

I am going to hack you, are you ready!?!?

Christian Prickaerts

Amsterdam, November 2015

Fighting cybercrime since 1999

Providing threat detection
services for >10 years

Fox-IT cyber security leadership

220 employees,
dedicated to online threats

International proven track
record in over 40 countries on
5 continents






Why are we here?



Quiz!



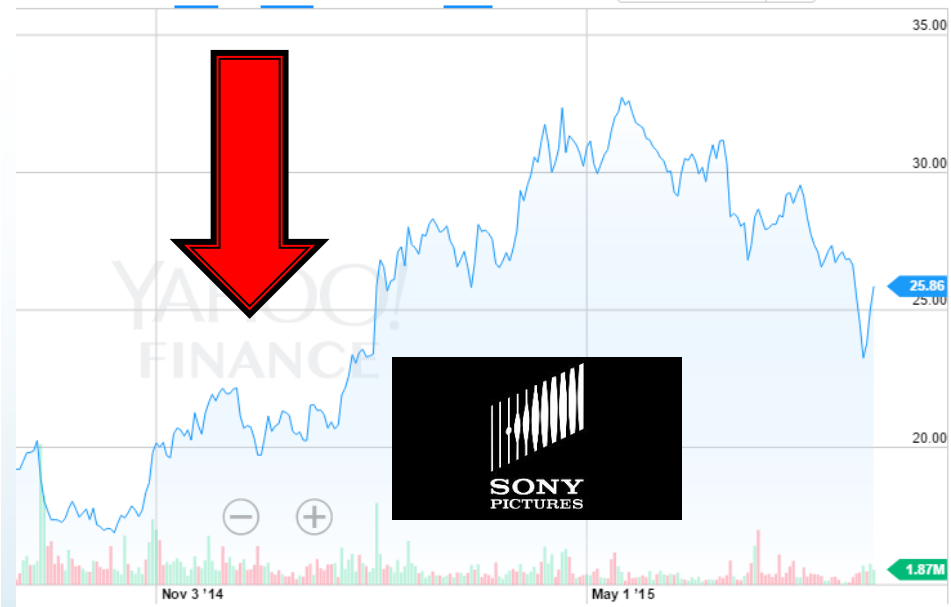
```
state      service
22/tcp     open      ssh

no exact OS matches for host

map run completed -- 1 IP address (1 host up) scanned
sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Setting root password to "Z10N0101".
System open: Access Level <9>
ssh 10.2.2.2 -l root
t@10.2.2.2's password: █
```

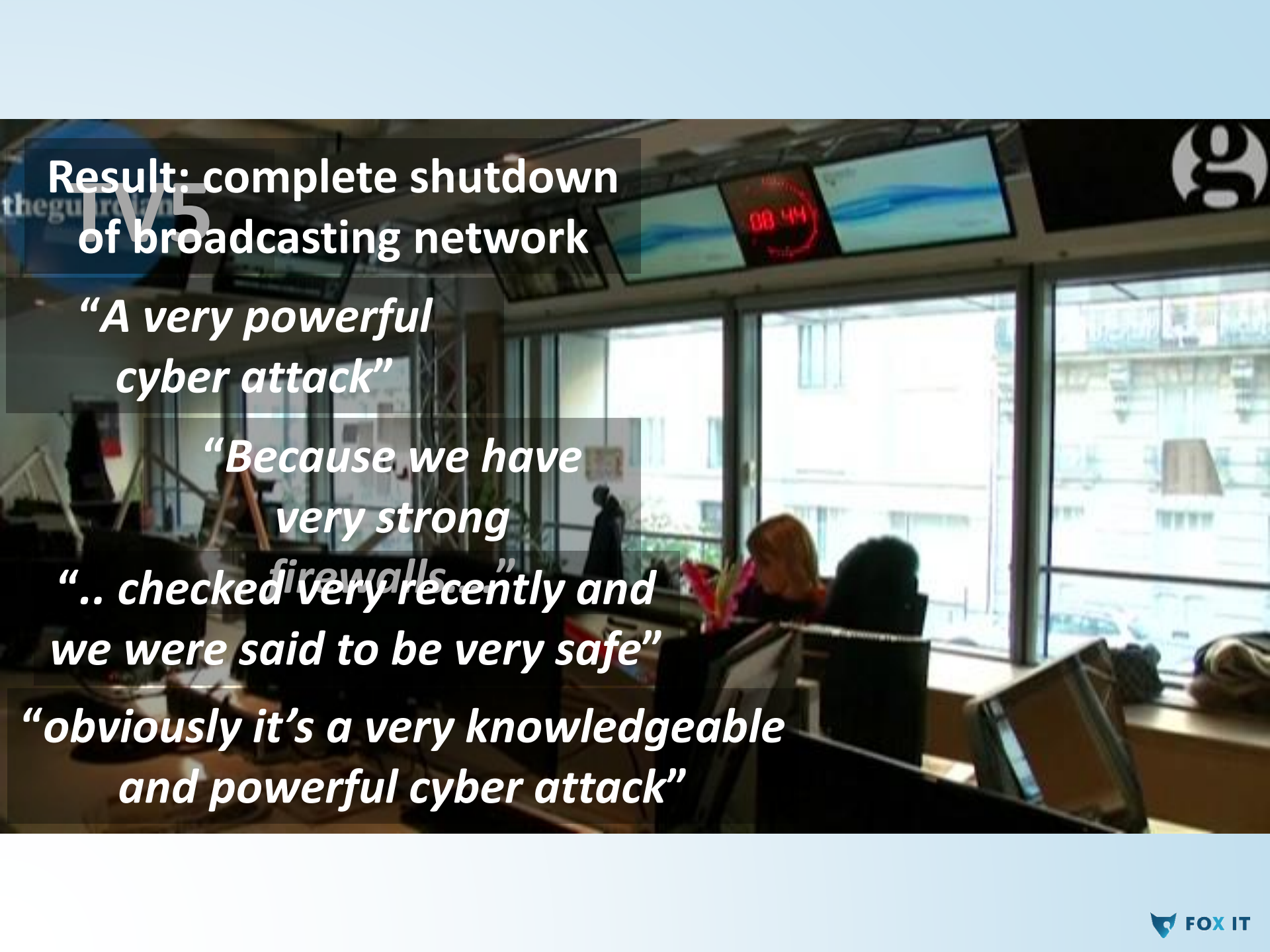
☐ ☐ enter password ☐

Who recently experienced a cyber security incident?



What happened?





Result: complete shutdown
of broadcasting network

*“A very powerful
cyber attack”*

*“Because we have
very strong*

*“.. checked very recently and
we were said to be very safe”*

*“obviously it’s a very knowledgeable
and powerful cyber attack”*



Christian Prickaerts

1st • PREMIUM

Manager Fox-IT Managed Security Services


The Hague Area, Netherlands | Computer & Network Security

Current Fox-IT, Stichting Geschillenoplossing Automatisering, SANS Institute
Previous Fox-IT, TRIFORENSIC, The Maastricht Forensic Institute
Education Leiden University

Send a message

500+
connections

 <https://nl.linkedin.com/in/christianprickaerts>

 Contact Info

Background



Summary

Highly experienced information security professional with experience in a wide variety of cases. Very passionate about technology and security in general. Always striving to set high standards and provide an example to others. Deems it important to share ones experience and knowledge. As a teacher able to convey technical complex topics to the non-technical.



Experience

Manager Fox-IT Managed Security Services

Fox-IT

April 2015 – Present (2 months) | Delft

Responsible for overall Fox-IT MSS business strategy and business development. Management of Fox-IT Managed Security Services team. Coordinating team skill development and managing key accounts. Spearheading Security Operating Center senior staff development.



Let's get started!

People Also Viewed



Ronald Prins ✓

Founder and CTO of Fox-IT IT Security

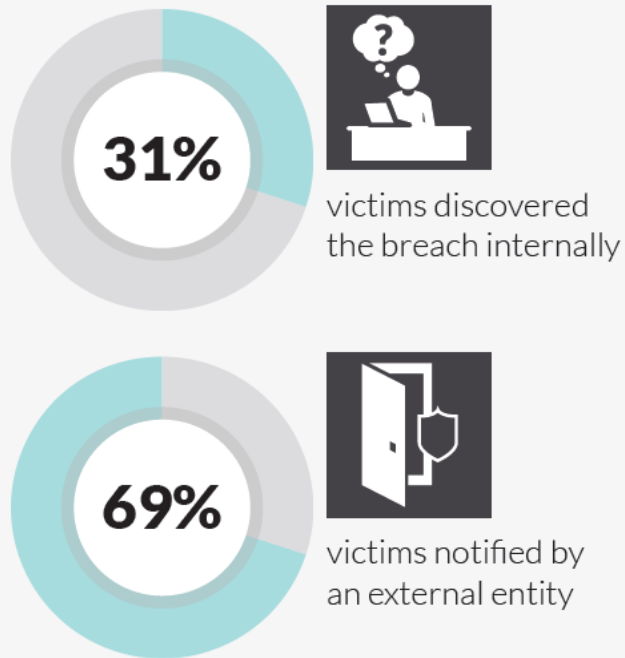


Kevin Jonkers

Manager Forensics & Incident Response at Fox-IT

So how bad is it?

How Compromises Are Being Detected



Time from Earliest Evidence of Compromise to Discovery of Compromise



median number of days that threat groups were present on a victim's network before detection

↓ 24 days less than 2013

Longest Presence: 2,982 days



2015 DATA BREACH INVESTIGATIONS REPORT

\$400 MILLION

The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.

HEALTHCARE

EDUCATION

World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 11th August 2015)

interesting story

YEAR

BUBBLE COLOUR

YEAR

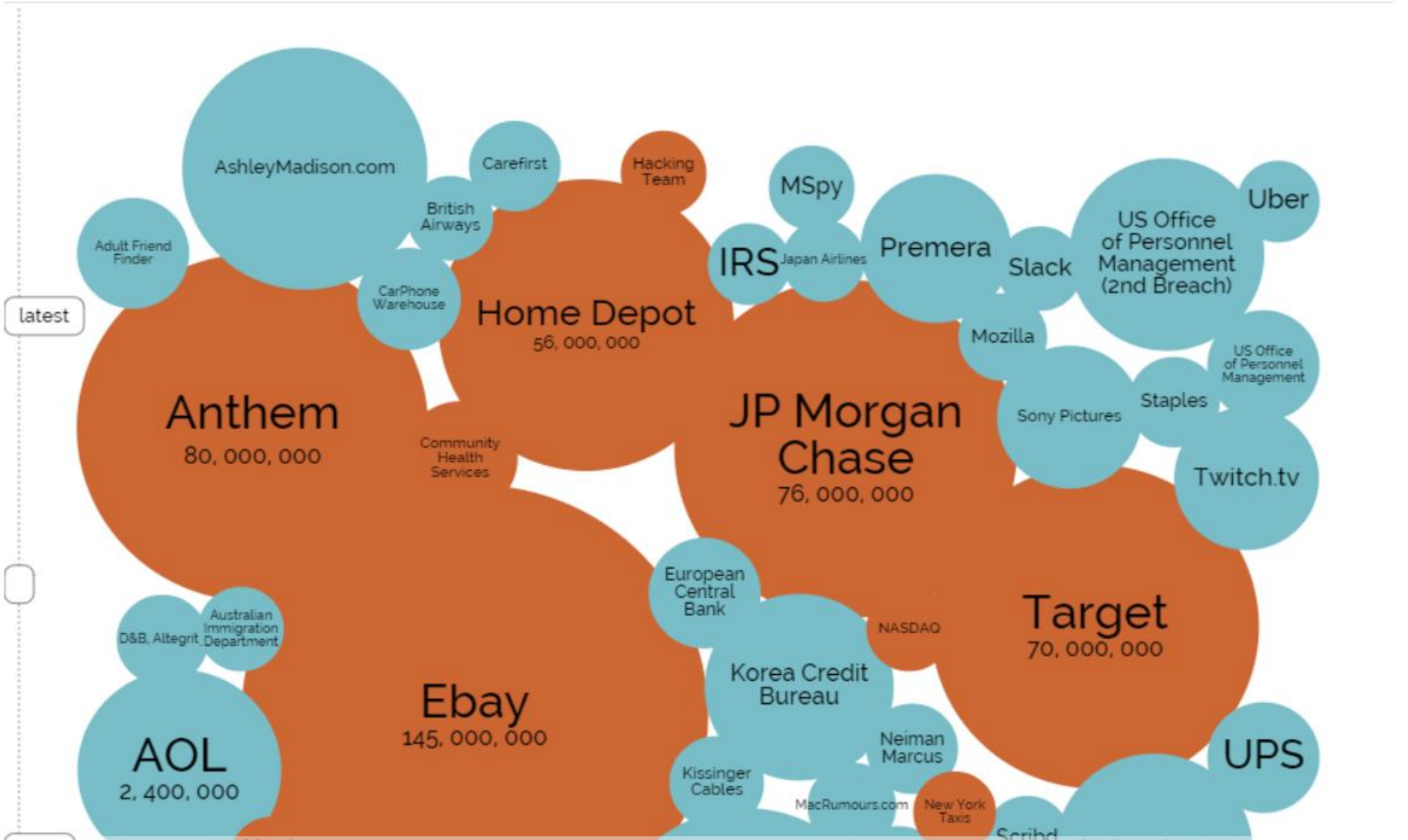
METHOD OF LEAK

BUBBLE SIZE

NO OF RECORDS STOLEN

DATA SENSITIVITY

☒ SHOW FILTER





Hackers Launch All-Out Assault on Norway's Oil and Gas Industry

August 31, 2014 // 04:17 PM EST

In what's being billed as the largest ever coordinated cyber attack, hackers have targeted some 300 different firms within Norway's oil and gas industry. The attacks were revealed last week by the Norwegian Security Authority (NSA), which had been told of the contacts."

The NSA cited 50 companies that were known to be targets, and 250 that may have been targets and who received information according to the Local, an English-language Norwegian news outlet.

Hackers attack Norway's oil, gas and defence businesses

18 November 2011 | Technology

Oil, gas and defence firms in Norway have been hit by a series of sophisticated hack attacks.

Industrial secrets and information about contract negotiations had been stolen, said Norway's National Security Agency (NSM).

It said 10 firms, and perhaps many more, had been targeted in the biggest wave of attacks to hit the country.

Norway is the latest in a growing list of nations that have lost secrets and intellectual property to cyber thieves.

The attackers won access to corporate networks using customised emails with viruses attached which did not trigger anti-malware detection systems.

Targeted attacks

The NSM said the email messages had been sent to specific named individuals in the target firms and had been carefully crafted to look like they had come from



Contracts, industrial drawings and logins were all stolen in the attacks

Hackers pop German steel mill, wreck furnace

Phishing proves too hot for plant



Maritime risk

Ship Tracking Hack Makes Tankers Vanish from View

A system used by ships worldwide to broadcast their location for safety purposes lacks security controls and is vulnerable to spectacular spoofing attacks, researchers show.

Marine & Shipping Top Five Risks

			2014 Rank	Trend
1	Intensified competition	29%	NEW	▲
2	Market fluctuations (e.g. foreign exchange rates/interest rates)	27%	NEW	▲
3	Natural catastrophes	27%	38% (1)	▼
4	Theft, fraud, and corruption	27%	24% (2)	▼
5	Political/social upheaval, war	21%	NEW	▲

Hackers working with a drug smuggling gang have previously infiltrated the computerized cargo tracking system of a port in order to identify the shipping containers in which drugs were hidden^{xviii}

THE DARKHOTEL APT ATTACKS

★★★★★ DARK HOTEL





Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



August 27, 2015

Alert Number
I-082715a-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

BUSINESS EMAIL COMPROMISE

This Public Service Announcement (PSA) is an update for the Business E-mail Compromise (BEC) PSA I-012215-PSA posted on www.IC3.gov and includes new information and updated statistical data as of August 2015.

DEFINITION

Business Email Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.¹

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices.

STATISTICAL DATA

The BEC scam continues to grow and evolve and it targets businesses of all sizes. There has been a 270 percent increase in identified victims and exposed loss since January 2015. The scam has been reported in all 50 states and in 79 countries. Fraudulent transfers have been reported going to 72 countries; however, the majority of the transfers are going to Asian banks located within China and Hong Kong.

Your personal files are encrypted.

Your personal files are encrypted.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' to connect to the secret server and follow instructions.



WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View

71:59:07

Next >>

can open it and use copy-paste for address and key.

LinkedIn Sockpuppets Are Targeting Security Researchers



Jennifer White

3rd

Mobile Security Talent Acquisition at Talent Src
London, United Kingdom | Staffing and Recruiting

Previous H&M

Education The University of Edinburgh

Send Jennifer InMail



500+
connections



 <https://uk.linkedin.com/pub/jennifer-white/b4/437/35>

Background



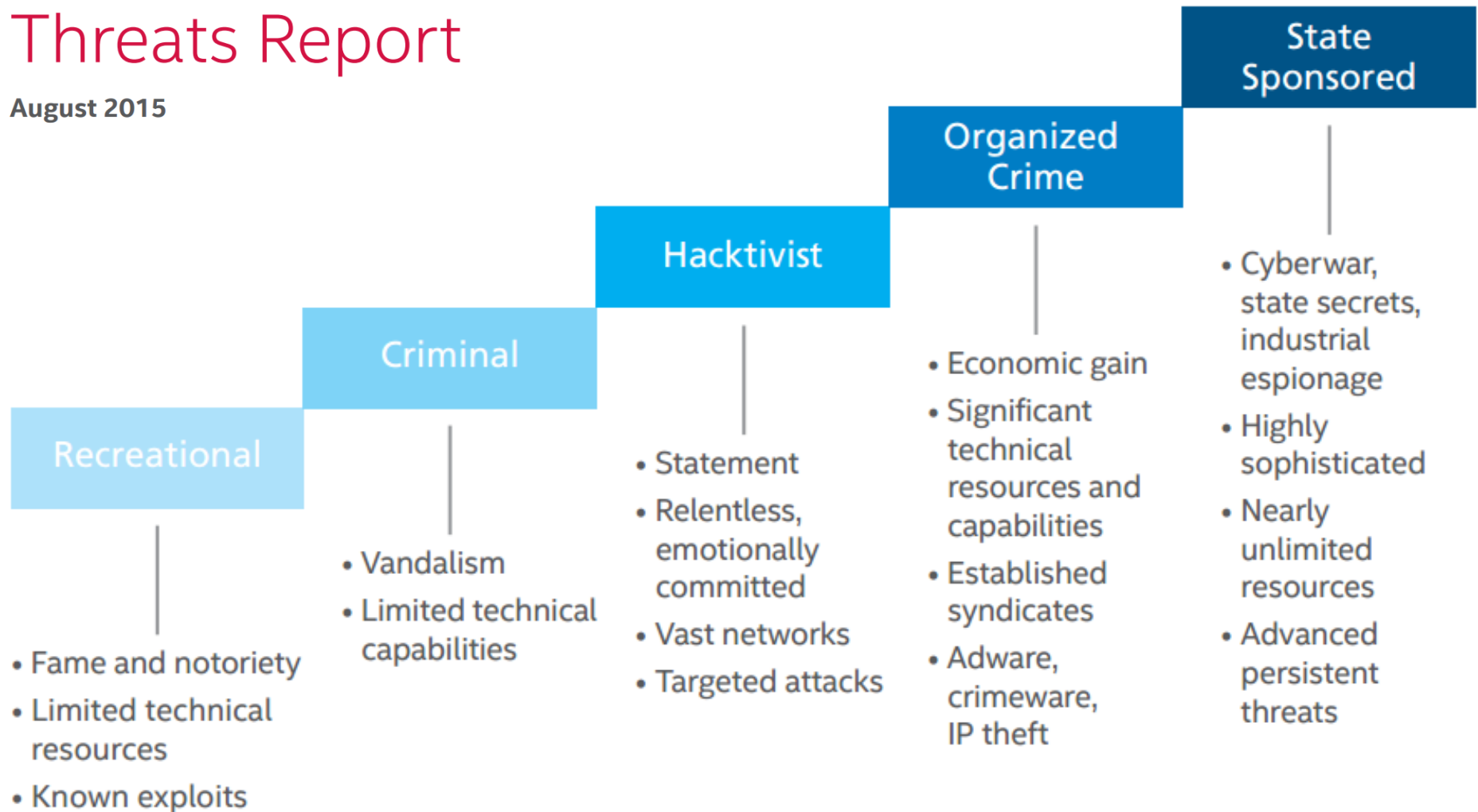
Summary

Our mission is simple.
We establish trusting and healthy relationships with the best talents in the world.

McAfee Labs Threats Report

August 2015

Changing Attacker Profiles



INCREASING RESOURCES AND SOPHISTICATION

The expansion of attacker types, their resources, and their sophistication.

damage ≠ damage



OUR NETWORK HAS BEEN BREACHED



Have a (communication) plan





FIRE

ALARM

BREAK GLASS

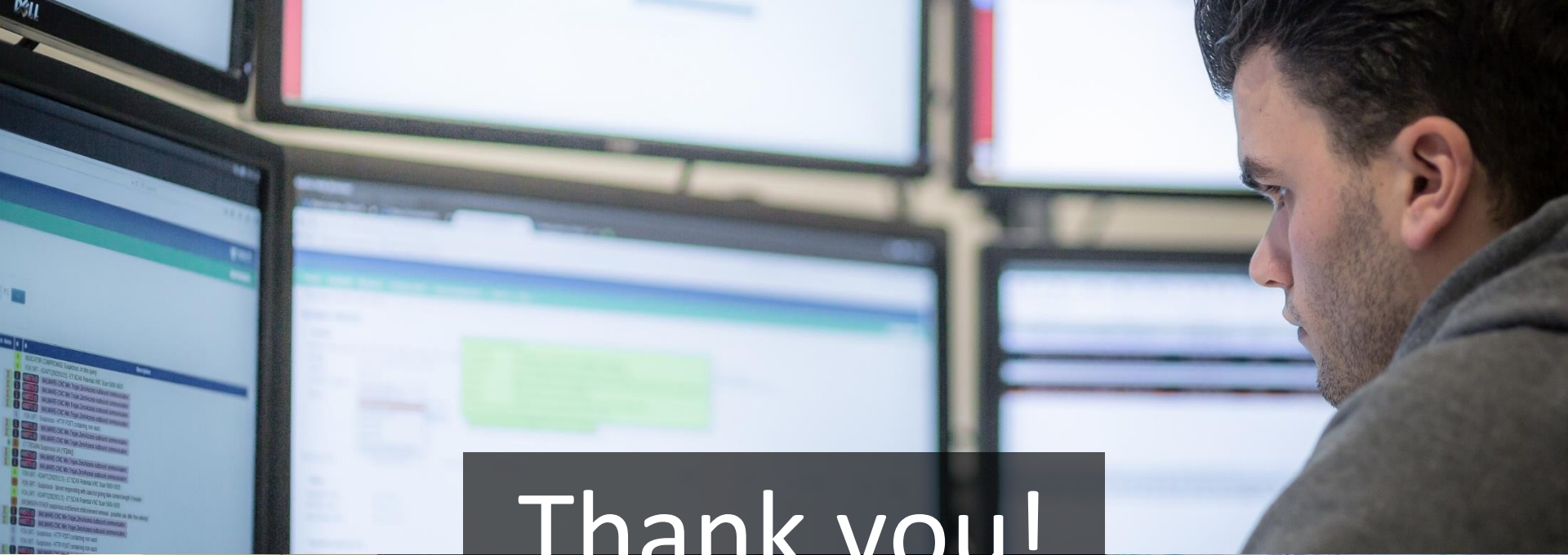
PULL DOWN

PULL HANDLE



Why should I care....





Thank you!

