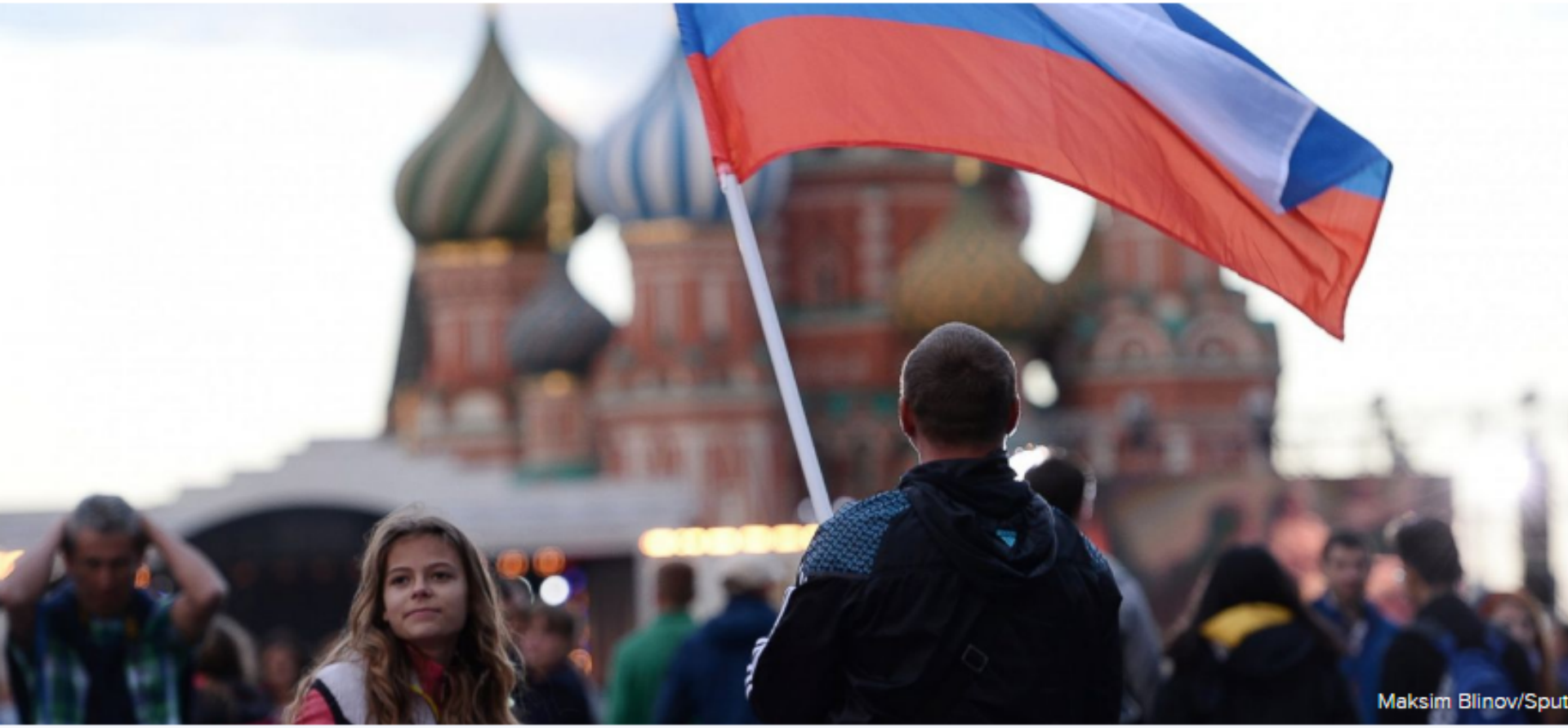
DNC – Russia – Hack Back

RiskBased SECURITY

The NSA Is Likely 'Hacking Back' Russia's Cyber Squads

By LEE FERRAN · ASPEN, Colorado — Jul 30, 2016, 2:30 PM ET

Share with Facebook | Share with Twitter



CH | IP Address Linked Russia to DNC Hack, Expert Says

Does it actually matter that we get Cyber Attribution correct?

Attribution – North Korea

Sony cyber-attack: North Korea faces new US sanctions

3 January 2015 | US & Canada

Share



The White House said the cyber-attack was an attempt by North Korea to restrict free expression

The US has imposed new sanctions on North Korea in response to a cyber-attack against Sony Pictures Entertainment.

Congress sends North Korea cyber sanctions bill to Obama

8 1 COMMENTS 0



Getty Images

By Cory Bennett - 02/12/16 03:25 PM EST

A bill to sanction North Korea for its burgeoning cyber warfare efforts is headed to President Obama's desk.

The House on Friday **approved** the North Korea Sanctions Policy and Enhancement Act, which would mandate penalties on those caught aiding the country's nefarious cyber campaigns. The measure would also sanction individuals involved in Pyongyang's nuclear program or in the censorship of the regime's well-documented human rights abuses.

Attribution – North Korea

Now that the U.S. declared a war on the DPRK, any problem arising in the relations with the U.S. will be handled under the latter's wartime law..."



U.S. considers economic sanctions against Russia for hacking

Public attribution would multiply the impact of such sanctions on Russian officials, says one policy expert.



By *Chris Bing*
AUGUST 3, 2016 7:30 PM

BIO



(iStockphoto)

The White House is considering the use of economic sanctions to punish the Russian government for their "nefarious activities in cyberspace," according to a statement from White House Press Secretary Josh Earnest on Wednesday.

"[Economic sanctions are] something that we have used before and could potentially be used in preparing a proportional response to cyber threats," said Earnest, answering a question regarding how the White

RiskBased SECURITY

So how can we actually figure out who is behind these "hacks"?

- No security firm typically agrees on who's done it
- Can't trust when people "claiming" attacks
- Easy to hide IP addresses via Proxy servers, TOR, etc.
- Correlations between certain pieces of malware isn't hard evidence (debatable)
- Information (evidence) not shared to protect sources
- Using a "behavioral analysis unit" of FBI experts trained to psychologically analyze foes based on their writings and actions isn't hard evidence

Do we need to improve our Cyber Attribution Capabilities?

Can We Improve?



Arrest Tracker

What Is It?



Arrest Tracker



Founded by Lee Johnstone

- –Security Researcher
- –Founder Cyber War News





Arrest Tracker

- Arrest Tracker (https://arresttracker.com/)
  - Started in 2013 by Lee J
  - The project aims to track computer intrusion incidents resulting in an arrest, detaining of a person or persons, seizure of goods, or other related activities that are directly linked to computer crimes.
- Track incidents from all types of "cyber" crime (drink!) and hacking related incidents.
- The Arrest Tracker project currently has 1,431 incidents collected as of 7/29/2016.
- More than just "arrests", Cyber Crime Incident Tracker
- Project is officially launching as of today!

Arrest Tracker - Fields

RiskBased SECURITY

Profile

- Name
- Alias
- Gender
- Age
- Wiki
- Twitter
- Location
- Collective
- Operation
- Occupation
- Active Since

Incident

- Incident Information
- Incident Date
- Incident Country
- Date of Crime
- Caught by
- Arrested
- Charged
- Custody
- Bail
- Wanted
- Raided
- Seized Items

Courts

- Deal
- Plead
- Extradited
- Trial
- Fined
- Fine Amount
- Fine Paid
- Restitution
- Convicted
- Convicted Date
- Sentenced
- Sentenced Date
- Sentenced Information
- Sentenced Months
- Sentenced Suspended
- Sentenced Probation
- Served
- Appeal

Legal

- Announcing Proscutor
- Judge
- Proscutor
- Lawyer
- Lawfirm

Authorites

- Authorites
- Authorites Operation
- Authorites Statement
- Authorites Assitance
- Informed on
- Informed on by
- Paid informant

Arrest Tracker

What Can It Help Us With?

Arrest Tracker Disclosures

We need to first recognize there are limitations with the data!

RiskBased SECURITY

We must also remember that this is based on mostly ARREST incidents, therefore it tells a story from that viewpoint.

Expanded to include more Cyber Crime and will continue to add more!

RiskBased SECURITY

We are using data based on reported arrests and raids.

We must also remember, in many cases, governments would rather track and follow criminals, rather than arrest them for various reasons.

What Can Arrest Tracker Tell Us?

- Provide detailed computer crime arrest information and statistics
- Who is behind these data breaches and cyber crime
- What are the demographics?
- Extraditions
- Details on Sentences
- Details on Monetary fines
- Learning about law enforcement
- Profile of a "hacker"
- More!

Face Of A “Hacker”



Face Of A “Hacker” – Google Images

RiskBased SECURITY

Google hacker

All News Images Videos Apps More Search tools View saved SafeSearch

anonymous | lizard squad | lulzsec | computer | android | laptop | phone | iphone | ps3 | background | security | matrix | system | software | data | white









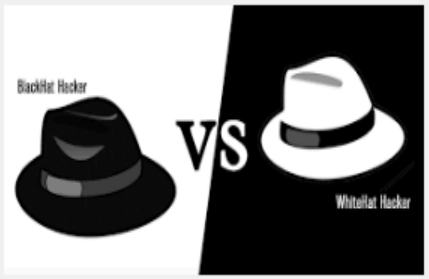












Face Of A “Hacker” – Mr Robot







Real Faces of Cyber Crime – Arrest Tracker

RiskBased SECURITY

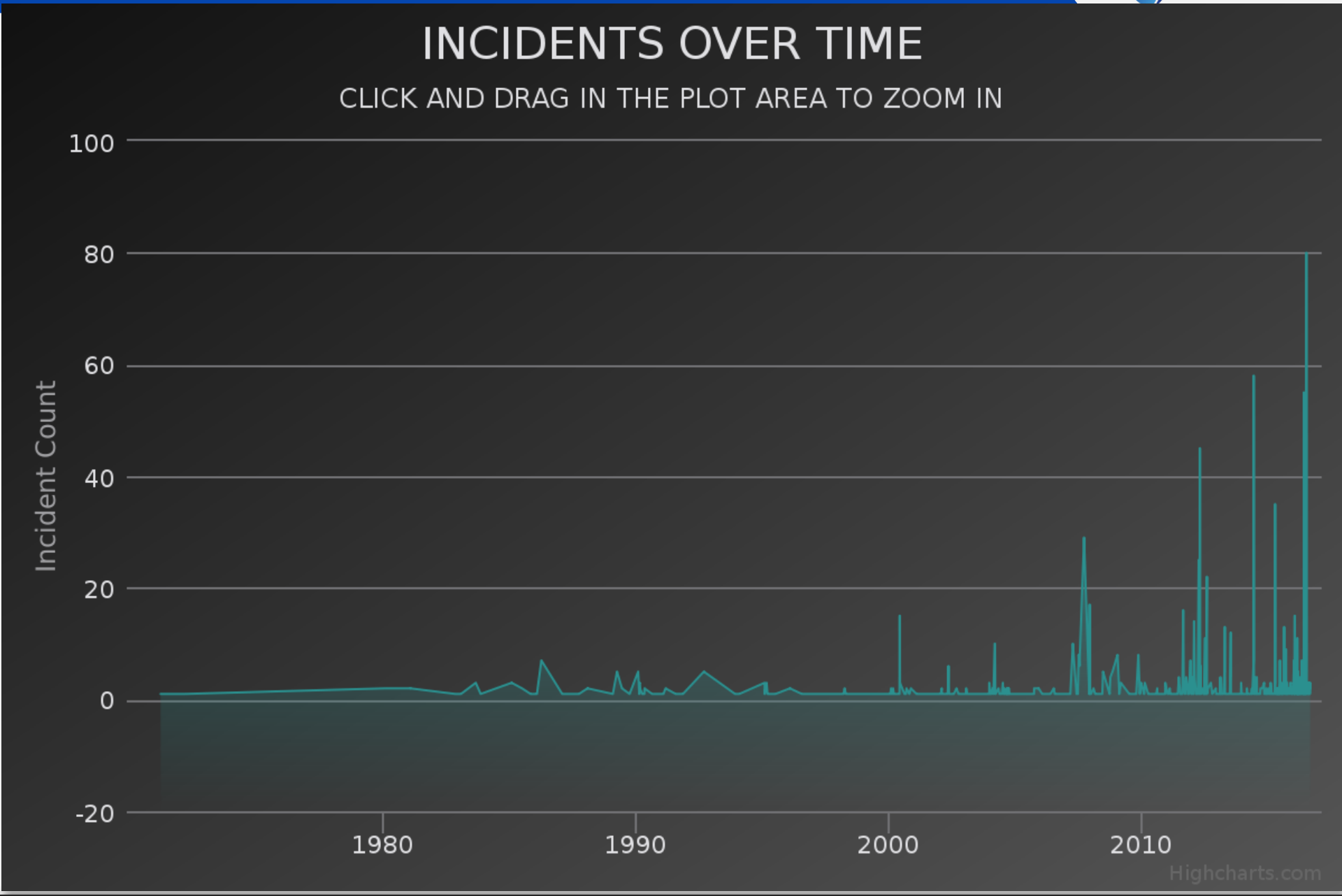


Cyber Arrests

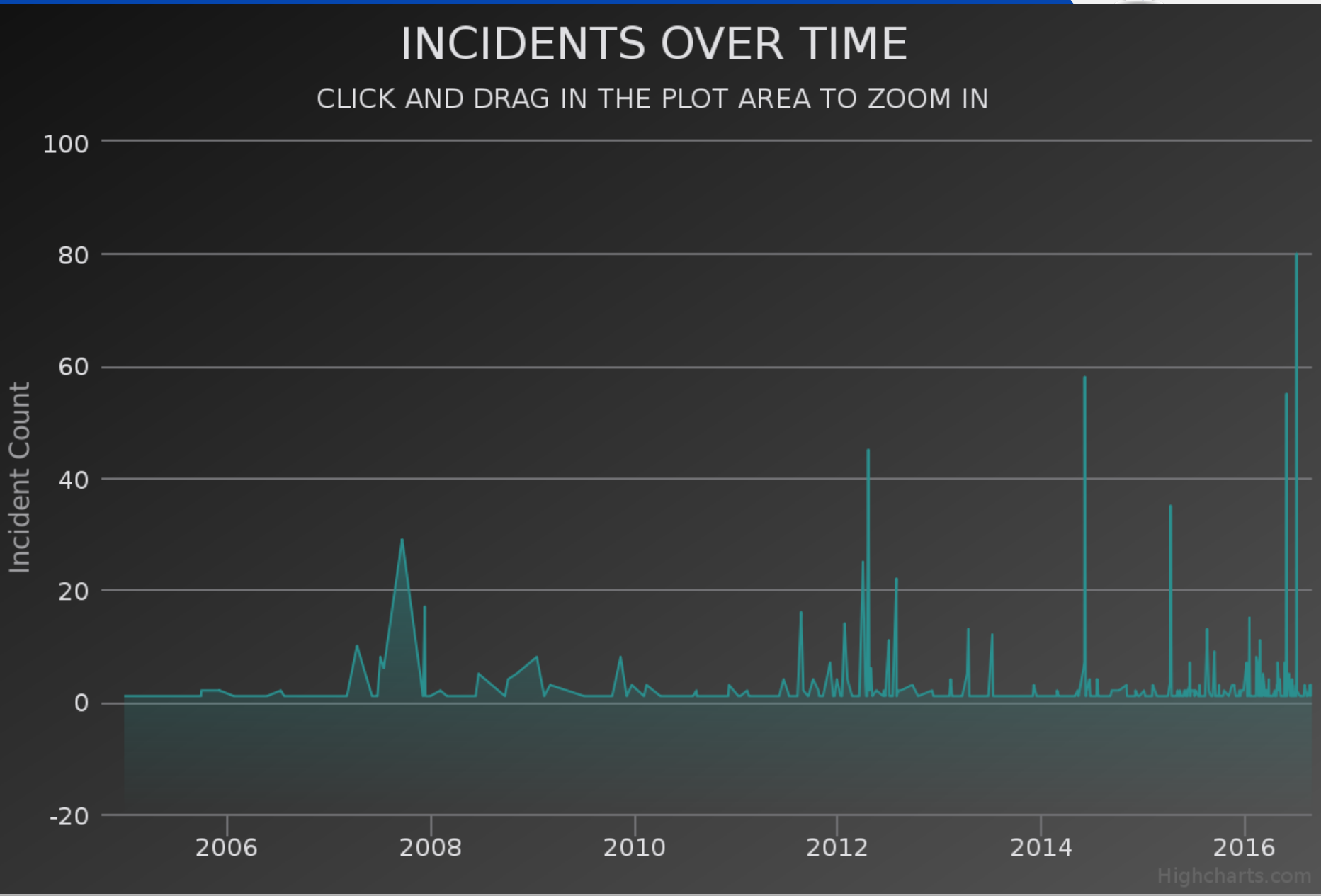
Timeline



Timeline


INCIDENTS OVER TIME
CLICK AND DRAG IN THE PLOT AREA TO ZOOM IN
Incident Count
100
80
60
40
20
0
-20
1980
1990
2000
2010
Highcharts.com

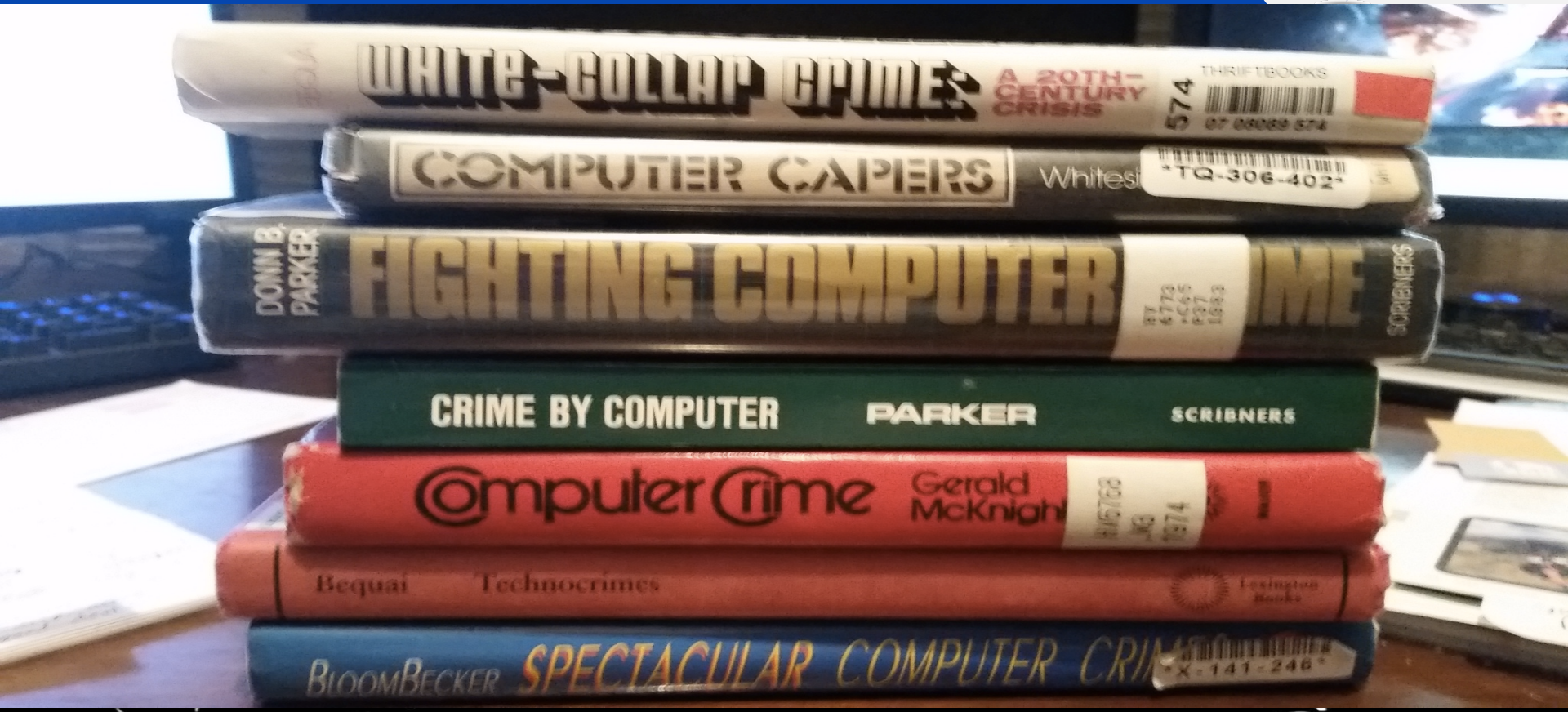
Timeline


INCIDENTS OVER TIME
CLICK AND DRAG IN THE PLOT AREA TO ZOOM IN
Incident Count
100
80
60
40
20
0
-20
2006
2008
2010
2012
2014
2016
Highcharts.com

Timeline

- Cyber Incidents in past decades:
  - 1970:'s 2 incidents
  - 1980:'s 37 incidents
  - 1990:'s 59 incidents
  - 2000:'s 345 incidents
  - 2010:'s 988 incidents

Early Crime Research





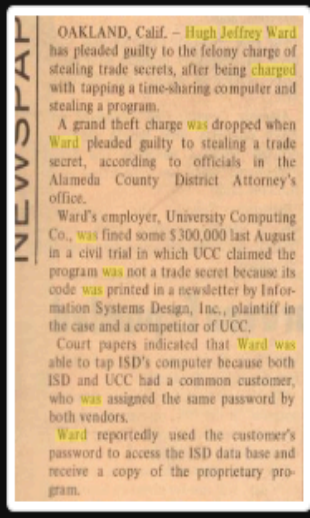
1970's - First Known Arrest

- Oldest Incident in Arrest Tracker is from 1971.
  - Hugh Jeffery Ward
  - 1971-02-19

Profile | Incident | Authorities | Courts | Legal | Groups | Sites | Orgs | Links | Documents | Updates

PROFILE

Name	Hugh Jeffery Ward
Alias	Eli Bart, Fred Darm
Gender	male
Age	29
Wiki	Hugh_Jeffery_Ward
Twitter	N/A
Location	United States
Collective	
Operation	
Occupation	IT
Active Since	0000-00-00



OAKLAND, Calif. – Hugh Jeffrey Ward has pleaded guilty to the felony charge of stealing trade secrets, after being charged with tapping a time-sharing computer and stealing a program.

A grand theft charge was dropped when Ward pleaded guilty to stealing a trade secret, according to officials in the Alameda County District Attorney's office.

Ward's employer, University Computing Co., was fined some $300,000 last August in a civil trial in which UCC claimed the program was not a trade secret because its code was printed in a newsletter by Information Systems Design, Inc., plaintiff in the case and a competitor of UCC.

Court papers indicated that Ward was able to tap ISD's computer because both ISD and UCC had a common customer, who was assigned the same password by both vendors.

Ward reportedly used the customer's password to access the ISD data base and receive a copy of the proprietary program.

Gallery



1970's - First Known Arrest

- Hugh Jeffery Ward
- Incident Occurred: 1971-02-19
- 29 years old at the time
- Accused of breaking into I.S.D computer systems and stealing data.
- Trade Secret Theft
- Plead Guilty
- Fined $5,000
- 36 Months of Probation

Most Friends On The Internet



Male
30 Years Old
CALIFORNIA
United States

Online Now!

Last Login:
3/11/2006

It's Tom!

1980's - MySpace Tom

RiskBased SECURITY

MySpace.com | Home The Web MySpace Search Help | SignOut

Home | Browse | Search | Invite | Film | Mail | Blog | Favorites | Forum | Groups | Events | Videos | Music | Comedy | Classifieds

Tom

":-)"



Male
30 years old
Santa Monica, CALIFORNIA
United States

Last Login: 8/27/2006

View My: **Pics** | **Videos**

Contacting Tom

Send Message | Forward to Friend
Add to Friends | Add to Favorites
Instant Message | Block User
Add to Group | Rank User

MySpace URL:
http://www.myspace.com/tom

Tom is in your extended network

Tom's Latest Blog Entry [**Subscribe to this Blog**]

private profiles (**view more**)

Top 8, 16, 20, 24 friends :) (**view more**)

MySpace Concert & Parties -Georgia, Orlando, Miami! (**view more**)

In Stores Today - MySpace Records Vol. 1 ! (**view more**)

MySpace Records - in stores soon! (**view more**)

[**View All Blog Entries**]

Tom's Blurbs

About me:
I'm here to help you with **MySpace**. Send me a message if you're confused by anything. **Before asking me a question, please check the FAQ to see if your question has already been answered.**

I may have been on your friend list when you signed up. If you don't want me to be, click "Edit Friends" and remove me!

MySpace Cofounder Tom Anderson Was A Real Life "WarGames" Hacker in 1980s

*Posted Aug 30, 2008 by **Michael Arrington** (@arrington)*

Late last year we discovered that MySpace cofounder Tom Anderson, arguably the most popular individual on the Internet with 240+ million MySpace friends (he is added by default to every MySpace account) was actually 37 years old, not the 32 that he continues to claim on his MySpace page.

Now we've learned a much more colorful part of Anderson's history: In 1985, when he was fourteen and in high school in Escondido, California, Anderson was subject to one of the largest FBI raids in California history after hacking into a Chase Manhattan Bank computer system and subsequently showing his friends how to do it. He was never arrested because he was a minor, but the FBI confiscated all of his computer equipment and some newspaper accounts of the incident stated incorrectly (see image below from a 1986 LA Times story) that he was *"convicted in federal court of computer hacking and placed on probation"* (the statements were corrected in subsequent articles). Anderson used the hacker name "Lord Flathead."



1980's - MySpace Tom

- Tom Andersen aka Lord Flathead
  - Aka Myspace Tom
  - 1985-10-01

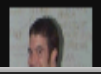
Profile | Incident | Authorities | Courts | Legal | Groups | Sites | Orgs | Links | Documents | Updates

PROFILE

Name	Tom Anderson
Alias	Lord Flathead
Gender	male
Age	16
Wiki	Tom_Anderson
Twitter	myspacetom
Location	United States
Collective	The Inner Circle



Gallery



1980's - MySpace Tom

- Tom Andersen aka Myspace Tom
- 1985-10-01
- 14 or16 years old at the time
- Hacked into Chase Manhattan bank and told friends how to do it.
- FBI raid in California and as a result had all computers seized by federal authorities.
- No charges or criminal convictions have ever been made in relation to this incident.
  - He was a minor at the time.

RiskBased SECURITY

Each incident in Arrest Tracker has a story to be told.

1990's



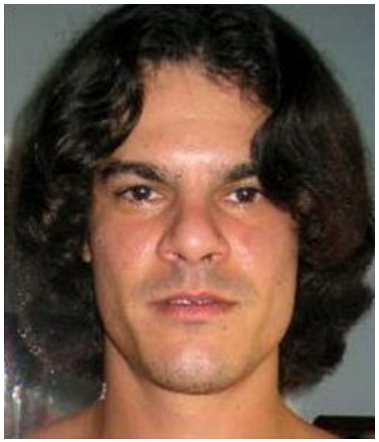
Kevin Mitnick



Max Butler



Kevin Poulsen



Albert Gonzalez



Adrian Lamo



Jeanson James Ancheta



Owen Thor Walker



Jonathan Joseph James



Barrett Brown



Weev



Aaron Swartz



Sabu

Other Notable Arrests

Many other notable arrests for various reasons:

- First prosecution of a particular type of crime
- Severity of the crime
- Length of jail time or fines
- Over reaching regulatory actions
- Impact to those accused
- Etc.

Arrest Tracker

Statistics





Age

- **Youngest Arrest**
  - 12 Years Old
  - Traded pirated information to the hacktivist group Anonymous for video games.

12yo Canadian boy hacked govt sites, gave info to Anonymous for video games

Published time: 27 Oct, 2013 22:56
Edited time: 28 Oct, 2013 08:44

Get short URL



AFP Photo / Philippe Huguen / AFP

A fifth grader has admitted of being the mastermind behind hacker attacks that took down government websites during the 2012 Quebec student protests and passing some of the hacked data to the Anonymous group in exchange for video games.

PROFILE

Name	unknown
Alias	
Gender	male
Age	12
Wiki	N/A
Twitter	N/A
Location	Canada
Collective	Anonymous
Operation	OpQuebec
Occupation	Student
Active Since	0000-00-00



Gallery



Age

- **Oldest Arrest**
  - John McHugh aka Devilman
  - 66 Years Old
  - Busted for selling cards on darkweb.

RiskBased SECURITY

The Register® Biting the hand that feeds IT

DATA CENTER | SOFTWARE | NETWORKS | SECURITY | INFRASTRUCTURE | DEVOPS | BUSINESS | HARDW

Security

DarkMarket carder forum revealed as FBI sting

Cybercrooks bamboozled

14 Oct 2008 at 12:16, John Leyden

Leaked documents have confirmed that carder forum DarkMarket was actually an FBI sting operation.

For the last two years until its shutdown earlier this month DarkMarket.ws posed as a forum where identity thieves, credit card fraudsters, crackers and other ne'er do wells could hang out and exchange tips as well as trading hacker tools and stolen data. In reality, the site was run by Federal agents based in Pittsburgh.

Profile | Incident | Authorities | Courts | Legal | Groups | Sites | Orgs | Links | Documents | Updates

PROFILE

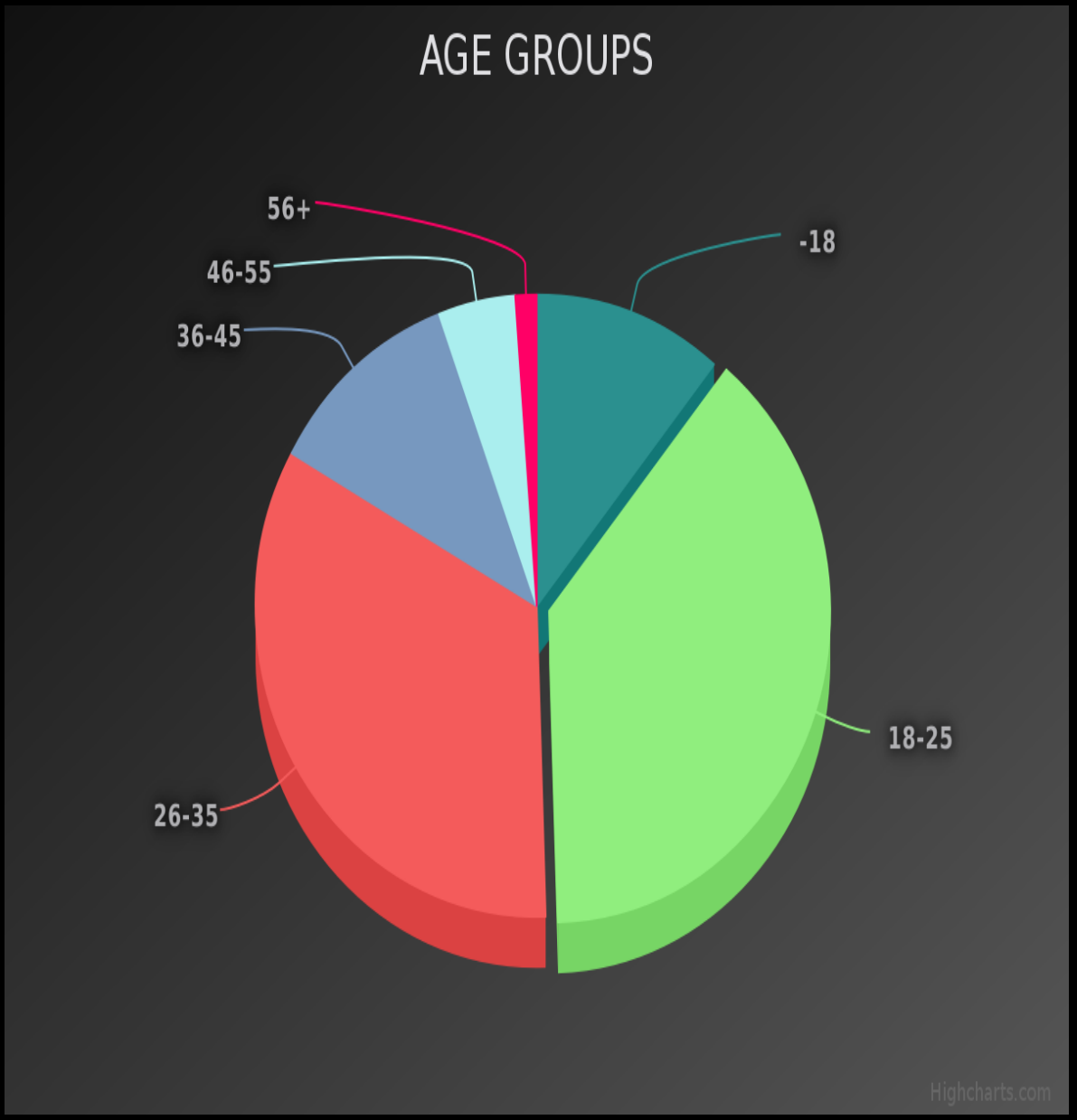
Name	John McHugh
Alias	Devilman
Gender	male
Age	66
Wiki	N/A
Twitter	N/A
Location	United Kingdom



Gallery



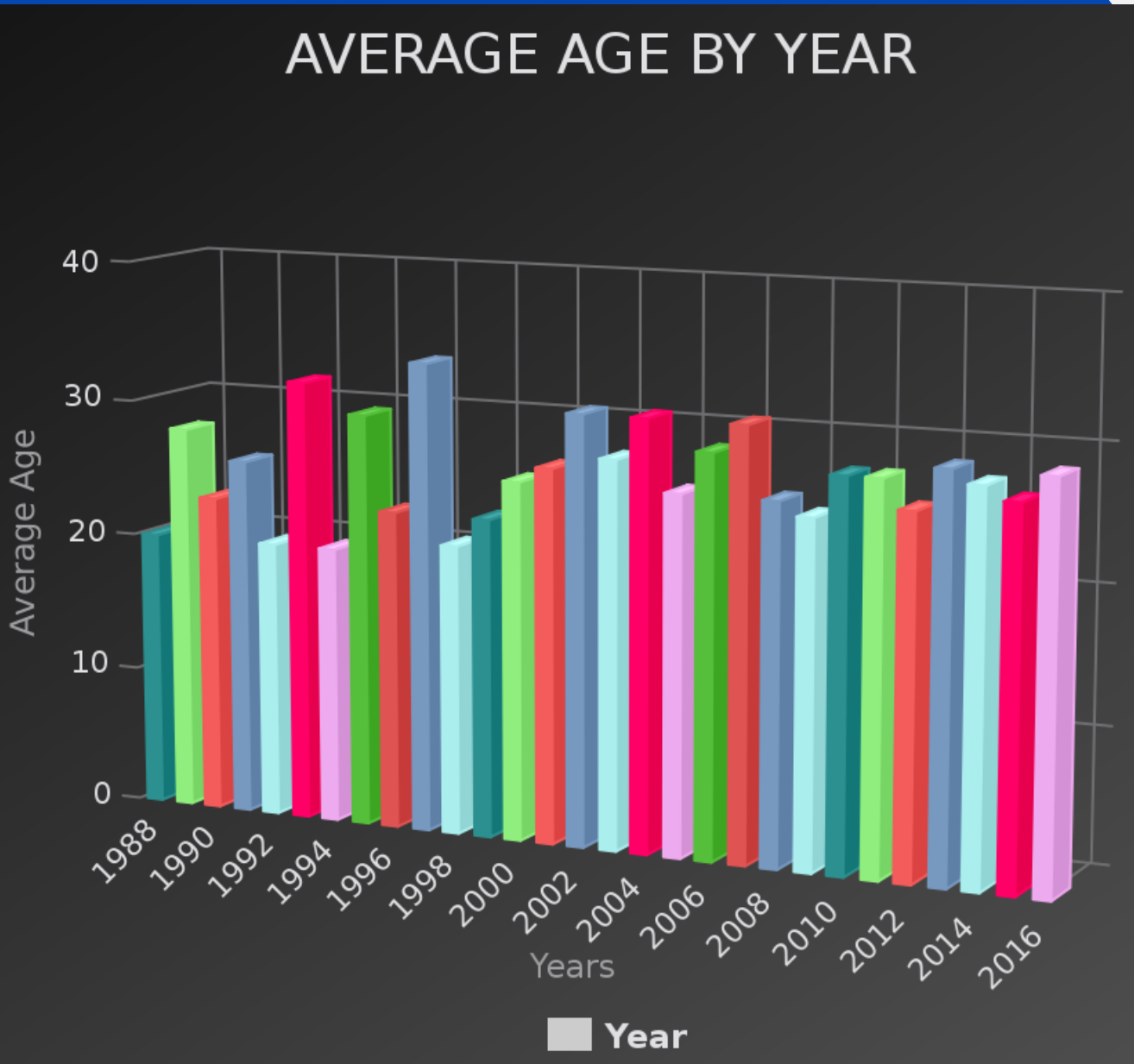
Age



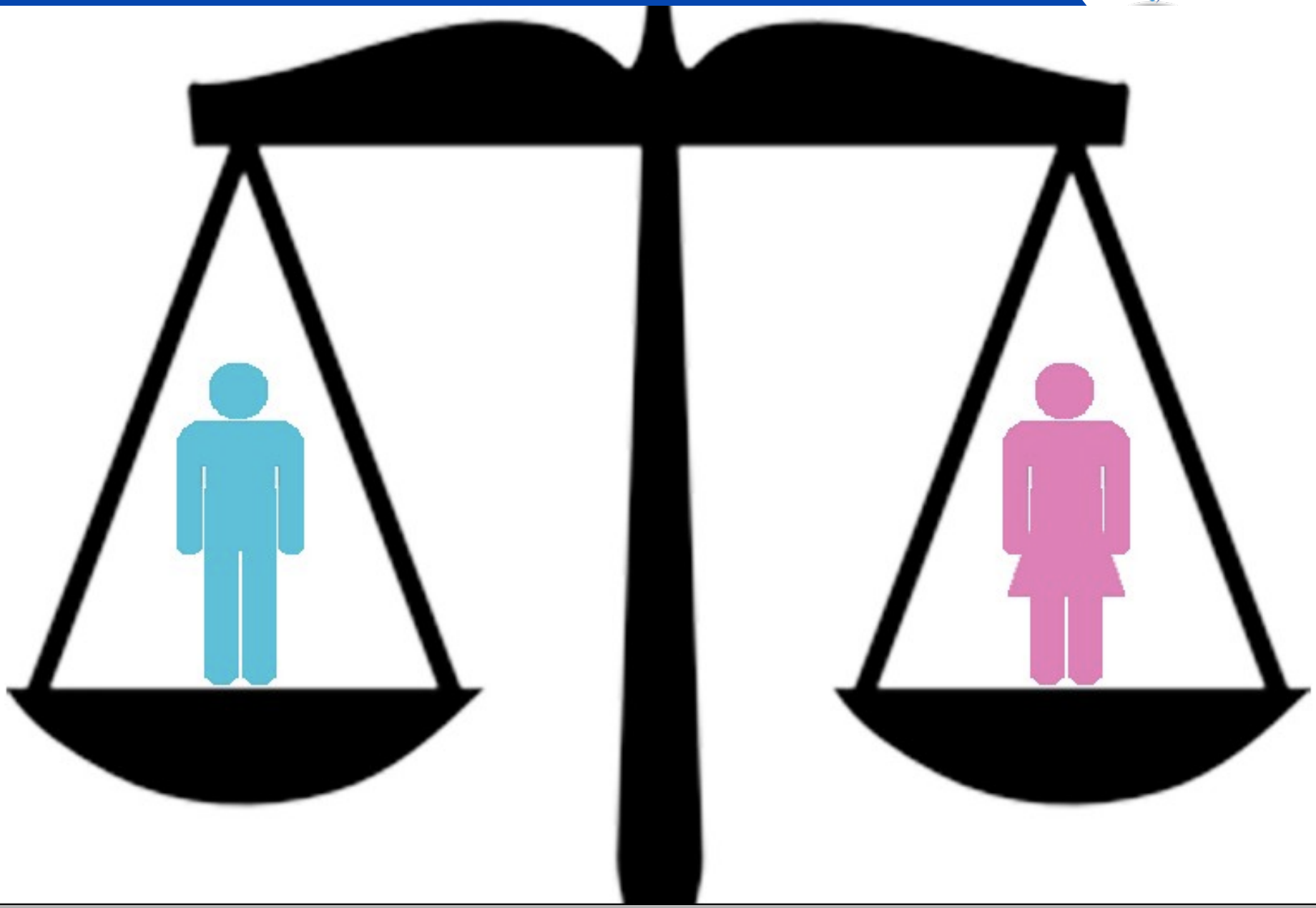
Age Group	Group Count
-18	98
18-25	349
26-35	304
36-45	101
46-55	40
56+	11

Average Age Is Currently 27.

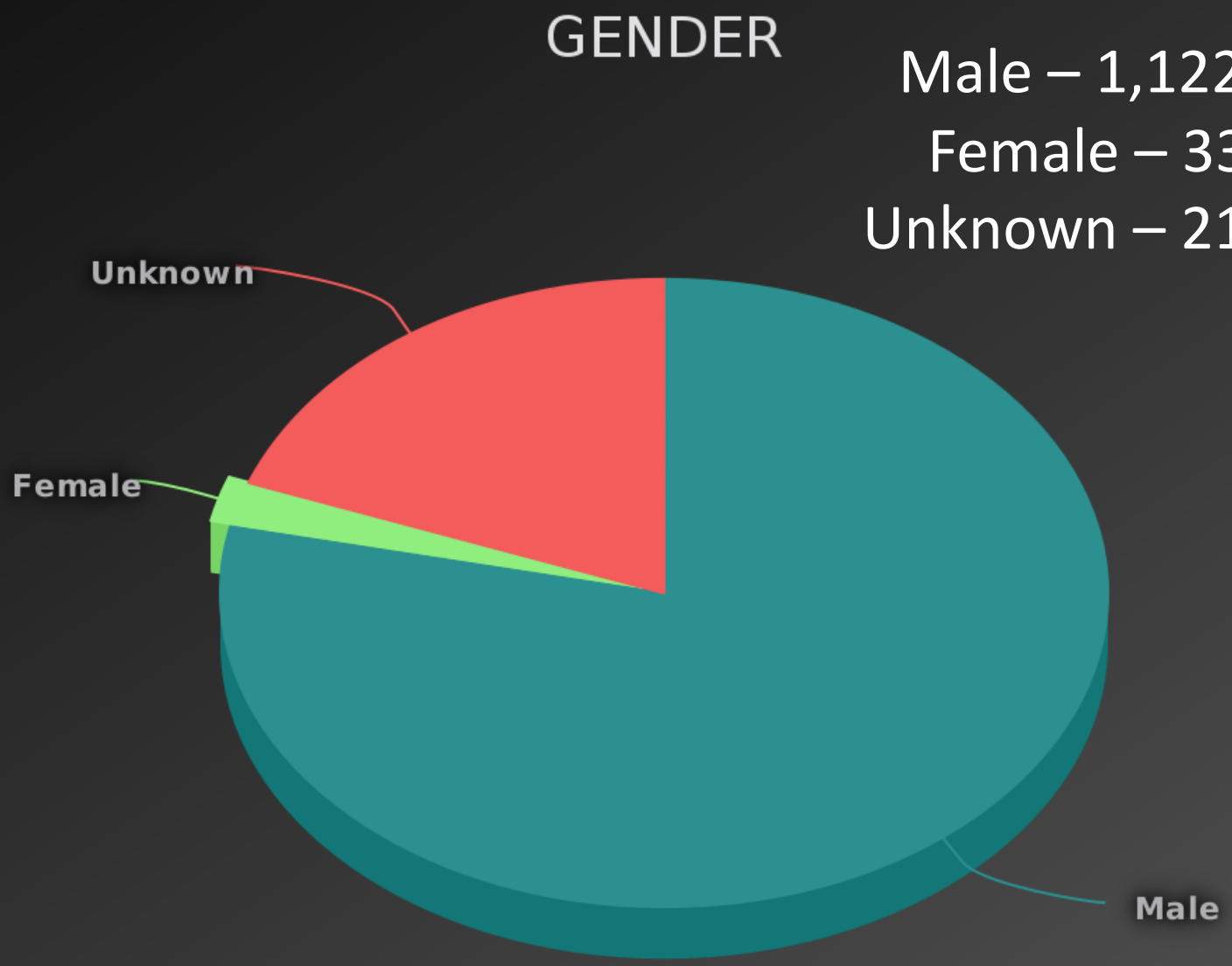
Age


AVERAGE AGE BY YEAR
Average Age
40
30
20
10
0
1988
1990
1992
1994
1996
1998
2000
2002
2004
2006
2008
2010
2012
2014
2016
Years
Year
Highcharts.com

Gender Statistics



Gender Statistics



Male – 1,122 (81.8%)

Female – 33 (2.4%)

Unknown – 215 (15.6%)

Which Countries Do Most Hackers Reside?

aka

Country of Origin For Arrest

Nationality



Nationality – Based On Arrests

United States	586
United Kingdom	154
Philippines	97
Russia	70
Spain	45
Romania	44
India	44
Australia	33
Brazil	29
China	28

Collectives

- Total of 58 known collectives that have had an confirmed incident:
  - Anonymous: 130
  - Western Express Cybercrime Group: 17
  - Legion Of Doom: 16
  - Pirates with Attitudes: 15
  - Masters of Deception: 8
  - Nihilist Order: 7
  - LulzSec: 7
  - Chaos Computer Club: 6

Operations

- **Total of 21 known Hacker Operations that have had a confirmed incident:**
  - OpPayBack: 21
  - OpPayPal: 14
  - Antisec: 7
  - OpTitstorm: 4
  - OpItaly: 2
  - OpScientology: 2

Arrest Inevitable?

Are You Definitely Arrested?

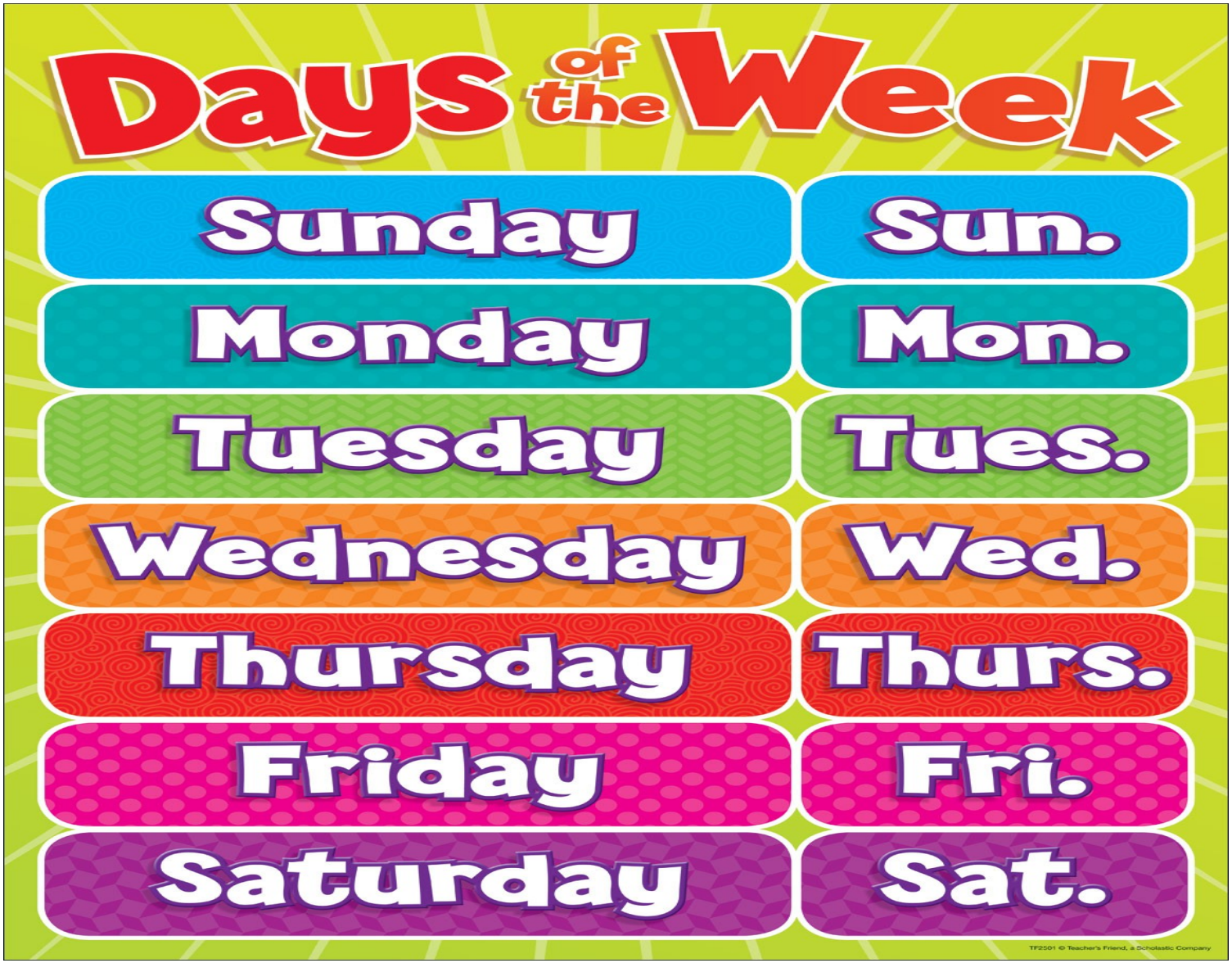


Data Breaches vs Arrests

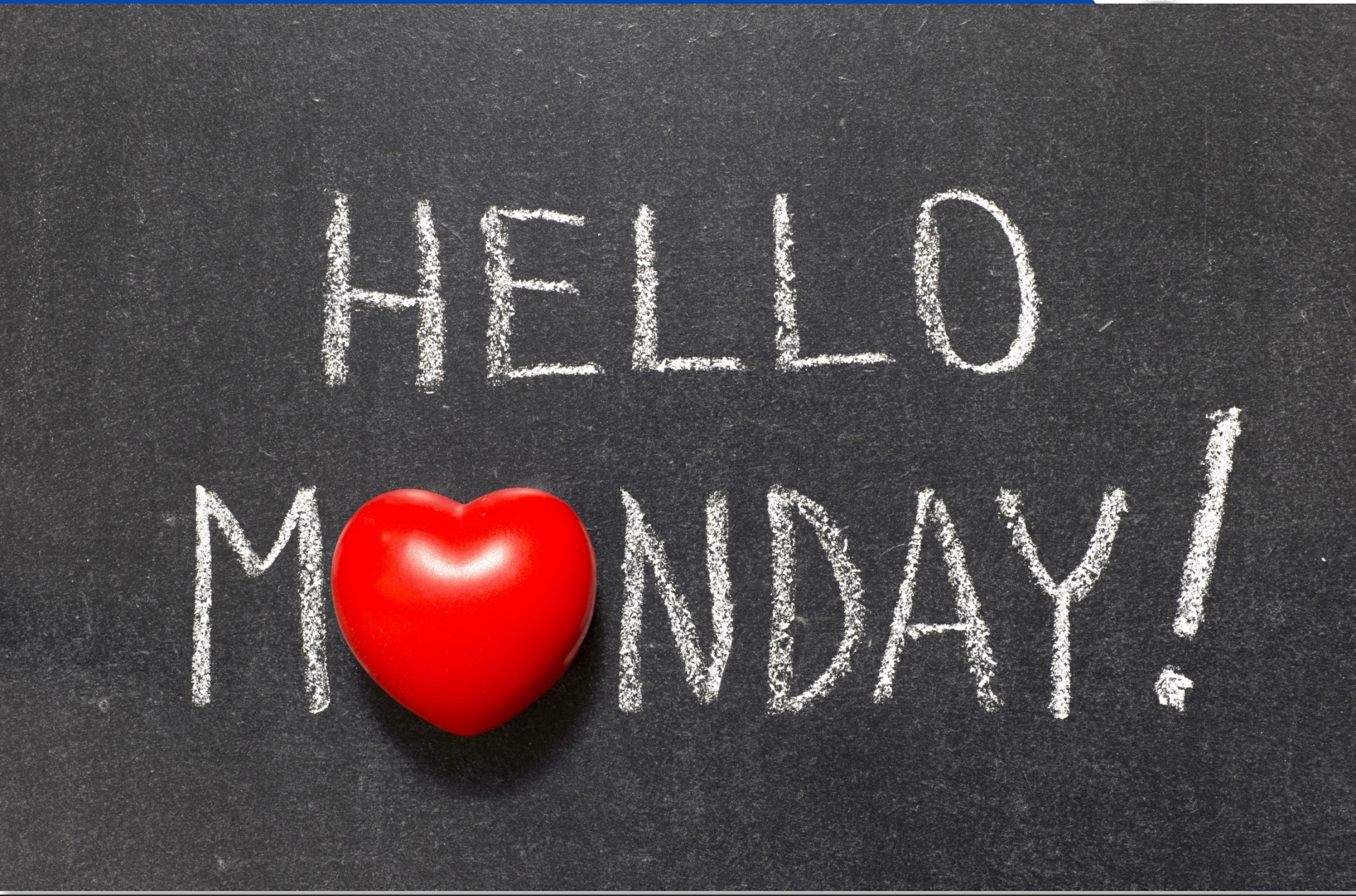
- ~2,000 data breaches 2016 YTD
  - 70 confirmed arrests YTD
- ~4,000 data breaches in 2015
  - 134 confirmed arrests
- ~3,000 data breaches in 2014
  - 47 confirmed arrests
- No where near the "arrests" based on the amount of data breaches

The data so far shows there are 610 days on average between the "crime" to the incident or arrest.

Days Of The Week – Most Likely To Be Arrested



Days Of The Week – Monday



Months Of The Year – Most Likely To Be Arrested



Months Of The Year – Most Likely To Be Arrested



Countries Pursuing Cyber Crime

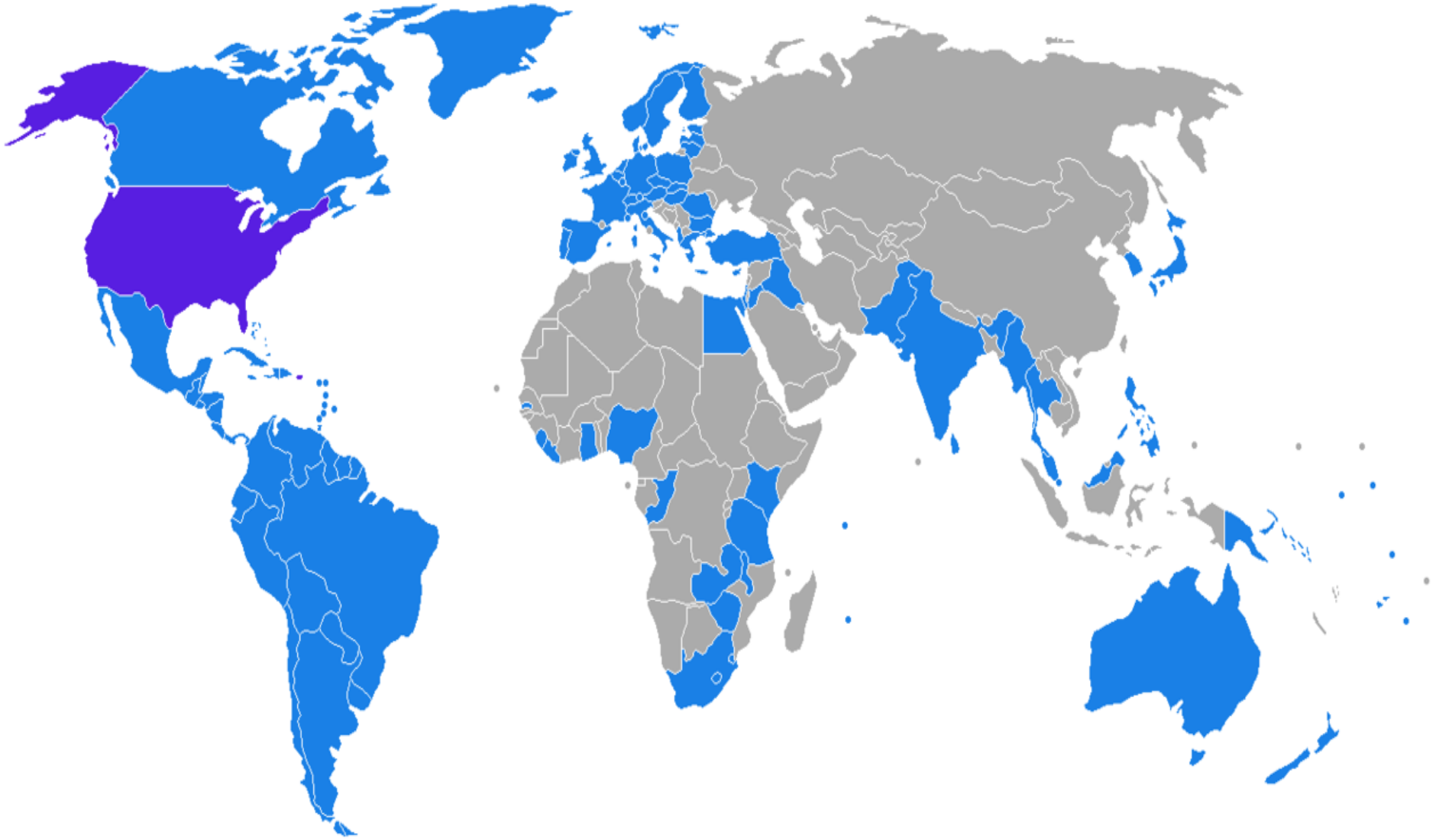
- As most can easily guess USA, is the most active, in computer crime enforcement.
- But the Top 10 might surprise you!

Incidents Countrys	
United States	673
United Kingdom	148
Philippines	116
Russia	60
Spain	45
India	44
Australia	32
Brazil	29
Romania	28
Netherlands	22

Countries - Extradition

- Extraditions:
  - Currently, only the USA has any extraditions tracked.
    - 42 total
  - Top 5 Countries
    - Russia to United States: 8
    - Romania to United States :7
    - Estonia to United States: 6
    - Canada to United States: 3
    - United Kingdom to United States: 3
- Not every country allows the USA to extradite:
  - The United States has extradition treaties with more than 100 countries.

Countries - Extradition



United States of America (shown in purple) has extradition treaties with the countries shown in light blue.

Jail Time

- **Longest Jail Time**
  - 334 years!
    - Onur Kopçak, Turkey
    - Created fake websites that impersonated banks in order to steal people's banking details in a phishing scam

PROFILE

Name	Onur Kopçak
Alias	
Gender	male
Age	23



Gallery

Fines

- **Average Fine**
  - ~1 Million USD
- **Most Common Fine**
  - $5,600 (occurred 13 times)
- **Largest Fine**
  - Viktor Pleshchuk
  - $8.9 Million USD
  - Worldpay hacker, convicted and tried in Russian court under FBI charges.

PROFILE	
Name	Viktor Pleshchuk
Alias	
Gender	male
Age	28
Wiki	N/A
Twitter	N/A
Location	Russia



Once Arrested, How Many Arrested Again?

- Some people just can't stop themselves
- Many times multiple cases over years are consolidated into one case
- But confirmed that 17 People have had Multiple Arrests



Once Arrested, How Many Assist Authorities

- We are asked all the time, how many people are assisting the authorities.
- Arrest Tracker does have fields to track this, however, it is extremely rare and hard to find this data for most incidents.
- Currently, there are **30 persons** that are confirmed to have Assisted Authorities.

Cyber Crime

What Is The Profile Of A “Hacker”?



The data suggests there is no single type of "Hacker" or Cyber Criminal.

Profile Of A Hacker – TELL US!

- Gender: Male
- Age: 27 (on average)
  - Range between 18 and 35
- Location: USA
  - If not, then UK or Philippines
- Crime: Hacking
  - If not, then Cyber Fraud, or Data Theft
- Active Since 2000
- Motivation: Still Unclear



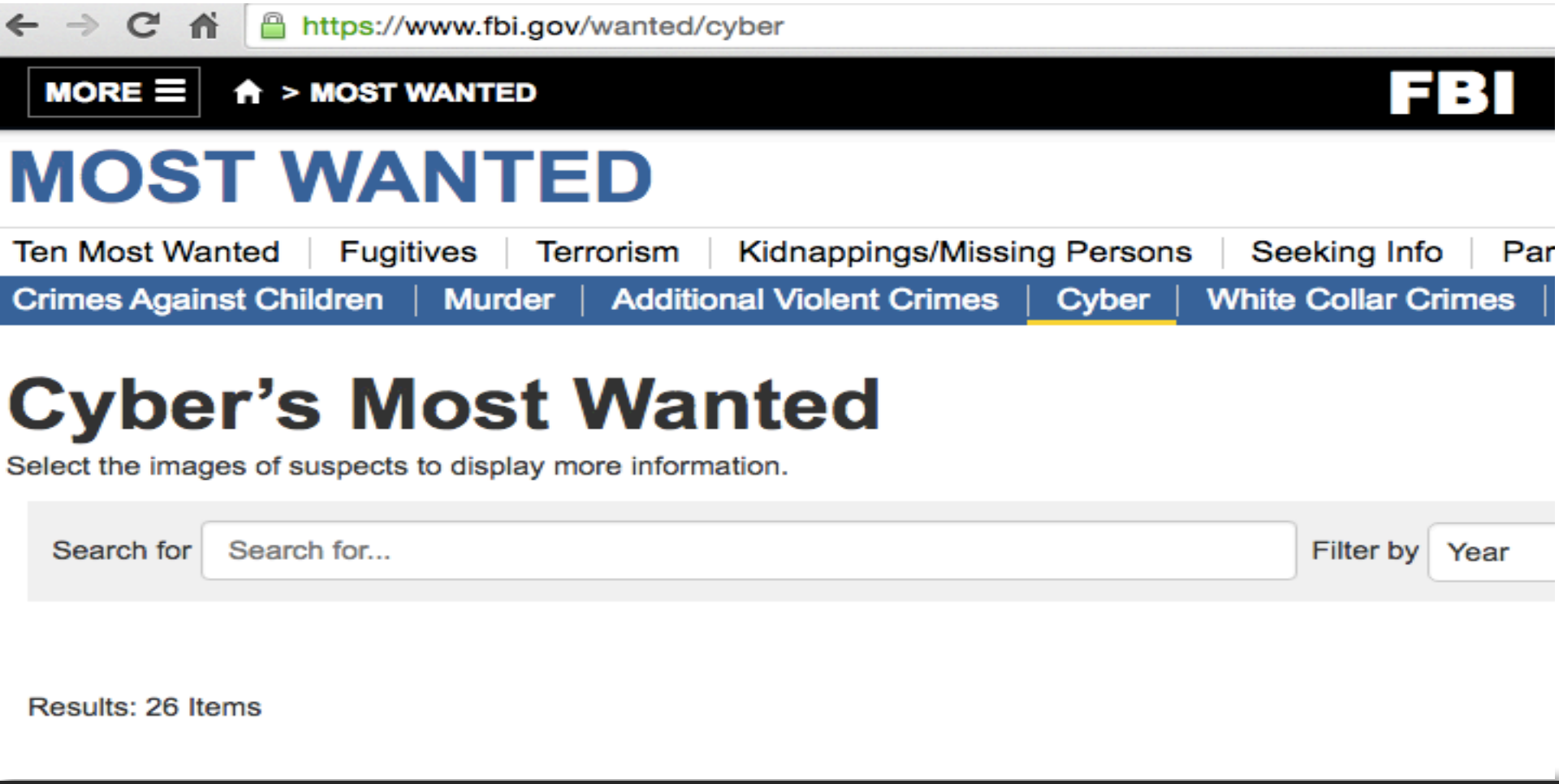
Most Wanted

Who Hasn't Been Arrested Yet?



FBI's Most Wanted

- https://www.fbi.gov/wanted/cyber
- 26 Total Listed As Of 8/1/2016



FBI's Most Wanted - Profiles

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

Twitter Facebook Email





View Poster

Download Poster

- English
- НА РУССКОМ
- на українській мові

FBI's Most Wanted - Profiles

Aliases:

Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

Date(s) of Birth Used	October 28, 1983
Hair	Brown (usually shaves his head)
Eyes	Brown
Height	Approximately 5'9"
Weight	Approximately 180 pounds
Sex	Male
Race	White
Occupation	Bogachev works in the Information Technology field.
NCIC	W890989955

Reward:

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

Remarks:

Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

FBI's Most Wanted - Profiles

RiskBased SECURITY

Caution:

Evgeniy Mikhailovich Bogachev, using the online monikers "lucky12345" and "slavik", is wanted for his alleged involvement in a wide-ranging racketeering enterprise and scheme that ins… without authoriz… malicious software known as "Zeus" on victims' computers. The software was used to capture ba… account numbers, passwords, personal identification numbers, and ot… accounts. While … distribut… … utilized to steal money from the victims' bank accounts. This … account takeover fraud has been investigated by the FBI since the summer of 2009.

Starting in September of 2011, the FBI began investigating a modified version of the Zeus Trojan, known as Gameover Zeus (GOZ). It is believed GOZ is responsible for more than one million computer infections, resulting in financial losses of more than $100 million.

On August 22, 2012, Bogachev was indicted … the nickname "lucky12345" by a federal grand jury in the District of Nebraska on charges of Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; and Aggravated Identity Theft. On May 19, 2014, Bogachev was indicted in his true name by a federal grand jury in the W… … Pennsylvania on charges of … piracy; Computer Fraud; Wire Fraud; Bank Fraud; and Money Laundering. On May 30, 2014, a criminal … was … … indicted nickname of "lucky12345" to Bogachev and charges him with Conspiracy to Commit Bank Fraud.

SHOULD BE CONSIDERED A FLIGHT RISK

Submit a Tip:

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

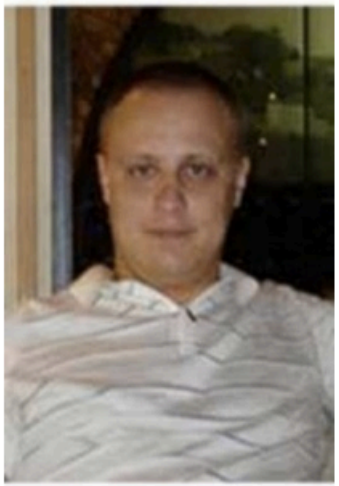
Field Offices: Omaha, Pittsburgh

"..offering a reward up to $3 million for information leading to the arrest and/or conviction.."

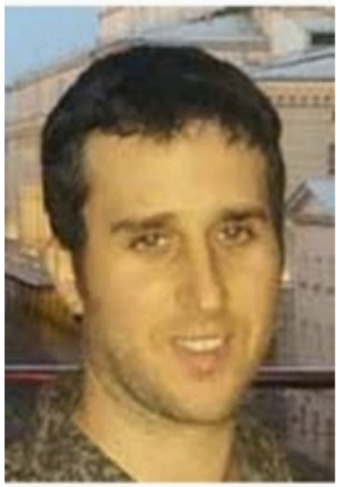
FBI's Most Wanted

RiskBased SECURITY

IRANIAN DDoS ATTACKS



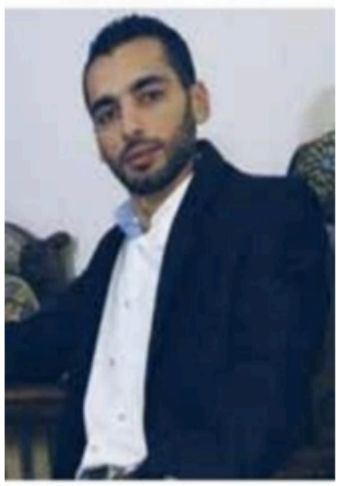
EVGENIY MIKHAILOVICH BOGACHEV



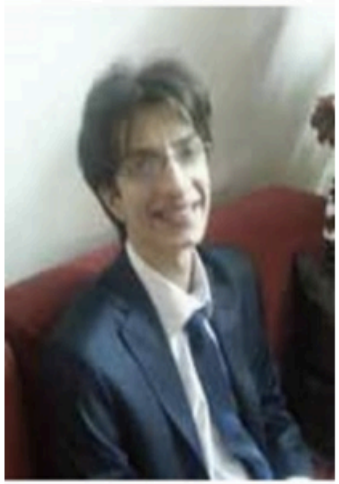
JOSHUA SAMUEL AARON



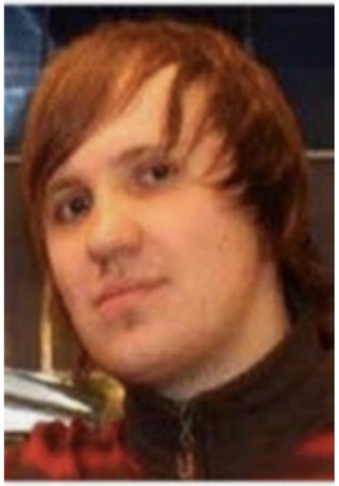
NICOLAE POPESCU



FIRAS DARDAR



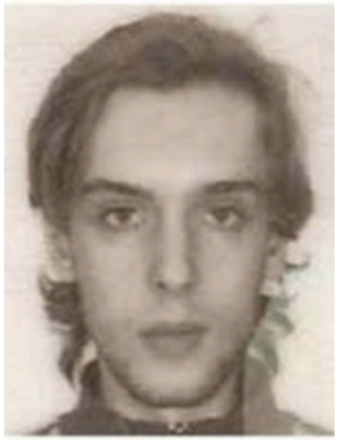
AHMED AL AGHA



ALEXSEY BELAN



VIET QUOC NGUYEN

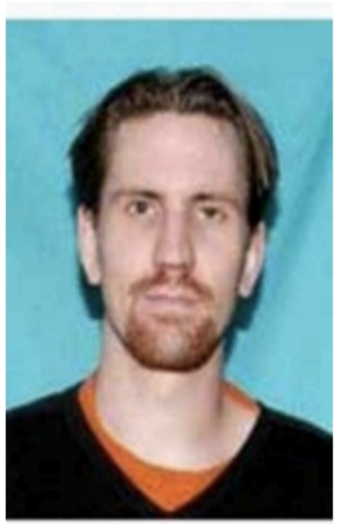


PETERIS SAHUROVS



SHAILESHKUMAR P. JAIN

FBI's Most Wanted



BJORN DANIEL SUNDIN

JABBERZEUS SUBJECTS



SUN KAILIANG



HUANG ZHENYU



WEN XINYU



WANG DONG



GU CHUNHUI



NOOR AZIZ UDDIN

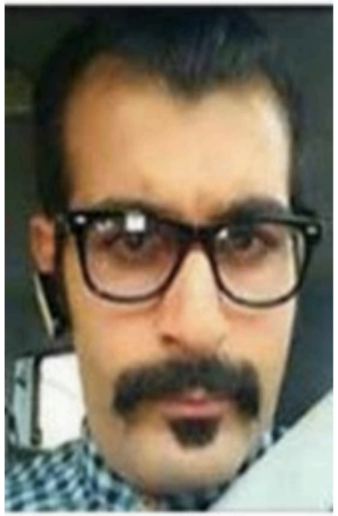


FARHAN UL ARSHAD

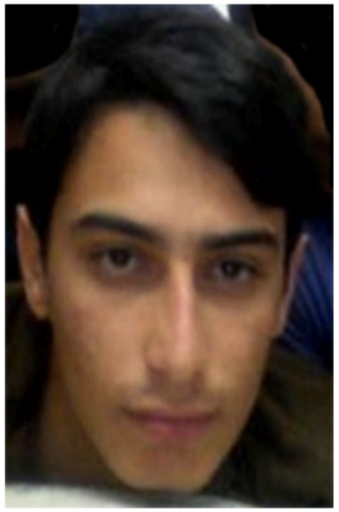


AHMAD FATHI

FBI's Most Wanted



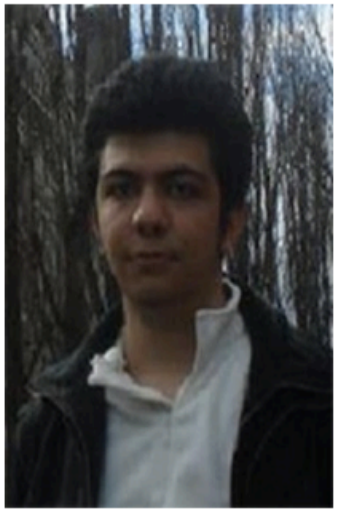
SINA KEISSAR



OMID GHAFFARINIA



AMIN SHOKOHI



MOHAMMAD SADEGH AHMADZADEGAN



HAMID FIROOZI



NADER SAEDI

Up to $4.49M in total potential rewards

Mar 13 2016

Taking pity on law enforcement, Romanian hacker "GhostShell" doxes himself

Posted by Dissent at 10:22 pm Commentaries and Analyses, Hack, Non-U.S., Of Note

What does a prolific Romanian hacker have to do to get arrested in Romania? And why would the 24-year old hacker known as GhostShell be willing to risk arrest by doxing himself? In a wide-ranging interview with DataBreaches.net and CyberWarNews.info, GhostShell discussed hacking, the scene, and the reasons for his unexpected decision to dox himself. This article by DataBreaches.net and CyberWarNews.info provides some background and identifies GhostShell.

In the Beginning

GhostShell, also known as DeadMellox and numerous other aliases, began his hacktivism on January 1, 2012 with attacks against his own government. The situation in Romania had deteriorated badly and had robbed him of the future he had envisioned for himself, he tells us. He frankly admits that he longer remembers whether he was the one who started #OpRomania, as other Romanian hackers were already active, but he did start the AnonOpsRomania account, and was active in attacking the government.

Ghostshell Revealed

- Revealed in March 2016 but still active!

ZDNet SEARCH VIDEOS CXO WINDOWS 10 CLOUD INNOVATION SECURITY DATA CENTERS MORE NEWSLETTERS ALL W

MUST READ THOSE FREE WINDOWS 10 UPGRADES ARE OVER. NOW WHAT?

GhostShell hacker leaks 39 million accounts in security "protest"

The databases contains critically-personal information, including names, email addresses, dates of birth, genders, and even social information.



By Zack Whittaker for Zero Day | June 3, 2016 -- 20:43 GMT (13:43 PDT) | Topic: Security

So What's Next?

Actions



Arrest Tracker Data



Arrest Tracker Future

- We are still working to ensure we are using the best data
- If you find something wrong, please contact us.
- We care about the data and want it to be accurate.
- We want more data!
  - Increase coverage of cyber crime incidents
  - More data fields per incident and by person

Arrest Tracker Future

RiskBased SECURITY

Future ideas/features:

- Add more tracking data about individual persons
  - Ability to handle complex issues such as Romania nationally, lived in Canada for 15 years, then arrested in USA
  - Add ability to track motivation
  - Add mapping to Data Breaches
- More work on "Most Wanted"
  - How long they were FBI most wanted, until arrested.
- Where are they now information?
  - How many work for security companies?
- Subsection for piracy related cases

Arrest Tracker Future

- What comes next?
  - Will we see arrests increase or decrease?
  - Will we see changes in legal environments leading to more arrests?
- Can we take Arrest Tracker information and apply it to your work!
- What new features / ideas do you want to see?
  - Open to feedback!
- And if you want to help……..
  - Please contact us!

Thank you!


This presentation would not have been possible without the collaboration and support of the following people!
• Lee Johnstone (RBS)
• Brian Martin (RBS)



RiskBased SECURITY

"Cyber" Who Done It?! Attribution Analysis Through Arrest History

Jake Kouns, CISO
jake@riskbasedsecurity.com
@jkouns

Lee Johnstone
Security Researcher
@83leej

August 2016