“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

NOT JUST SECURITY, THE RIGHT SECURITY
Looking Back At The Last Five Years

**Number of Incidents**

- 2011: 1,281
- 2012: 3,265
- 2013: 2,529
- 2014: 3,192
- 2015: 3,930

**Number of Records Exposed**

- 2011: 413M
- 2012: 266M
- 2013: 1.0B
- 2014: 1.1B
- 2015: 736M

Source: CyberRiskAnalytics.com
2015 – Threat Vector

2015 Incidents by Threat Vector

- Outside: 3053
- Inside-Accidental: 290
- Inside-Malicious: 275
- Inside-Unknown: 184
- Unknown: 128

77.7% of incidents involved outside the organization activity.

Source: CyberRiskAnalytics.com
2015 - Breach Types

2015 Incidents by Breach Type

- Hacking: 2540
- Skimming: 270
- Fraud: 189
- Mishandled Documents: 136
- Web: 111
- eMail: 91
- Data Misuse/Mishandling: 85
- Unknown: 84
- Snooping: 81
- Virus: 74
- Snail Mail: 54
- Stolen Laptop: 52
- Phishing: 36
- Other Misc.: 127

Source: CyberRiskAnalytics.com
## 2015 Incidents by Country - Top 10

<table>
<thead>
<tr>
<th>Country</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>1593</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>246</td>
</tr>
<tr>
<td>Canada</td>
<td>114</td>
</tr>
<tr>
<td>Australia</td>
<td>99</td>
</tr>
<tr>
<td>Thailand</td>
<td>84</td>
</tr>
<tr>
<td>India</td>
<td>79</td>
</tr>
<tr>
<td>China</td>
<td>65</td>
</tr>
<tr>
<td>Netherlands</td>
<td>48</td>
</tr>
<tr>
<td>Taiwan</td>
<td>43</td>
</tr>
<tr>
<td>France</td>
<td>41</td>
</tr>
</tbody>
</table>

USA and UK account for 46.8% of incidents.

Source: CyberRiskAnalytics.com
2,000+ reported data breaches

1.1+ Billion exposed records

2016 Year To Date
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)

Cyber Attribution

Who did this?
What the HELL did you just do!
Cyber Attribution

I CAN HAZ REASONZ?

NOT JUST SECURITY, THE RIGHT SECURITY
Why Do People Care About Attribution?

KNOWLEDGE IS POWER
Why Do People Care About Attribution?

Attribution is power.

Jeff Rich
Warning:

We’ve already warned you, and this is just a beginning. We continue till our request be met. We’ve obtained all your internal data including your secrets and top secrets if you don’t obey us, we’ll release data shown below to the world. Determine what will you do till November the 24th, 11:00 PM (GMT).

Data Link:

https://www.sonymoviesstockfootage.com/SPEData.zip
http://dmplaehwh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip
Cyber War Attribution

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

Cyber War Attribution by Risk Based Security.
Sony Hack Attribution Generator

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 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 monikers "Guardians of 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 attempt on North 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 Veracode, among others, examined the 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 much more compelling case to discount the possibility that the attack was carried out by state-sponsored actors under the control of North Korea, a theory that has been all but discredited by the Sony hack.

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 only operated in the dark, without anyone else knowing about them. The research team believes that the group was a fiction created by the hackers 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 been linked to actors based 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 malicious files have 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 released...
Sony Hack Attribution Generator

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 employees and 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 "Guardians of 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 of the North 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 by the Sony breach. Our research has provided insight into the likely source of these attacks. Though not definitive, our analysis provides a much clearer picture and suggests an organized criminal group operating out of Romania is responsible for the data breach impacting Sony Pictures Entertainment. This disclosure casts further 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 by a host of security professionals since the attack, 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, and 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 been carried out 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 these vulnerabilities have also been used in Romanian attacks.

NOT JUST SECURITY, THE RIGHT SECURITY
Sony Hack Attribution Generator

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 "Guardians of 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 attempt on a North 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 has given us insight into the likely source of these attacks. Though not definitive, our analysis provides a much clearer picture and suggests an organized criminal group operating in the Democratic People's Republic of Korea is responsible for the data breach impacting Sony Pictures Entertainment. This disclosure casts further 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 by a host of security professionals since the story became public, including noted security consultant Dan Tantler.

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 Tantler, 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 claims 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 attributed to North Korea in the past, 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 these 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 shared.
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)
“Don’t waste money on high priced forensic investigations.... Just roll the dice!”
Cyber attack attribution dice.
cyberattribution.com/#!/Country-Att … - This needs to be done as a "magic 8 ball"
Got a breach that needs attribution? Got you covered!

Joined February 2015

Tweet to Attribution 8 Ball

10 Followers you know

Attention, I have an announcement....China!

I foresee a breach announcement coming soon. Seeing too many new CCs numbers. My guess is hospitality industry this time.

You guys haven't seen anything yet. It's about to get real.
Attribution 8 Ball - Duo

Stop guessing at attribution. Use Duo.

NOT JUST SECURITY, THE RIGHT SECURITY
*shakes magic 8-ball*

Myspace blames data breach on Russian hacker behind LinkedIn and Tumblr attacks

RETWEETS 33  LIKES 96

3:05 PM - 1 Jun 2016
Attribution 8 Ball - Threatbutt

Defense in derp™
Maximum protection from threatening thready threats like
People's Republic of China

Winner of the RSA Conference "best vendor" award!

Published on May 5, 2015
TOTALLY INTEGRATED WITH THE THREATBUTT API, TOO! NOW GIVE US YOUR MONEY.
Sony Pictures - The Interview

Who did it?
Sony Pictures - The Interview – Who?

North Korea
Country in East Asia

North Korea

INSIDER

NORSE

CROWDSTRIKE

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

NOT JUST SECURITY, THE RIGHT SECURITY
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 master-minded by North Korea and that insiders were key to the implementation of one of the most devastating attacks in history”. Stammberger says Norse data is pointing towards a woman who calls herself “Lena” and claims to be associated with the so-called “Guardians of Peace” hacking group. Norse believes it’s identified this woman as someone who worked at Sony in Los Angeles for ten years until leaving the company this past May.
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 [...]}

Why I *still* don’t 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 [...]}

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 [...]
THE EVIDENCE THAT NORTH KOREA HACKED SONY IS FLIMSY
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.
PBS - Cyber Attribution Debate Live!

Marc Rogers
CLOUDFLARE

Dmitri Alperovitch
CROWDSTRIKE

PBS NEWSHOUR

NOT JUST SECURITY, THE RIGHT SECURITY
"... the FBI now has enough information to conclude that the North Korean government is responsible."

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, we confirmed that it was the victim of a cyber attack that destroyed systems and stole a large quantity of personal and commercial data. The attacks appeared to be orchestrated by a group of hackers who have a history of such attacks. 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.

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’ personal information, including financial and travel data. 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.
Lots of Debate – Main Two Players!

CROWDSTRIKE

VS!

NORSE

NOT JUST SECURITY, THE RIGHT SECURITY
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?
FBI Defends Sony Hack Attribution

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

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

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.
Sources: Security Firm Norse Corp. Imploding

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

www.democrats.org

NOT JUST SECURITY, THE RIGHT SECURITY
Give Hillary Money For Cybersecurity

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

First name

Last name

TICKET SELECTION

SECURE

NOT JUST SECURITY, THE RIGHT SECURITY
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 Matt Daloise

The Democratic National Committee (DNC) released a report that concluded Russian cyber operatives were behind the hack. The report was authored by CrowdStrike, a security firm that determined the likely hacking group was the Russian military intelligence (GRU). The report states, "Russia's military intelligence service (GRU) was responsible for the hack, and there is evidence that it was working on behalf of the Russian government. The report builds on previous evidence that shows the GRU has a history of using cyber attacks to further its 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."
Fidelis is also very confident it is Russian actions due to:

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

NEW DETAILS
FBI INVESTIGATES DNC EMAIL HACK
OFFICIALS: RUSSIANS LIKELY BEHIND CYBERATTACK
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.
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
Russia cyber attack: Large hack 'hits government'

30 July 2016 | Europe

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

By LEE FERRAN • ASPEN, Colorado — Jul 30, 2016, 2:30 PM ET
Does it actually matter that we get Cyber Attribution correct?
Sony cyber-attack: North Korea faces new US sanctions

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

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.
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

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
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?
Founded by Lee Johnstone
—Security Researcher
—Founder Cyber War News

WWW.CYBERWARNEWS.INFO

CYBER WAR NEWS

NOT JUST SECURITY, THE RIGHT SECURITY
• **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!
<table>
<thead>
<tr>
<th>Profile</th>
<th>Incident</th>
<th>Courts</th>
<th>Legal</th>
<th>Authorites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Incident Information</td>
<td>Deal</td>
<td>Announcing Prosecutor</td>
<td>Authorites</td>
</tr>
<tr>
<td>Alias</td>
<td>Incident Date</td>
<td>Plead</td>
<td>Judge</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>Incident Country</td>
<td>Extradited</td>
<td>Procurator</td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>Date of Crime</td>
<td>Trial</td>
<td>Lawyer</td>
<td></td>
</tr>
<tr>
<td>Wiki</td>
<td>Caught by</td>
<td>Fined</td>
<td>Lawfirm</td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td>Arrested</td>
<td>Fine Amount</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Charged</td>
<td>Fine Paid</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collective</td>
<td>Custody</td>
<td>Restitution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td>Bail</td>
<td>Convicted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occupation</td>
<td>Wanted</td>
<td>Convicted Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Since</td>
<td>Raided</td>
<td>Sentenced</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Seized Items</td>
<td>Sentence Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sentenced Info</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sentence Months</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sentence Suspended</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sentence Probation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Served</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Appeal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOT JUST SECURITY, THE RIGHT SECURITY**

cyber
Arrest Tracker

What Can It Help Us With?
We need to first recognize there are limitations with the data!
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!
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” – Mr Robot
Real Faces of Cyber Crime – Arrest Tracker
Cyber Arrests

Timeline
Timeline

INCIDENTS OVER TIME

CLICK AND DRAG IN THE PLOT AREA TO ZOOM IN
• 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
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

It’s Tom!
1980’s - MySpace Tom

Tom

":-)"

Male
30 years old
Santa Monica,
CALIFORNIA
United States

Last Login:
8/27/2006

Contacting Tom

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

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 URL:
http://www.myspace.com/tom
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
• Tom Andersen aka Myspace Tom
• 1985-10-01
• 14 or 16 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.
Each incident in Arrest Tracker has a story to be told.
1990’s

Kevin Mitnick  Max Butler  Kevin Poulsen

cyber

NOT JUST SECURITY, THE RIGHT SECURITY
2000’s

Albert Gonzalez

Adrian Lamo

Jeanson James Ancheta

Owen Thor Walker

Jonathan Joseph James
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
?
• **Youngest Arrest**
  – 12 Years Old
  – Traded pirated information to the hacktivist group Anonymous for video games.
## Age

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

<table>
<thead>
<tr>
<th>Profile</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>John McHugh</td>
</tr>
<tr>
<td><strong>Alias</strong></td>
<td>Devilman</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td>male</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td>66</td>
</tr>
<tr>
<td><strong>Wiki</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Twitter</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
Average Age Is Currently 27.
Gender Statistics
Gender Statistics

**GENDER**

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

NOT JUST SECURITY, THE RIGHT SECURITY
<table>
<thead>
<tr>
<th>Nationality</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>586</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>154</td>
</tr>
<tr>
<td>Philippines</td>
<td>97</td>
</tr>
<tr>
<td>Russia</td>
<td>70</td>
</tr>
<tr>
<td>Spain</td>
<td>45</td>
</tr>
<tr>
<td>Romania</td>
<td>44</td>
</tr>
<tr>
<td>India</td>
<td>44</td>
</tr>
<tr>
<td>Australia</td>
<td>33</td>
</tr>
<tr>
<td>Brazil</td>
<td>29</td>
</tr>
<tr>
<td>China</td>
<td>28</td>
</tr>
</tbody>
</table>
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

Sunday
Mon.
Tues.
Wed.
Thurs.
Fri.
Sat.
Days Of The Week – Monday

HELLO MONDAY!
Months Of The Year – Most Likely To Be Arrested
Months Of The Year – Most Likely To Be Arrested

April
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!

<table>
<thead>
<tr>
<th>Country</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>673</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>148</td>
</tr>
<tr>
<td>Philippines</td>
<td>116</td>
</tr>
<tr>
<td>Russia</td>
<td>60</td>
</tr>
<tr>
<td>Spain</td>
<td>45</td>
</tr>
<tr>
<td>India</td>
<td>44</td>
</tr>
<tr>
<td>Australia</td>
<td>32</td>
</tr>
<tr>
<td>Brazil</td>
<td>29</td>
</tr>
<tr>
<td>Romania</td>
<td>28</td>
</tr>
<tr>
<td>Netherlands</td>
<td>22</td>
</tr>
</tbody>
</table>
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.
United States of America (shown in purple) has extradition treaties with the countries shown in light blue.
**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

<table>
<thead>
<tr>
<th>Profile</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Onur Kopçak</td>
</tr>
<tr>
<td>Alias</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>male</td>
</tr>
<tr>
<td>Age</td>
<td>23</td>
</tr>
</tbody>
</table>
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.
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 MIKAHILOVICH 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

Download Poster
- English
- На РУССКОМ
- Чип українській мові

View Poster

NOT JUST SECURITY, THE RIGHT SECURITY
FBI’s Most Wanted - Profiles

Aliases:
Yevgeniy Bogachev, Evgeniy Mikhailovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

<table>
<thead>
<tr>
<th>Date(s) of Birth Used</th>
<th>October 28, 1983</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hair</td>
<td>Brown (usually shaves his head)</td>
</tr>
<tr>
<td>Eyes</td>
<td>Brown</td>
</tr>
<tr>
<td>Height</td>
<td>Approximately 5'9&quot;</td>
</tr>
<tr>
<td>Weight</td>
<td>Approximately 180 pounds</td>
</tr>
<tr>
<td>Sex</td>
<td>Male</td>
</tr>
<tr>
<td>Race</td>
<td>White</td>
</tr>
<tr>
<td>Occupation</td>
<td>Bogachev works in the Information Technology field.</td>
</tr>
<tr>
<td>NCIC</td>
<td>W890989955</td>
</tr>
</tbody>
</table>

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.
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 infected, without authorization, malicious software known as ‘Zeus’ on victims’ computers. The software was used to capture bank account numbers, passwords, personal identification numbers, and other information. While the malware spread, the administrator would oversee the continued operation and distribution, often via email attachments or infected site or compromised domain controller. Bogachev and his associates utilized to steal money from the victims’ bank accounts. This online account takeover fraud has been investigated by the FBI since the summer of 2009.

Starting in September of 2011, the FBI began investigating the malicous software known as the Zeus Trojan, also known as Banker or Zeus (QBQ). It was determined Bogachev was responsible for more than one million computer infections, resulting in financial losses of more than $100 million.

On August 22, 2012, Bogachev was indicted under the nickname “lucky12345” by a federal grand jury in the District of Nebraska on charges of Conspiracy to Participate in a 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 Western District of Pennsylvania on charges of Computer Fraud; Wire Fraud; Bank Fraud; and Money Laundering. On May 30, 2014, a criminal complaint was filed in the District of Nebraska charging Bogachev with Conspiracy to Commit Bank Fraud.

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

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
FBI’s Most Wanted

- 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

NOT JUST SECURITY, THE RIGHT SECURITY
FBI’s Most Wanted

BJORN DANIEL SUNDIN

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 SHOKOH
MOHAMMAD SADEGH AHMADZADEGAN
HAMID FIROOZI

Up to $4.49M in total potential rewards

NOT JUST SECURITY, THE RIGHT SECURITY
Taking pity on law enforcement, Romanian hacker “GhostShell” doxes himself

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 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.

So What’s Next?

Actions
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
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)
“Cyber” Who Done It?! Attribution Analysis Through Arrest History

Jake Kouns, CISO
jake@riskbasedsecurity.com
@jkouns

Lee Johnstone
Security Researcher
@83leej

August 2016