Thomas Ljungberg Kristensen

96 Aarhus Universitet, Datalog

03 Systematic, Systems Engineer

07 Danske Bank, Developer

12 Kamstrup, Systems Engineer

14 FortConsult, Senior Security Consultant

15 WelcomeSecurity, Security Advisor

Hacking is an industry and it is targeting you! because it is easy!

Hacking is an industry
and it is targeting you!
because it is easy!

New security issues each day…


Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop

By RACHEL ABRAMS AUG. 5, 2014

http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html

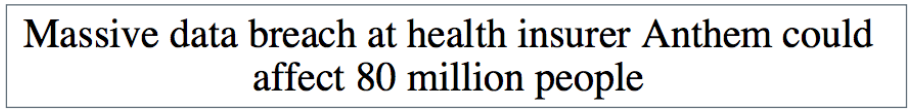

10 April 2014 Last updated at 15:04 GMT

Share

Heartbleed bug creates confusion online

By Mark Ward
Technology correspondent, BBC News

http://www.bbc.com/news/technology-26971363


Massive data breach at health insurer Anthem could affect 80 million people

http://theweek.com/5things/537729/massive-data-breach-health-insurer-anthem-could-affect-80-million-people


Amy Lee Become a fan

Why Does Sony Keep Getting Hacked?

Posted: 06/08/2011 6:17 pm EDT | Updated: 08/08/2011 5:12 am EDT

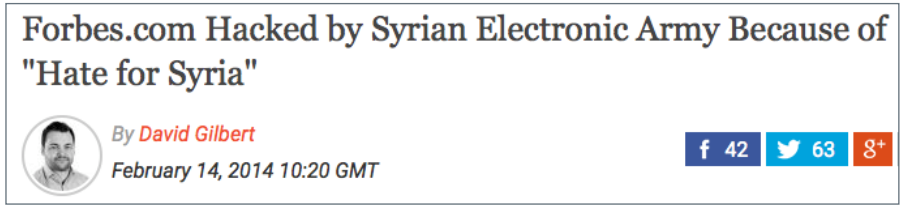
http://www.huffingtonpost.com/2011/06/08/sony-hack-problems_n_873443.html


Lenovo hit by lawsuit over Superfish adware

Consumers and attorneys are already looking to the legal system for recourse following revelations that Lenovo installed potentially dangerous software on its PCs.

by Lance Whitney @lancewhit / February 24, 2015 9:29 AM PST

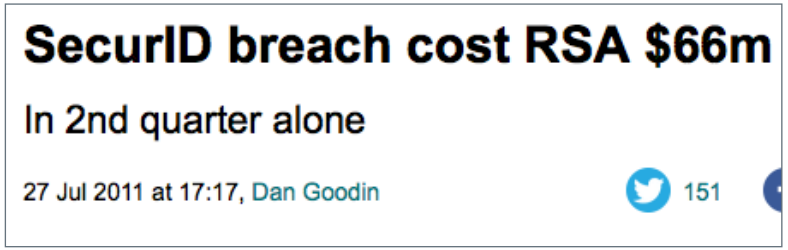
http://www.cnet.com/news/lenovo-hit-by-lawsuit-over-superfish-adware/


Forbes.com Hacked by Syrian Electronic Army Because of "Hate for Syria"

By David Gilbert
February 14, 2014 10:20 GMT

f 42 63

http://www.ibtimes.co.uk/forbes-com-hacked-by-syrian-electronic-army-because-hate-syria-1436415


SecurID breach cost RSA $66m

In 2nd quarter alone

27 Jul 2011 at 17:17, Dan Goodin

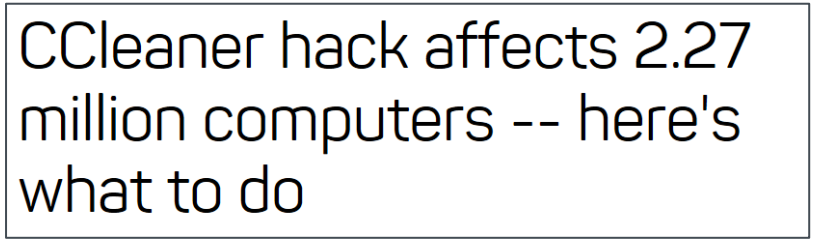
151

http://www.theregister.co.uk/2011/07/27/rsa_security_breach/


JP Morgan reveals data breach affected 76 million households

Elizabeth Weise, USATODAY 11:19 a.m. EDT October 3, 2014

http://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/


CCleaner hack affects 2.27 million computers -- here's what to do

https://www.cnet.com/how-to/ccleaner-was-hacked-heres-what-to-do-next/

Mærsk

NYHEDER

DR

TEMA HACKERANGREB

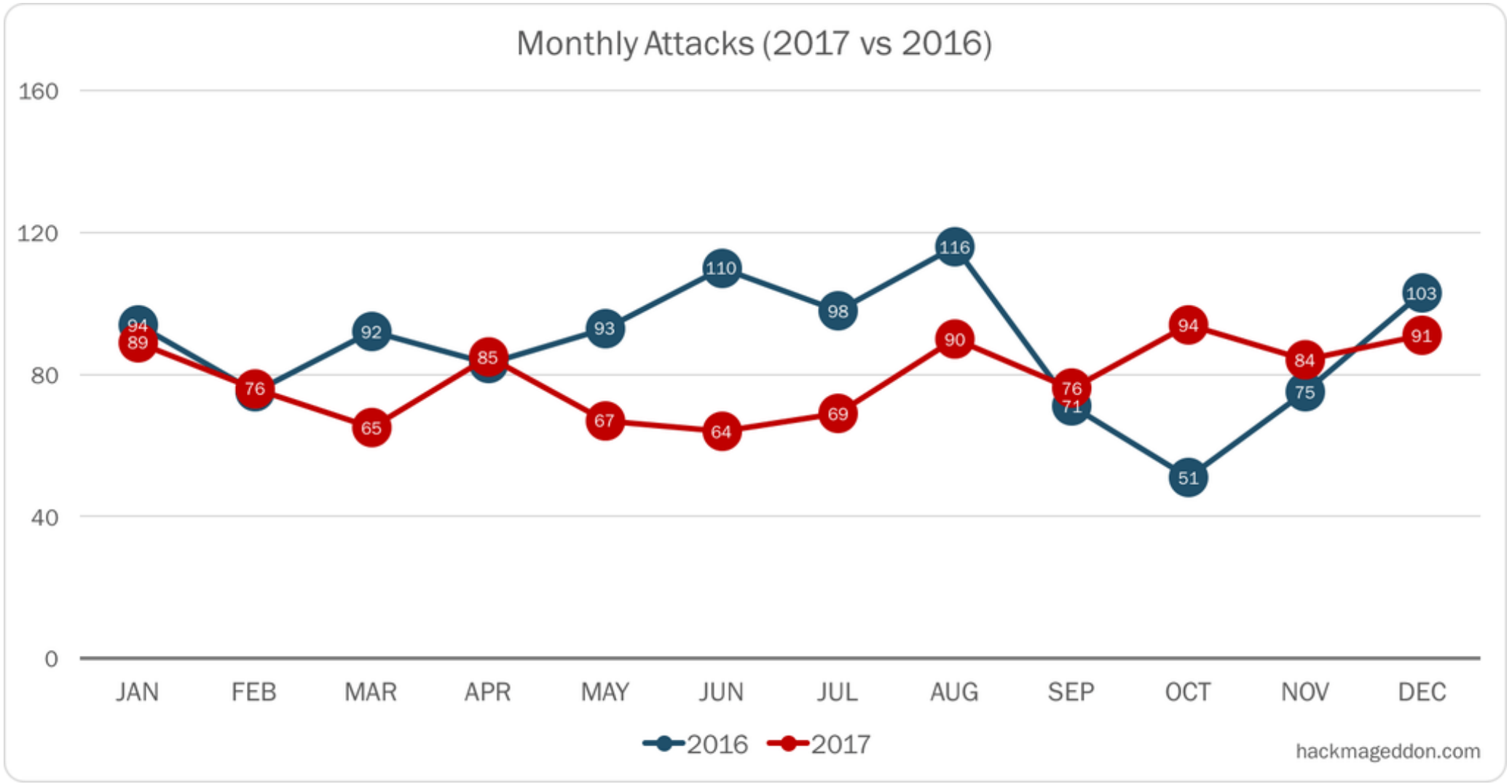
37 ARTIKLER

Hackerangreb koster Mærsk milliardbeløb

Mærsk anslår, at hackerangrebet fra juni og juli vil koste selskabet 1,3 til 1,9 milliarder kroner.

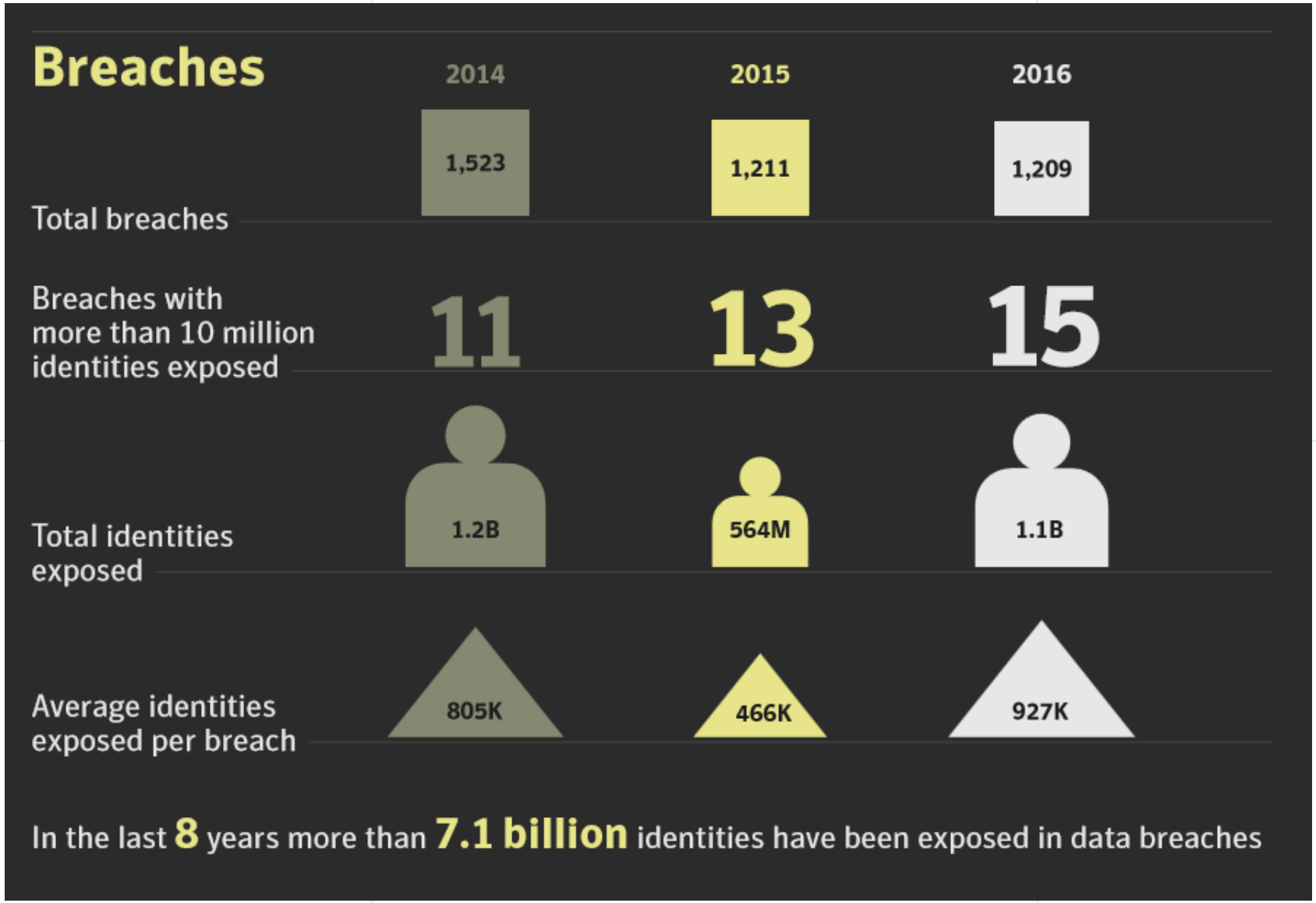
Source: https://www.dr.dk/nyheder/penge/hackerangreb-koster-maersk-milliardbeloeb

Not even just one attack per day!



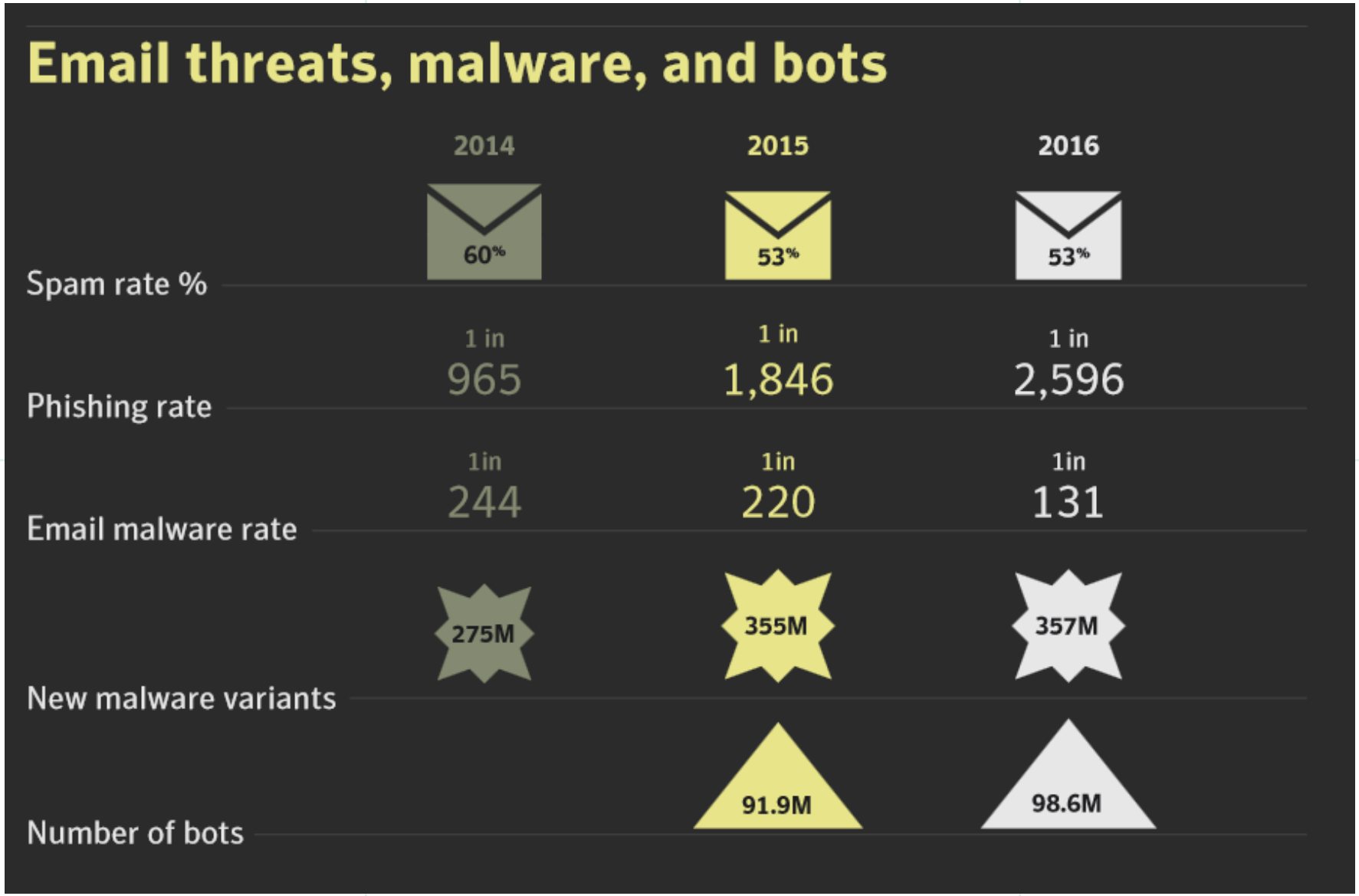
Source: http://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/

Numbers!



Source: Symantec 2017 Internet Security Threat Report

More numbers!



Source: Symantec 2017 Internet Security Threat Report

Crime-As-A-Service

Sources: http://www.forbes.com/sites/ciocentral/2013/02/01/why-cybercrime-remains-big-business-and-how-to-stop-it/

Bring a company offline?

Source: https://www.youtube.com/watch?v=vn-lU3Zu3dw

Renting hacker services…

Annual license: $ 1500
Half-year license: $ 1000
3-month license: $ 700

Update cryptor $ 50
Changing domain $ 20 multidomain $ 200 to license.
During the term of the license all the updates are free.

Rent on our server:

1 week (7 full days): $ 200
2 weeks (14 full days): $ 300
3 weeks (21 full day): $ 400
4 weeks (31 full day): $ 500
24-hour test: $ 50

- There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract.

Providing our proper domain included. The subsequent change of the domain: $ 35
No longer any hidden fees, rental includes full support for the duration of the contract.

Sources: http://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit-3/

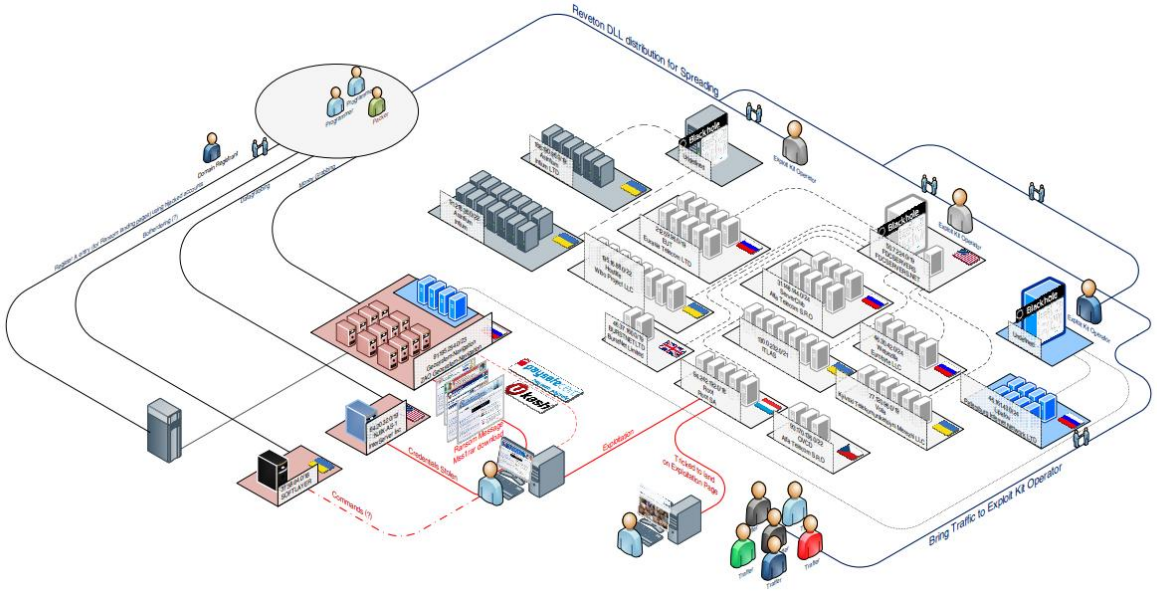
…an emerging trend with traditional organized crime syndicates and criminally minded technology professionals working together and pooling their resources and expertise…

Sources: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Organization of the IT criminals…

The most common 'positions' or specializations according to the FBI are:

1. **Programmers.** Who develop the exploits and malware used to commit cyber-crimes.
2. **Distributors.** Who trade and sell stolen data and act as vouchers for the goods provided by other specialists.
3. **Tech experts.** Who maintain the criminal enterprise's IT infrastructure, including servers, encryption technologies, databases, and the like.
4. **Hackers.** Who search for and exploit applications, systems and network vulnerabilities.
5. **Fraudsters.** Who create and deploy various social engineering schemes, such as phishing and spam.
6. **Hosted systems providers.** Who offer safe hosting of illicit content servers and sites.
7. **Cashiers.** Who control drop accounts and provide names and accounts to other criminals for a fee.
8. **Money mules.** Who complete wire transfers between bank accounts. The money mules may use student and work visas to travel to the U.S. to open bank accounts.
9. **Tellers.** Who are charged with transferring and laundering illicitly gained proceeds through digital currency services and different world currencies.
10. **Organization Leaders.** Often "people persons" without technical skills. The leaders assemble the team and choose the targets.



Sources: "The Cyber-crime black market uncovered" by Panda Security

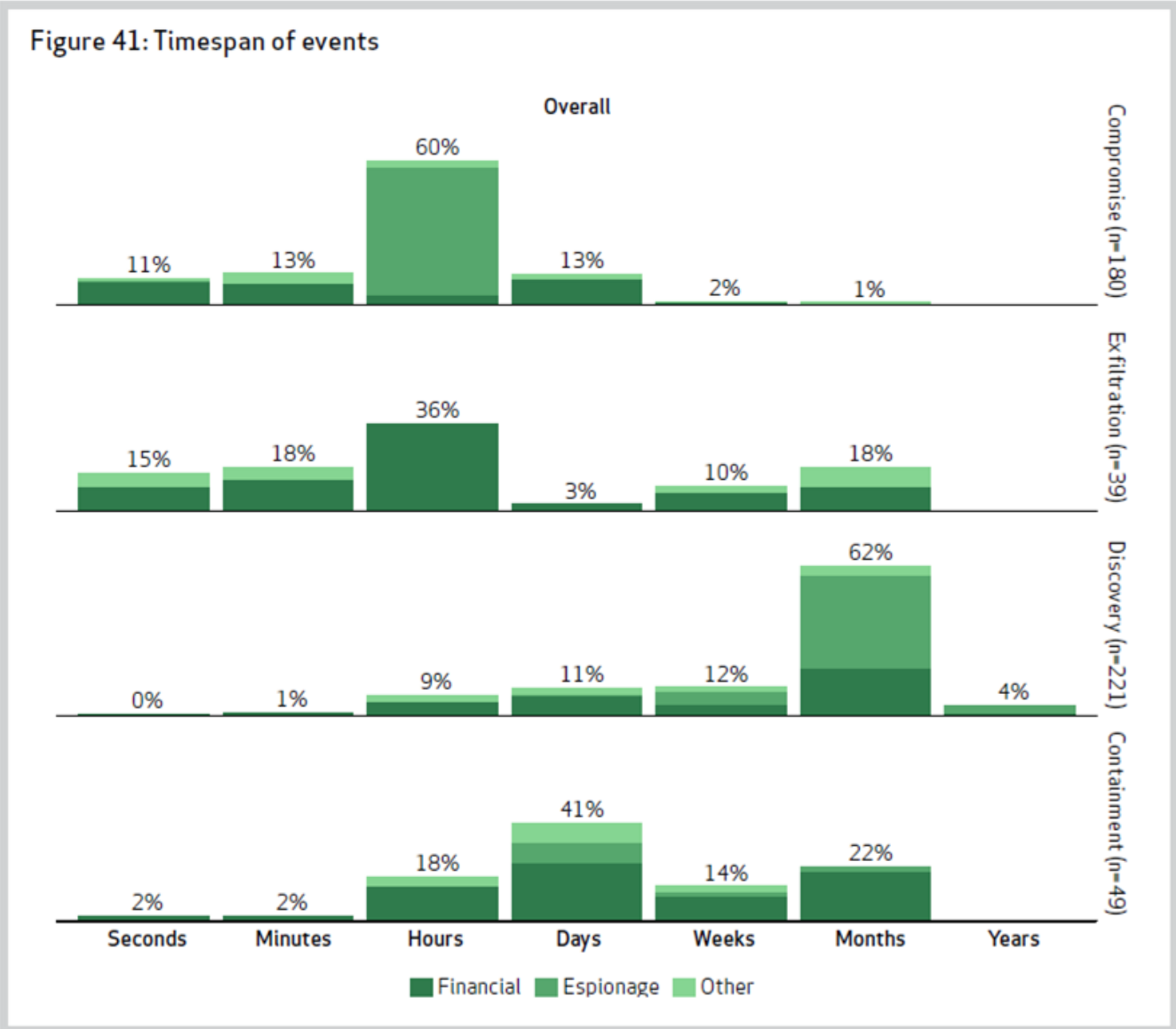
Sources: http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

Multi layered attack

Sources: http://www.symantec.com/theme.jsp?themeid=apt-infographic-1

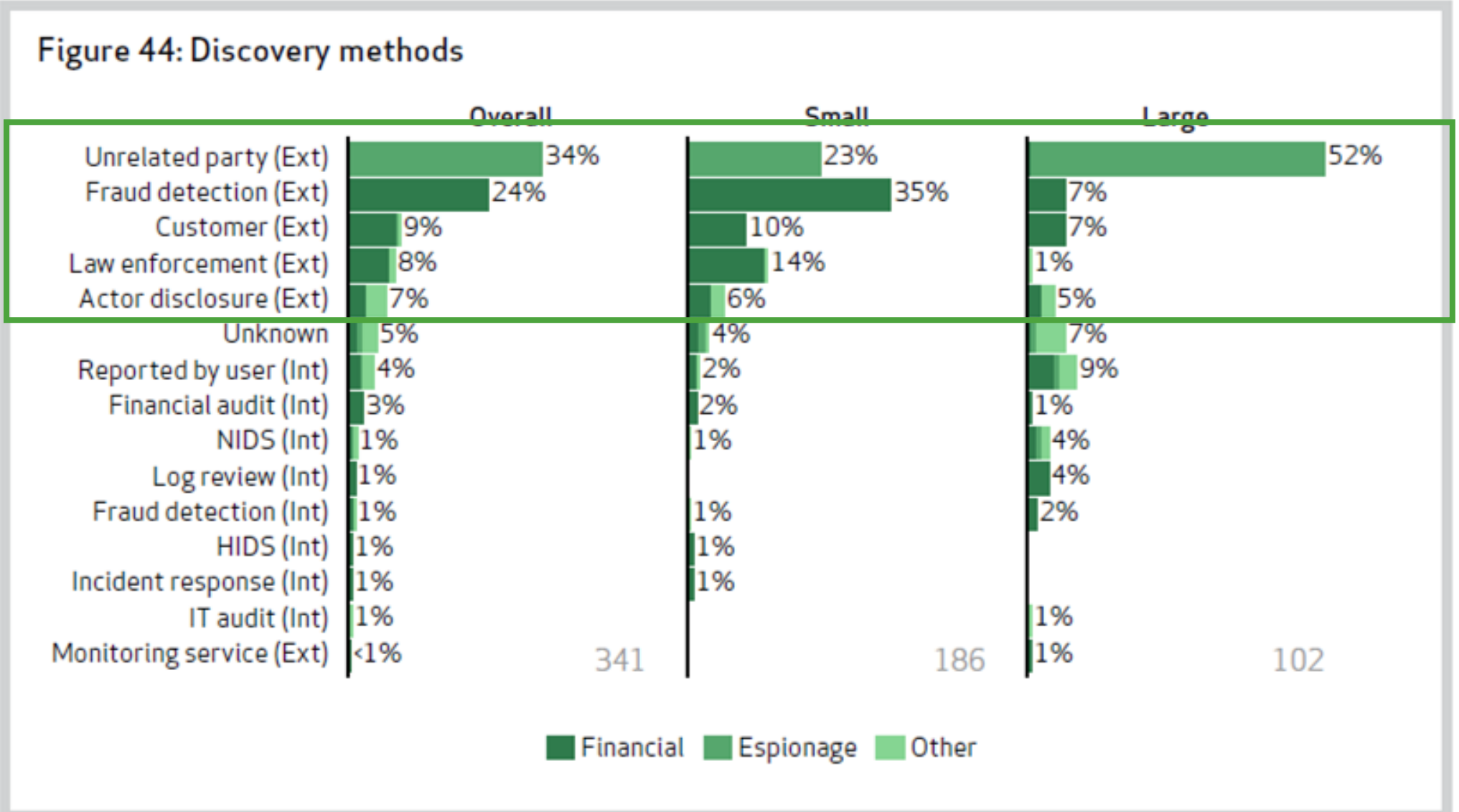
Sequence of events

Compromise
Exfiltration
Discovery
Containment



Sources: Verizon, 2013 Data Breach Investigations Report

Discoveried by…



Sources: Verizon, 2013 Data Breach Investigations Report

And than there is:

state-sponsored cyber attack,
cyber-terrorism,
cyber-espionage,
cyber-warfare!

Source: http://www.deloitte.co.uk/ers/cyber/companies.htm

Hacking is an industry and it is targeting you! because it is easy!

YOU ARE A TARGET

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- *Your bank or financial accounts, where they can steal or transfer your money.*
- *Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.*
- *Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.*
- *Your UPS or Fedex accounts, where they ship stolen goods in your name.*

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- *All the names, email addresses and phone numbers from your contact list.*
- *All of your personal or work email.*

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- *Your online gaming characters, gaming goods or gaming currencies.*
- *Any software licenses, operating system license keys, or gaming licenses.*

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- *Sending out spam to millions of people.*
- *Launching Denial of Service attacks.*

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

www.securingthehuman.org/ouch

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- *Your Facebook, Twitter or LinkedIn account.*
- *Your email accounts.*
- *Your Skype or other IM accounts.*

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- *Hosting phishing websites to steal other people's usernames and passwords.*
- *Hosting attacking tools that will hack people's computers.*
- *Distributing child pornography, pirated videos or stolen music.*

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- *Your credit card information.*
- *Your tax records and past filings.*
- *Your financial investments and retirement plans.*

Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- *Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.*
- *Encrypting all the data on your computer and demanding payment to decrypt it.*
- *Tracking all websites you visit and threatening to publish them.*

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com

378 millions victims per year or

Sources: ”2013 Norton Cybercrime Report”

378 millions victims per year or
1+ millions per day or

Sources: ”2013 Norton Cybercrime Report”

378 millions victims per year or
1+ millions per day or
12 victims per second

Sources: ”2013 Norton Cybercrime Report”

THE ODDS OF	
1. Being Struck By Lightning	576,000 to 1
2. Dating A Supermodel	88,000 to 1
3. Getting A Hole In One	5,000 to 1
4. Having Your Identity Stolen	200 to 1
5. Losing Your Cell Phone	15 to 1

Odds of being individually hacked in the next twelve months:

4 to 1

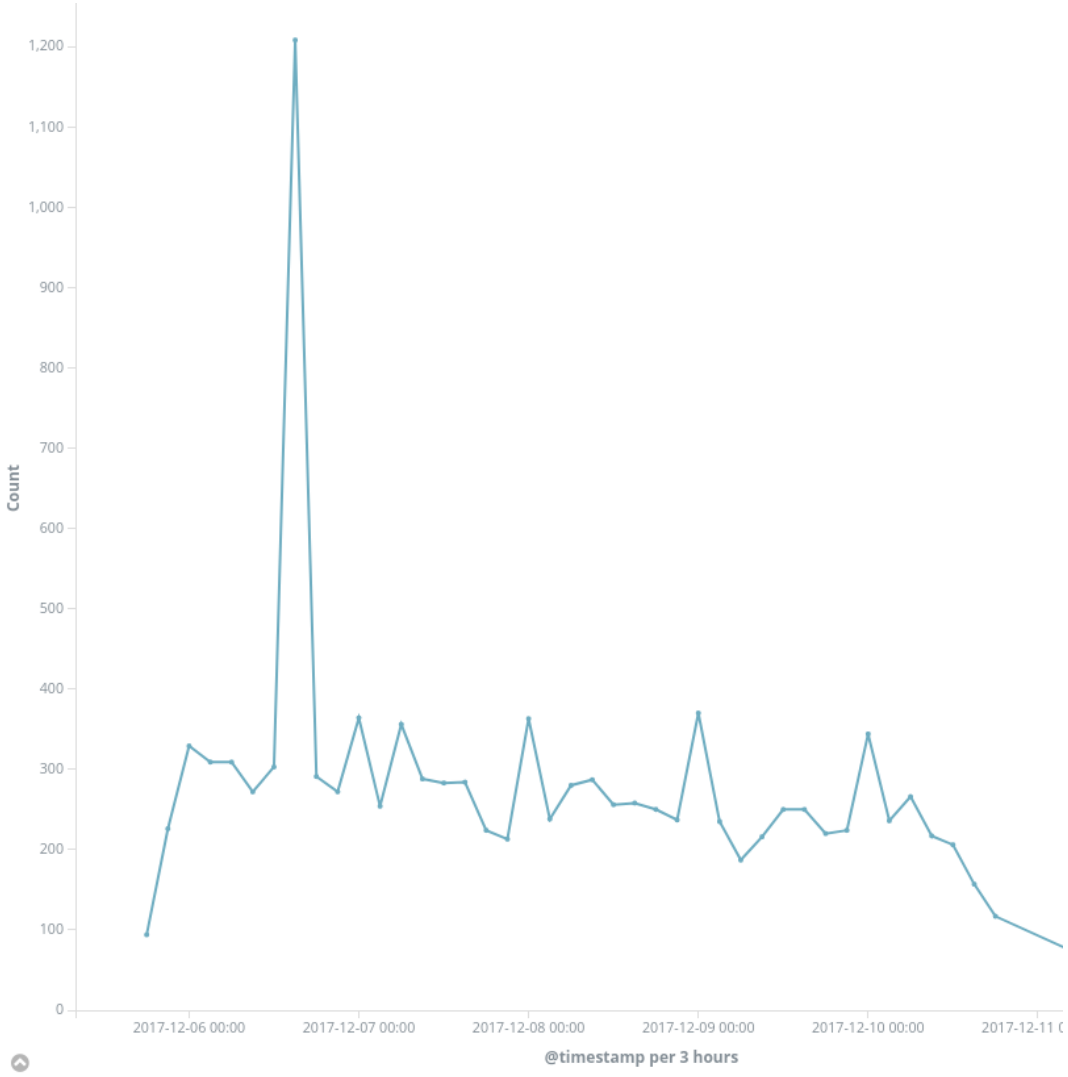
THE ODDS OF	
1. Being Struck By Lightning	576,000 to 1
2. Dating A Supermodel	88,000 to 1
3. Getting A Hole In One	5,000 to 1
4. Having Your Identity Stolen	200 to 1
5. Losing Your Cell Phone	15 to 1

FBI Director Robert Mueller

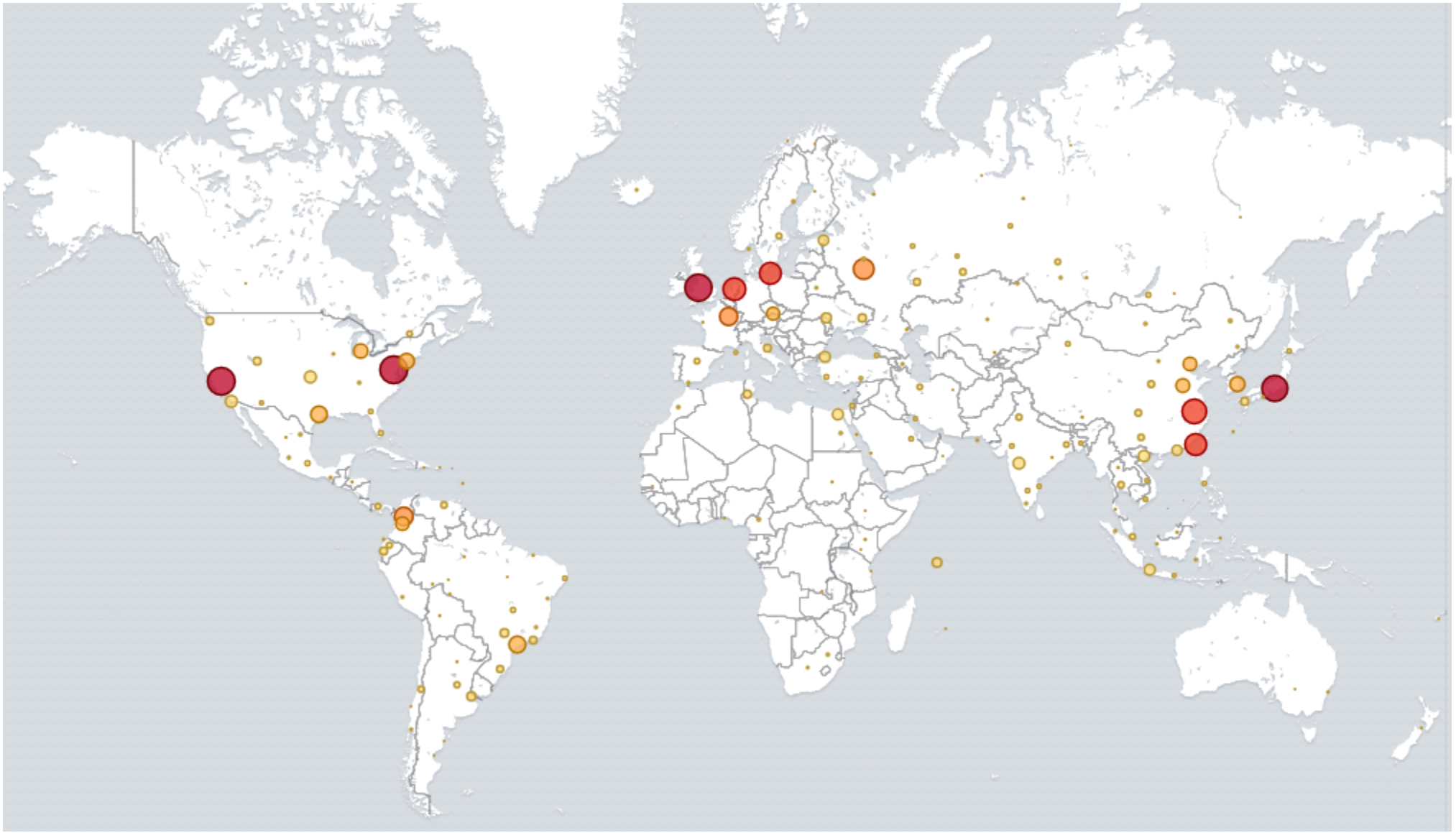
"There are only two types of companies: Those that have been hacked, and those that will be."

Sources: http://www.foxnews.com/tech/2012/03/02/cyber-threats-will-become-top-worry-fbi-director-says/

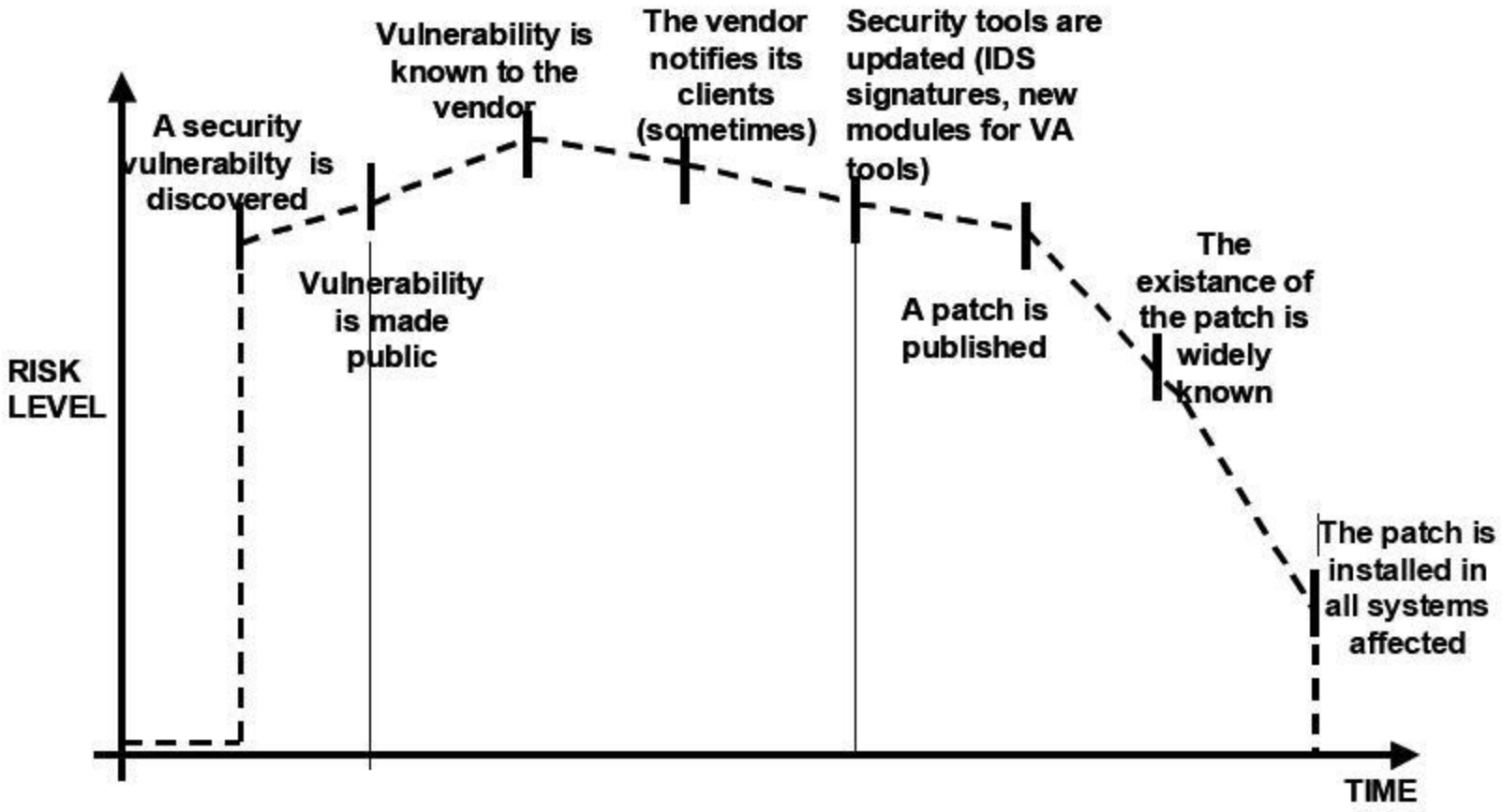
And it is really real!



Really real…

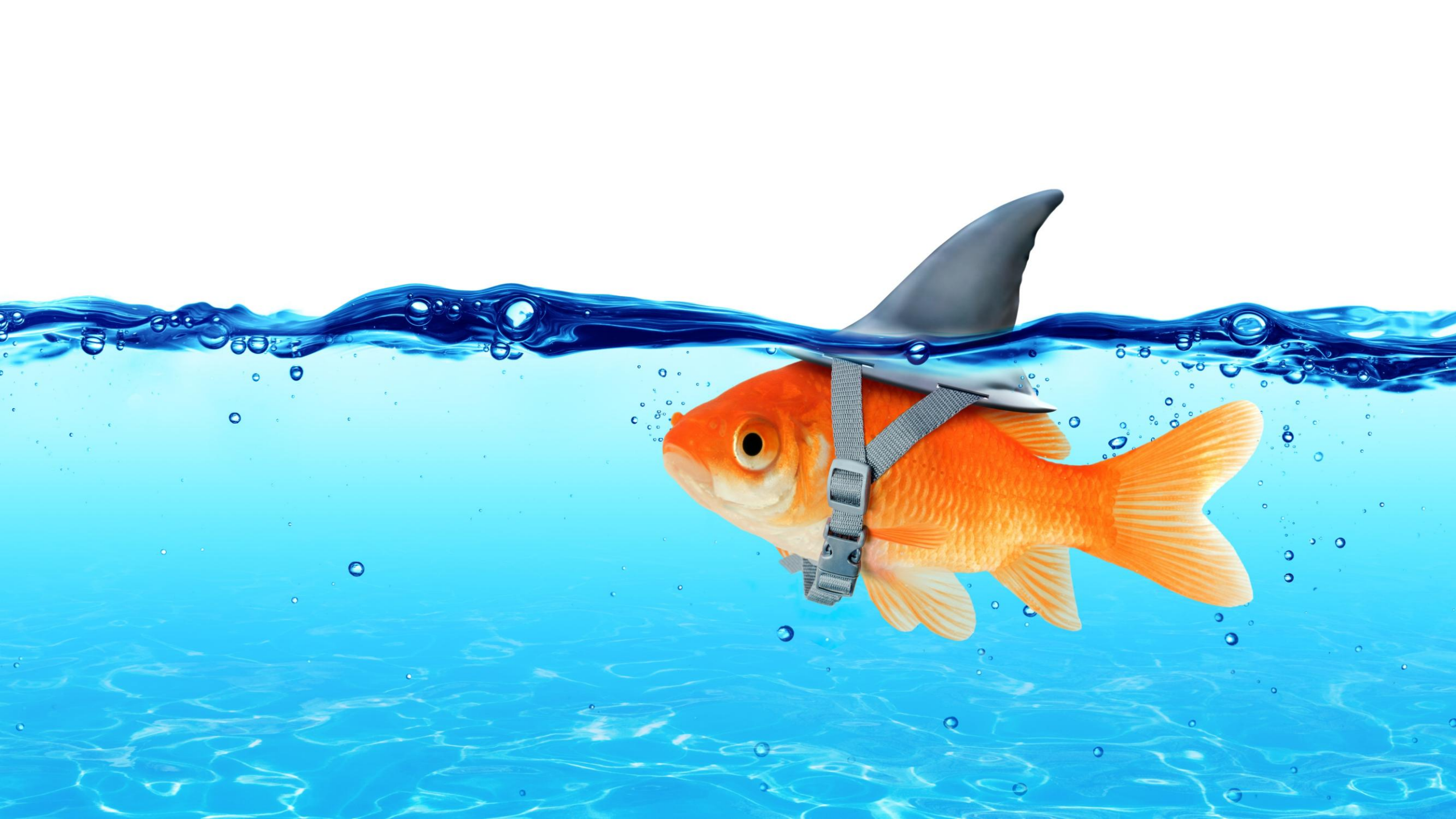


Life of a vulnerability

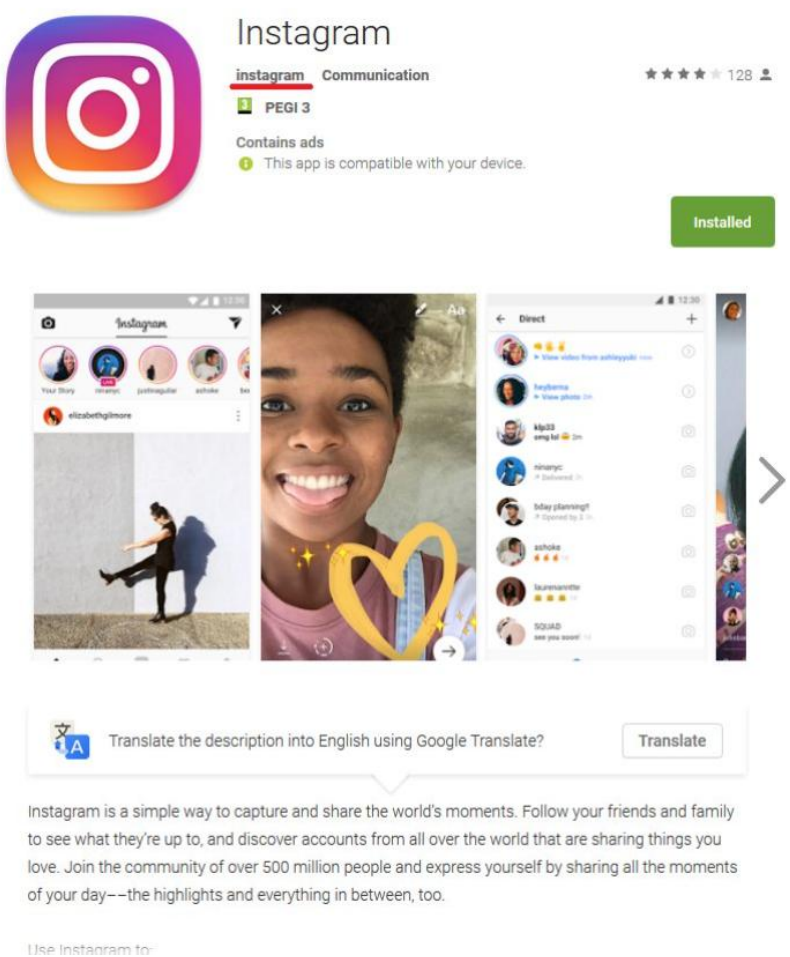


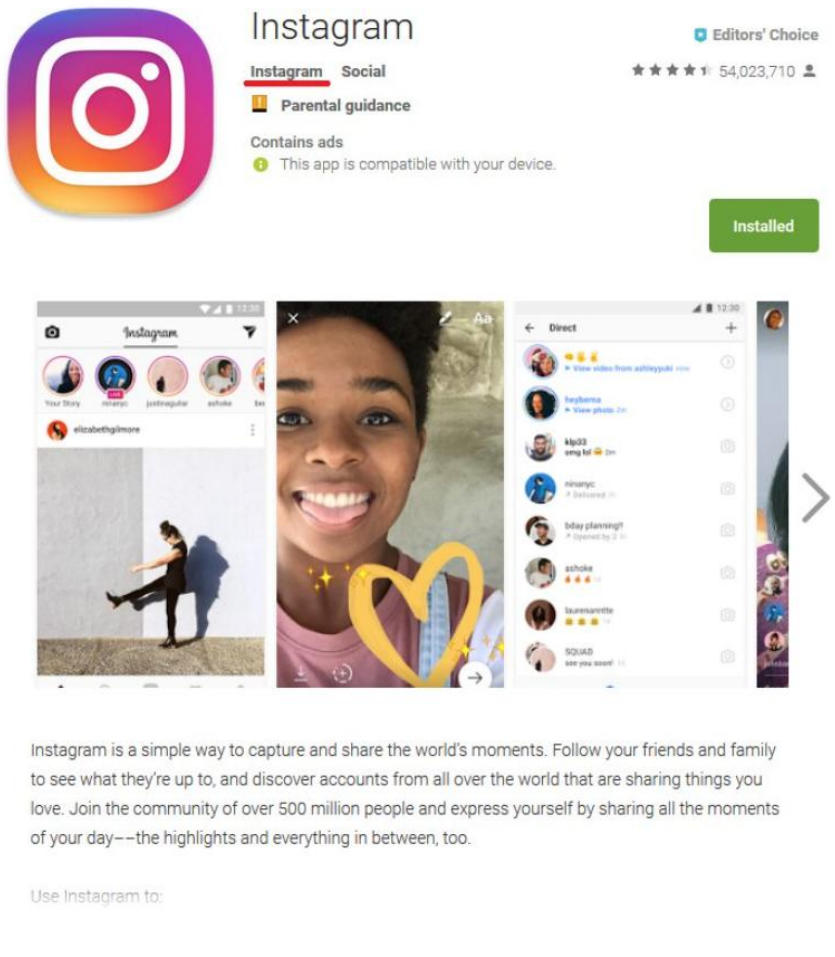
Kilde: https://www.owasp.org/index.php/Testing_Guide_Introduction

Hacking is an industry and it is targeting you! because it is easy!



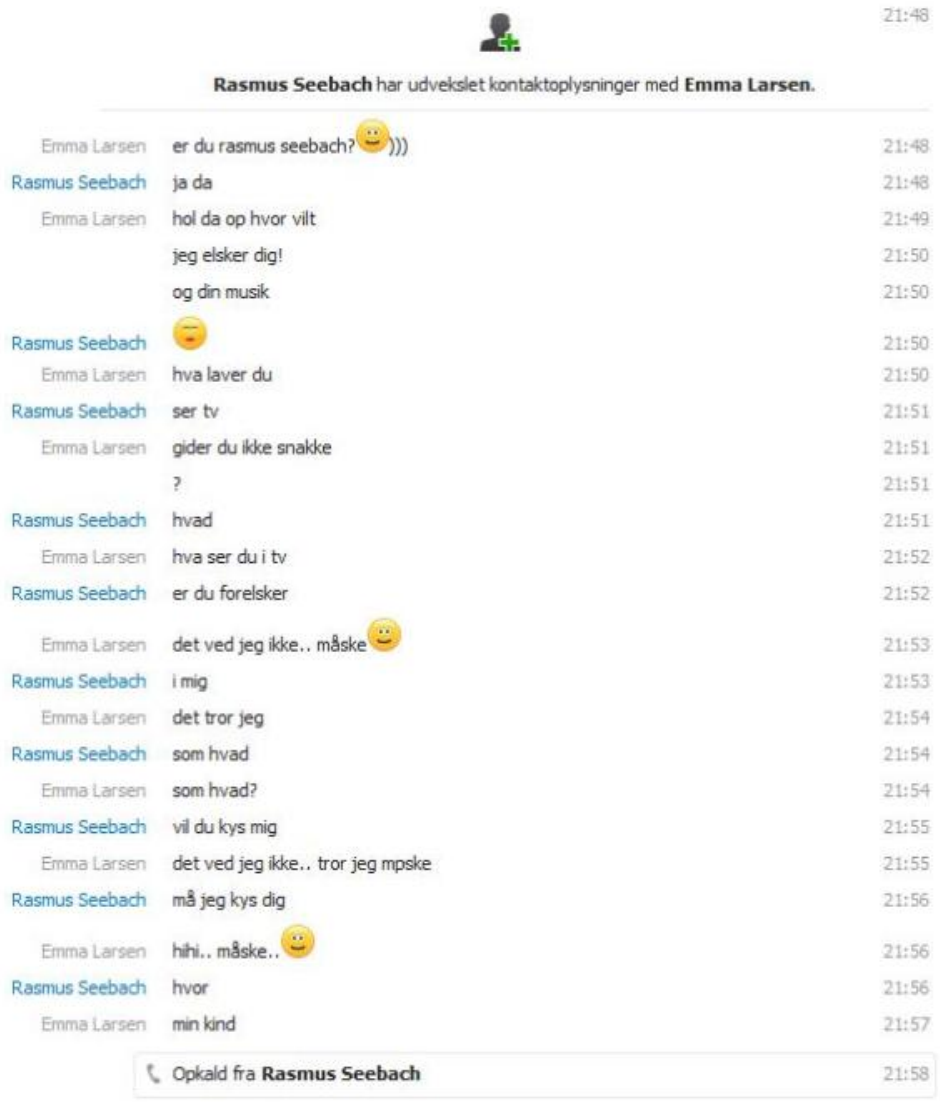
Security is hard … even for us!





Sources: https://twitter.com/LukasStefanko/status/909753129478082565

The fake Rasmus Seebach …



Source : https://www.mx.dk/nyheder/danmark/story/13307249

How many Rasmus Seebach are there?

Rasmus Seebach

36 years old

SPONSORED:

Vital Records | Social Profile | Username Report

ASSOCIATED WITH: Ditte Marie Lund , Ida Marie Steensborg , Flemming Daniel Frederiksen , Ulla Rostgaard Poulsen , Frederik Lassen Hesseldahl , Nina Maglehøj Skjødt , Steffen Rise Andersen , Mette Hestehave Hansen , Jette Güldner Knudsen , Kamilla Juel Sørensen , 6 more »

Rasmus Seebach, rasmus.seebach, rasmus.seebach.9 - Svenstrup & ...
facebook.com/people/_/546092605
Personal Web Profile - Facebook

Rasmus Seebach, 36 years old
en.wikipedia.org/wiki/Rasmus_Seebach
The Free Encyclopedia - Wikipedia

Rasmus Seebach, Kristian Klinge (krillerone)
flickr.com/people/37901254@N02
Online Photo Album - Flickr

facebook.com/people/_/100003858655822
Personal Web Profile - Facebook

Rasmus Seebach, rasmus.seebach.75
facebook.com/people/_/100003157308966
Personal Web Profile - Facebook

Rasmus Seebach, rasmus.seebach.7
facebook.com/people/_/100003795579810
Personal Web Profile - Facebook

Rasmus Seebach, rasmus.seebach.1238
facebook.com/people/_/100003522528600
Personal Web Profile - Facebook

Rasmus Seebach, rasmus.seebach.12
facebook.com/people/_/100001115043646
Personal Web Profile - Facebook

Rasmus Seebach, rasmus.seebach.750
facebook.com/people/_/100004124554813
Personal Web Profile - Facebook

Rasmus Seebach Seebach
facebook.com/people/_/100000640895528
Personal Web Profile - Facebook

Billedkilde: www.pipl.com

Phishing

Fra: Info Nets <noreply@nets.com>
Dato: 8. marts 2017 kl. 10.07.57 CET
Til:
Emne: Adgang Til Dine Konto

Kære kunder Nets,

Det ser ud til, at en anden bruger din konto.

For din sikkerhed, har vi blokeret din konto
Vi har brug for nogle oplysninger for at løse dette problem

> Klik her https://www.nets.eu/dk-da/I%C3%B8sninger/dankort/022136

© Nets i Danmark (HQ)-kontoteamet

POST

Du har uforløste pakken

Vi har modtaget din pakke **CT5389919582DK** på **2015/09/21**. Courier var ude af stand til at levere denne pakke til dig

Få og udskrive forsendelsesetiketten, og vise det på det nærmeste posthus for at få din pakke.

Få en adresselapp

Hvis pakken ikke er modtaget inden 20 arbejdsdage PostNord AB vil være berettiget til at kræve kompensation fra dig - 55 kroner for hver dag i at holde. Du kan finde oplysninger om fremgangsmåden ved og betingelserne af pakken holde i det nærmeste kontor.

Dette er en automatisk genereret meddelelse. Klik her for at afmelde

Fra: **Skat.dk** <skat@skat.dk>
Dato: 1. okt. 2013 12.00
Emne: ID:38933 - tilbagebetaling af skat - DKK 6940,00
Til: XXX

SKAT

Bemærk: Tilbagebetaling af skat for året 2012

Kære skatteyder,

Vores registreringer viser, at du er kvalificeret til en tilbagebetaling af skat af:
DKK 6940,00

For at få adgang til din skat tilbagebetaling, klik venligst her.

Udfyld venligst formularen indtil d. **02-10-2013.**
Den hurtigste og nemmeste måde at modtage din tilbagebetaling på er ved direkte inc
check/opsparingskonto.

Vores hovedkontor adresse kan findes på vores hjemmeside på
http://www.skat.dk

Source : http://www.it-blogger.dk/post-nord-virus-rammer-danmark/, http://skat.dk/SKAT.aspx?oId=68747 og https://www.nets.eu/dk-da/digital-sikkerhed/Pages/Phishing.aspx

An attack is low risk and high ROI

Dedicated server (powerful servers)	0.50 – 1 (10 – 20)
1000 downloads in EU	80
Programming Services	? (100 – 250)
1 day DDoS	30 – 70
Cheap email spamming	10 per 1,000,000 emails
Email spamming, custom database	50 – 500 per 50,000 to 1,000,000 emails
SMS spamming	3 – 150 per 100 – 10,000 SMS
1 hour call flooding	2 – 5
Bots	200 for 2,000 bots
Copy of scanned EU passport	5
Windows 7 Ultimate license	7
Fake website	5 – 20
Credit card details	2 – 90 (add 190 for physical card)
Bank Credentials (with guaranty)	80 – 700
Purchase and forward of products	30 – 300

Sources: "Russian Underground 101" by Trend Micro and "The Cyber-crime black market uncovered" by Panda Security

Return of investment

Fake web site	$20
1,000,000 spam emails	$10
5 Servers to host site	$70
	$100

Break-even at 0.005% (or 50) people entering credit card details

Stay Safe

WelcomeSecurity
Enabling value through security

Perfect security does not exist!

You can try to prevent being compromised and you should:

- Do not use the administrator account for everyday use,
- Use a password manager to manage good passwords,
- Maintain physical control over the equipment,
- Enable automatic updates,
- Run antivirus,
- Use firewall

However, an attacker can find a "way in", therefore:

- Make several backups and at least one offline,
- Encrypt the data

Nevertheless, the easiest way in for an attacker is **YOU!**

- Do not blindly install or run programs or add-ons,
- Do not blindly provide personal information,
- Do not click on unsolicited links,

You have to prepare or it will be too late!

Stay Safe

For more information visit: www.welcomesecurity.net

WelcomeSecurity
Enabling value through security

Assume Breach
Cover the web camera when not in use

To install the web camera cover:
1. Remove double tape tabs
2. Position base over the camera lens then press firmly
3. Once installed, simply slide to open and close

Spotting wrong behavior

01 It is too good to be true…

If an offer or email is too good to be true, it probably is!

02 Immediate actions

If something requires you to do an immediate actions or something bad would happen, it may be a trick

03 Check the sender

Even if the sender appears to legit, it does not have to be the case. If an email is from a friend, give him or her a phone call to verify

04 Do not click links

If you receive a link that seems legit, consider entering it manually instead of clicking it.

05 Do no open attachment

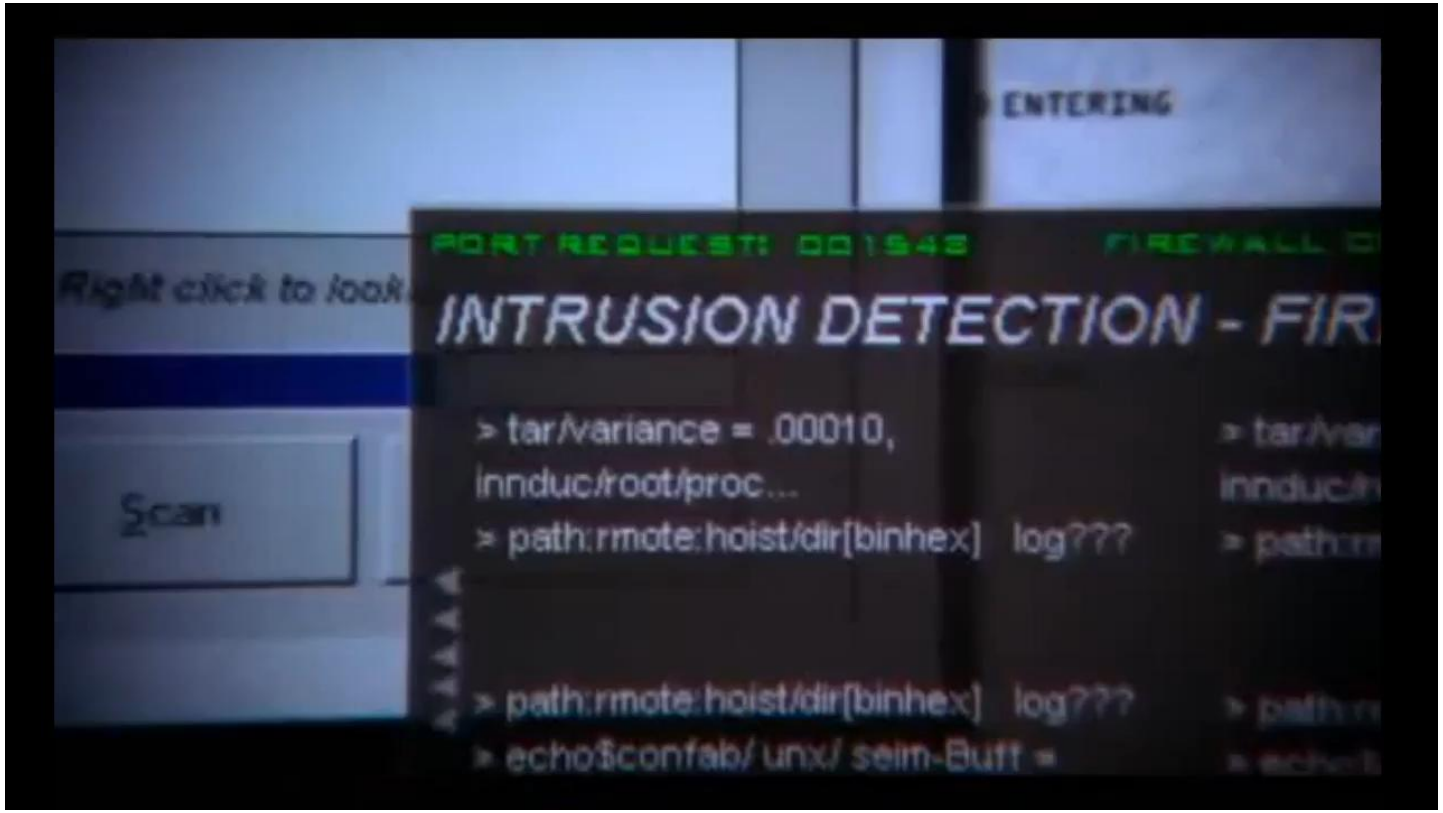
If you did not expect the attachment, do not open it or call the sender to ask what it is about

06 Be skeptical!

Enabling value through it security

Hacking

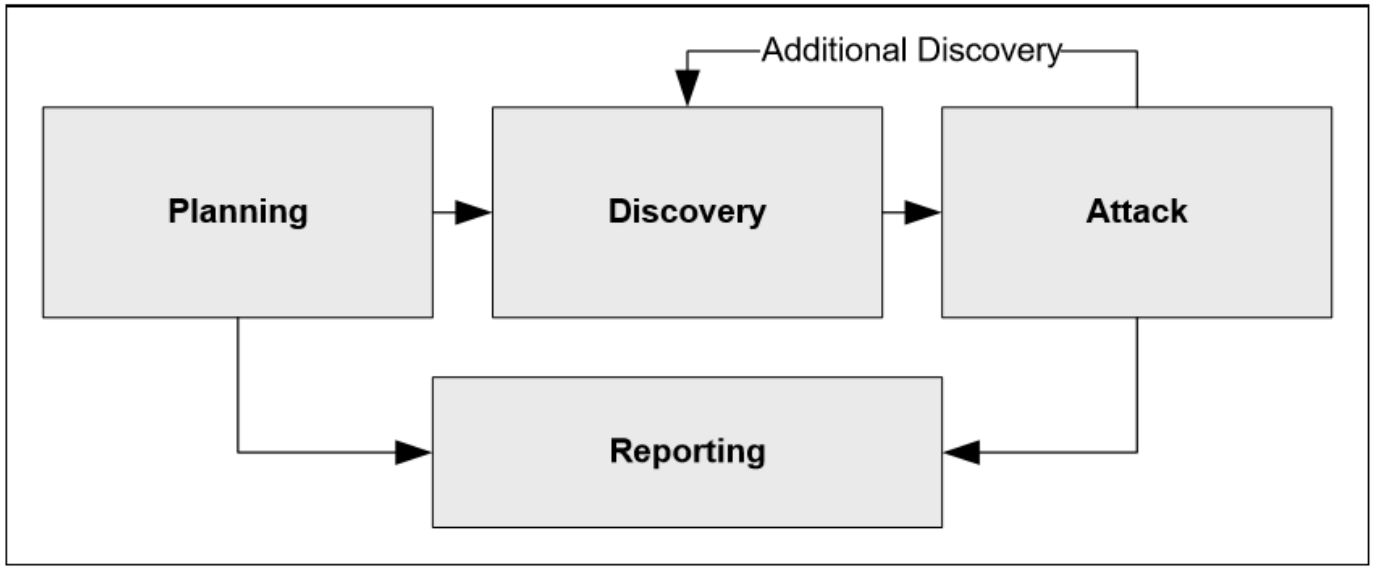
What it is not!

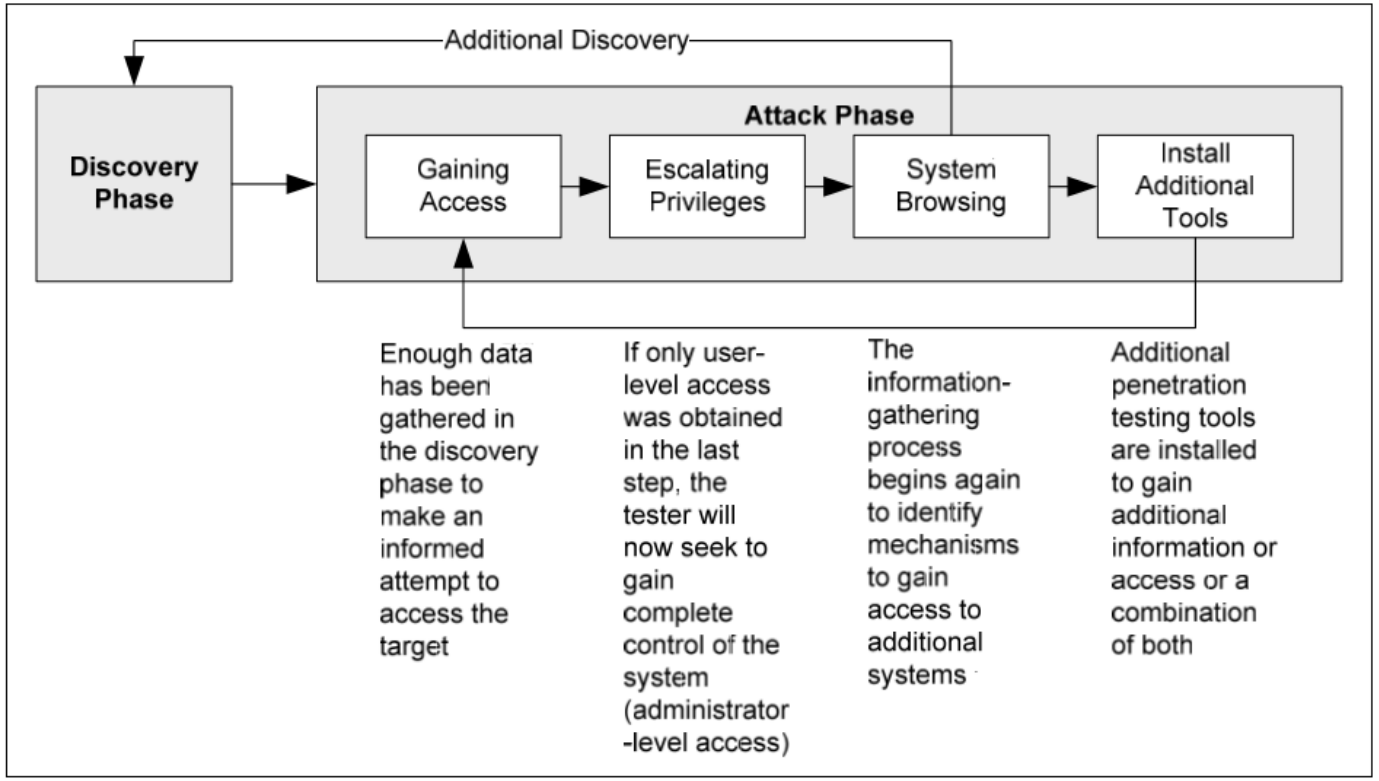


Source: http://www.youtube.com

Penetration Testing or legal hacking

Exploiting the holes





Source: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

WelcomeSecurity
Enabling value through IT security

CONTACT US

www.welcomesecurity.net

+45 2158 1410
Info@welcomesecurity.net