The Unknown Enemies of Cyber security – learnings from the real world

Floris van den Broek

WCCT 21 November 2018

Bitdefender invests to deepen customer protection, enhance technology and expand portfolio well beyond the endpoint

Overview

- A look at the customer
- Recent changes in cyber security environment
- Comparison with physical world
- How do we prevent them
- Advanced attacks
- How DDos attacks work and how we found the criminal

Cyber security and Hacking is on the mind of most people…

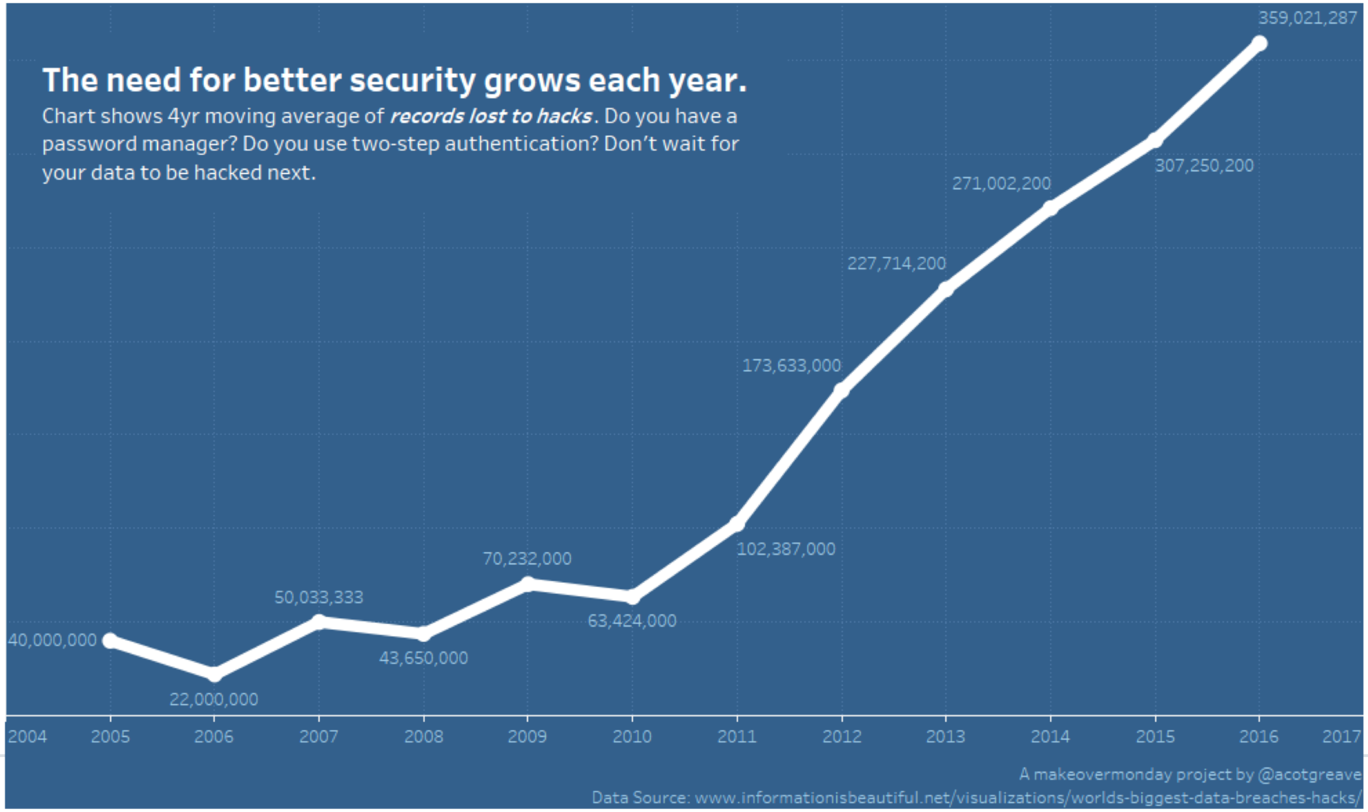
Customers are cooperating to protect themselves and others against attacks
But: They like to do things easily, without too much security related hassle

..but do customers really want to cooperate?

- Ease-of-use and Security form a trade off
- Customers mostly prefer ease-of-use and leave security for the bank to sort out => choose a low-security option and will walk away if security becomes cumbersome
- Customers will only act after harm has been done
- They have a choice (most banks offer choice of limits for low-security transaction) and don’t want to be bothered
- Success of the unsecure business models (examples)
  - PayPal
  - Credit cards in Japan
  - Use of Netflix accounts
- Best security is hardly noticable => just like in the real world
- Trust in the big names in banking

Still dataleaks are on a fast rise…

- More and more data becomes available to cyber criminals through data breaches
- The number of (known) vulnerabilities in IT systems in increasing
- Cybercriminals move from simple ‘opportunity crimes’ to advanced, well-planned attacks (advanced persistent threats)



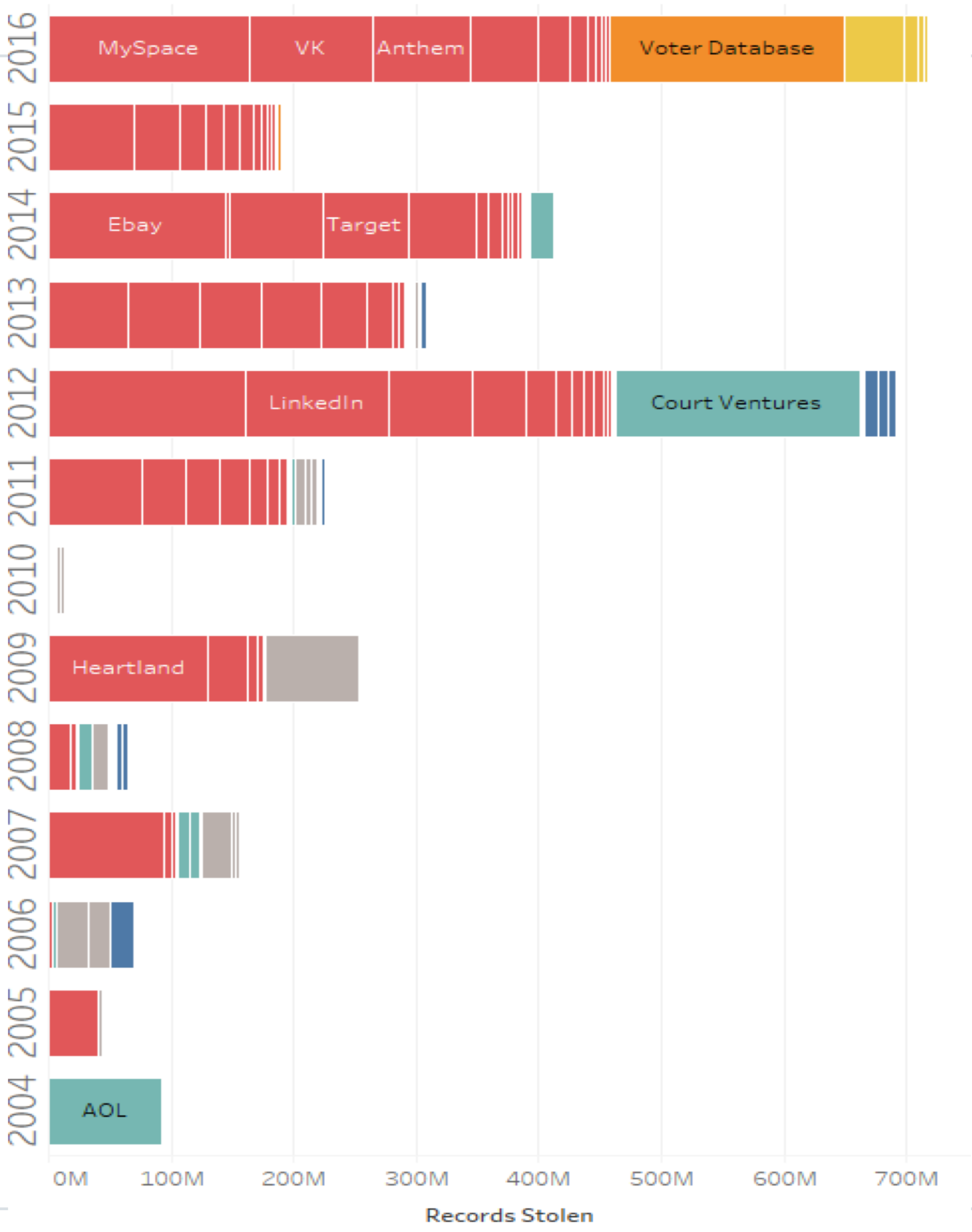
The need for better security grows each year.

Chart shows 4yr moving average of ***records lost to hacks***. Do you have a password manager? Do you use two-step authentication? Don’t wait for your data to be hacked next.

A makeovermonday project by @acotgreave

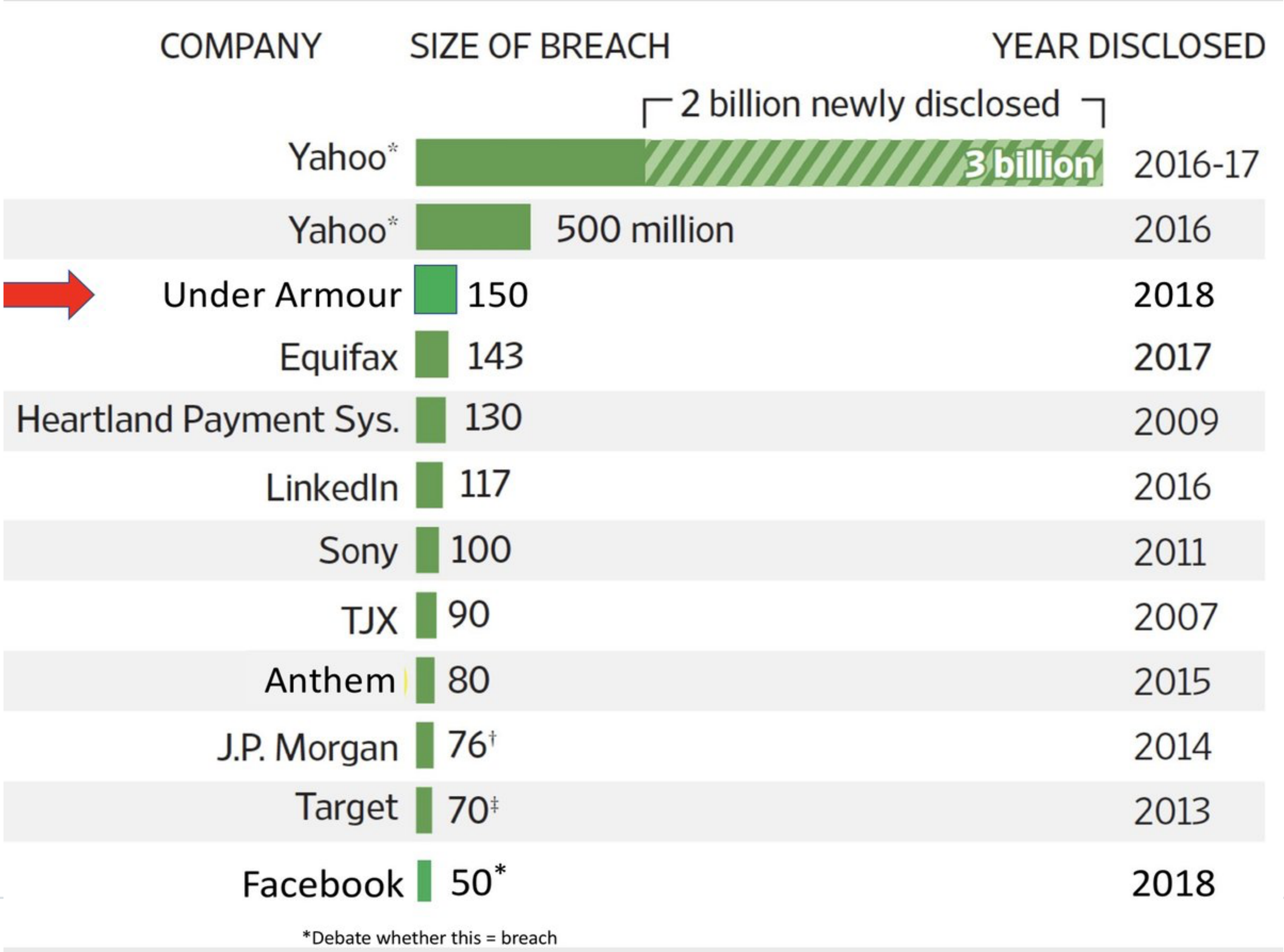
Data Source: www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Data breaches now include much citizen data (US Voters)



Verizon Threat Report 2017

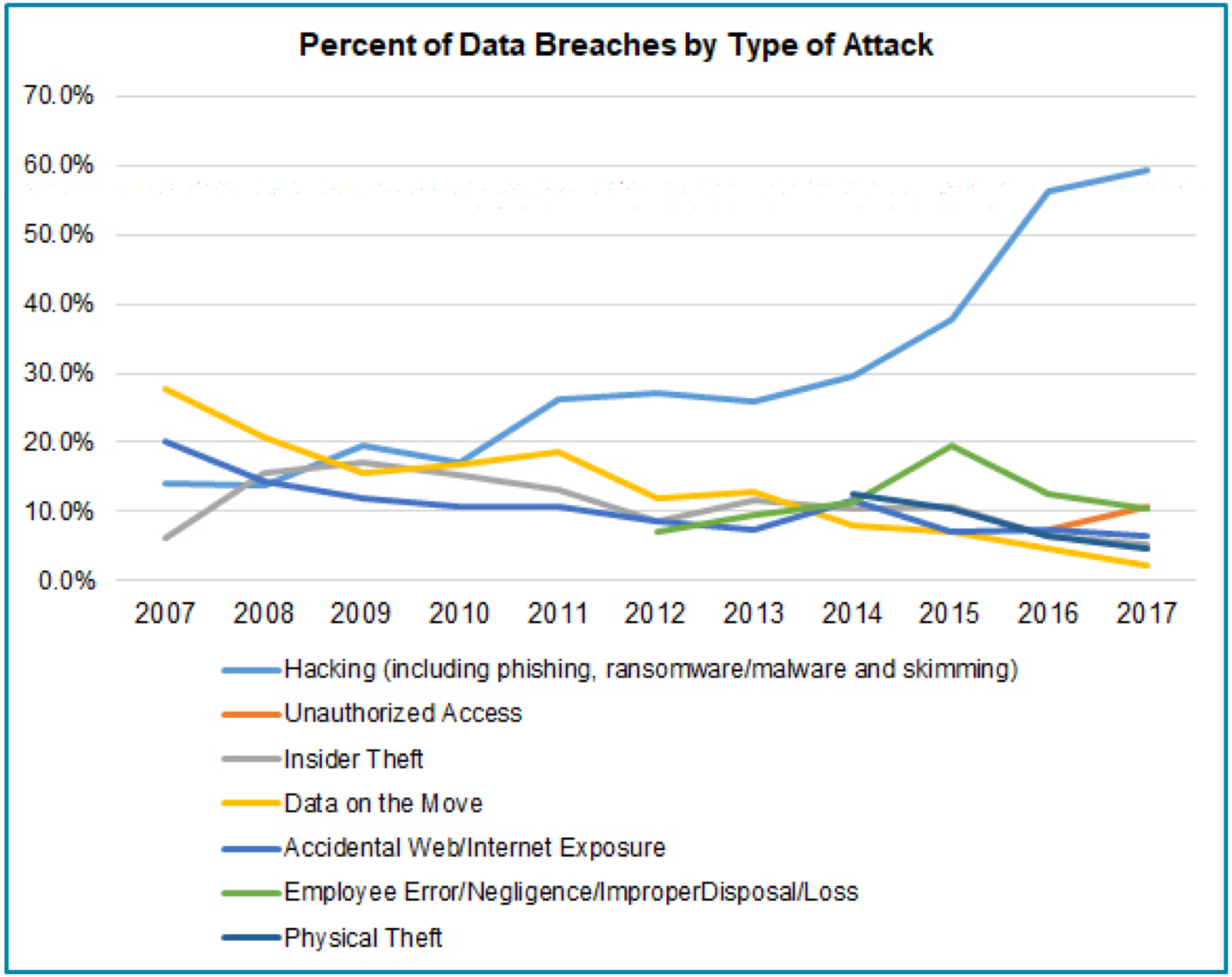
…and since GDPR, public is more aware of personal data leaks



*Debate whether this = breach

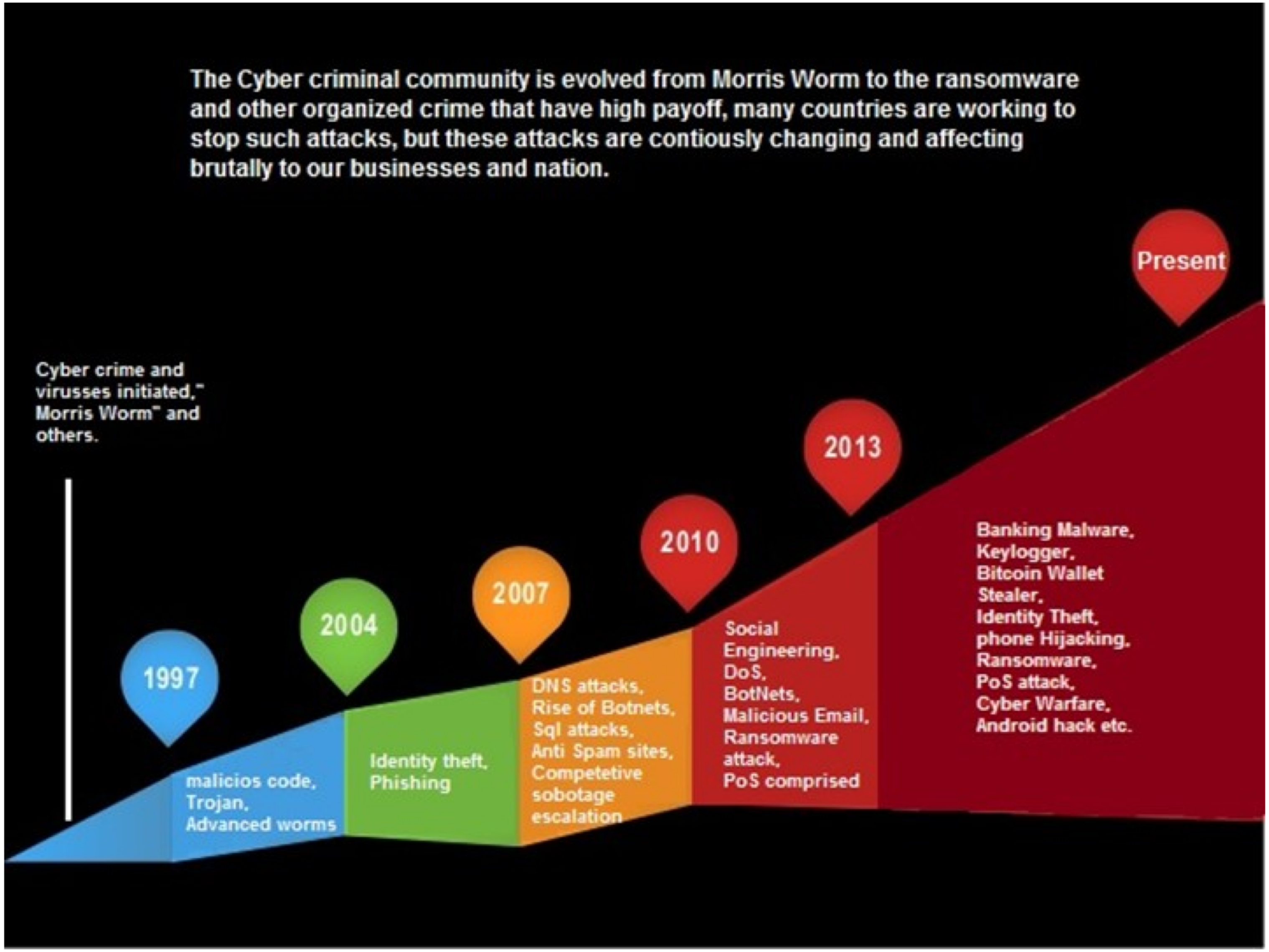
Under Armour MyFitnessPal includes much personal data

Some security measures are posting effect -> shift focus to hacking



Source: Identity Theft Resource Center, 2018

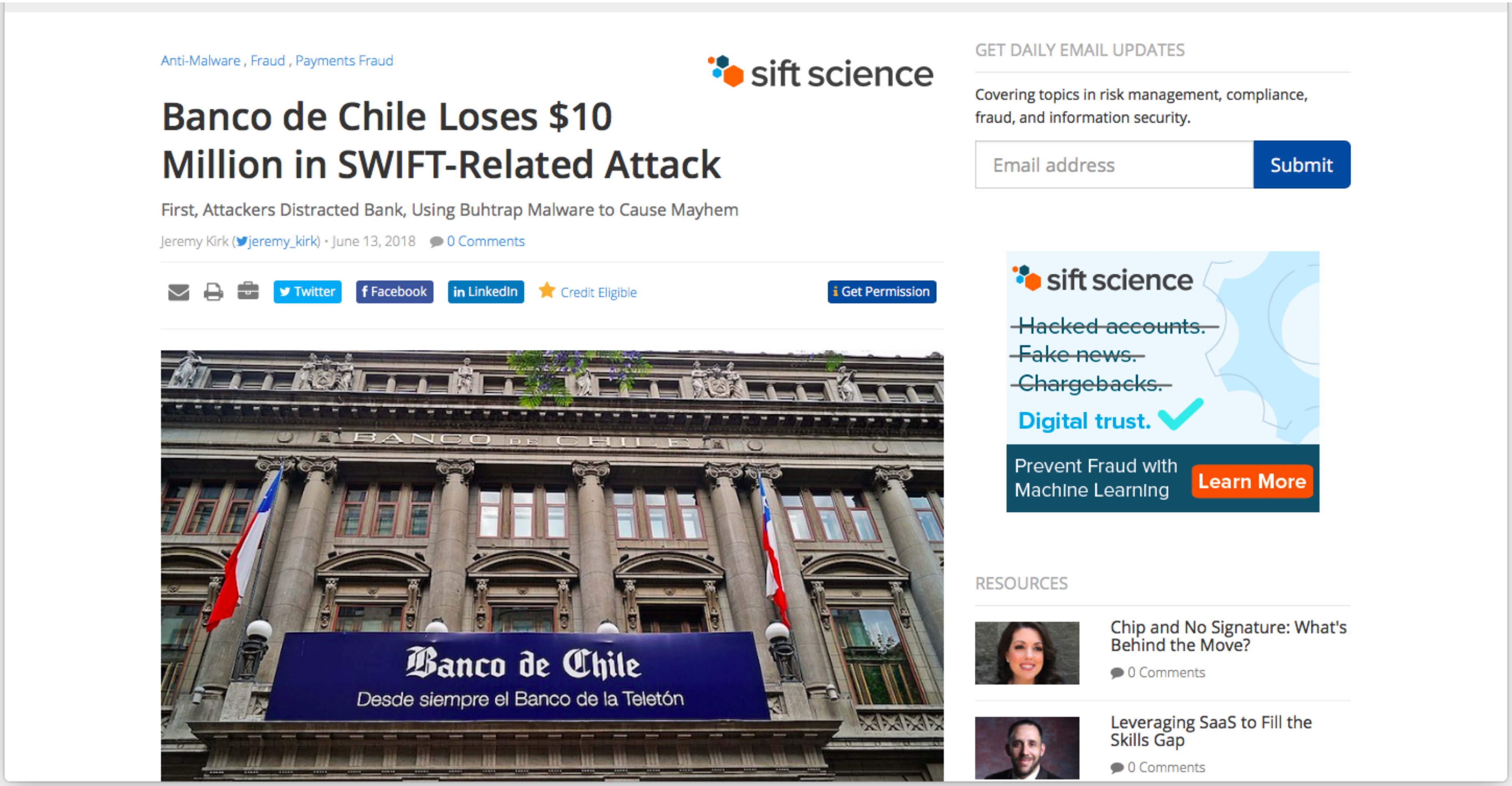
..and new hacking methods appear with more tools..



The Cyber criminal community is evolved from Morris Worm to the ransomware and other organized crime that have high payoff, many countries are working to stop such attacks, but these attacks are contiously changing and affecting brutally to our businesses and nation.

Verizon Threat report

Attacks are moving more to the inside of networks…



Anti-Malware , Fraud , Payments Fraud

Banco de Chile Loses $10 Million in SWIFT-Related Attack

First, Attackers Distracted Bank, Using Buhtrap Malware to Cause Mayhem

Jeremy Kirk (jeremy_kirk) • June 13, 2018 0 Comments

GET DAILY EMAIL UPDATES

Covering topics in risk management, compliance, fraud, and information security.

RESOURCES

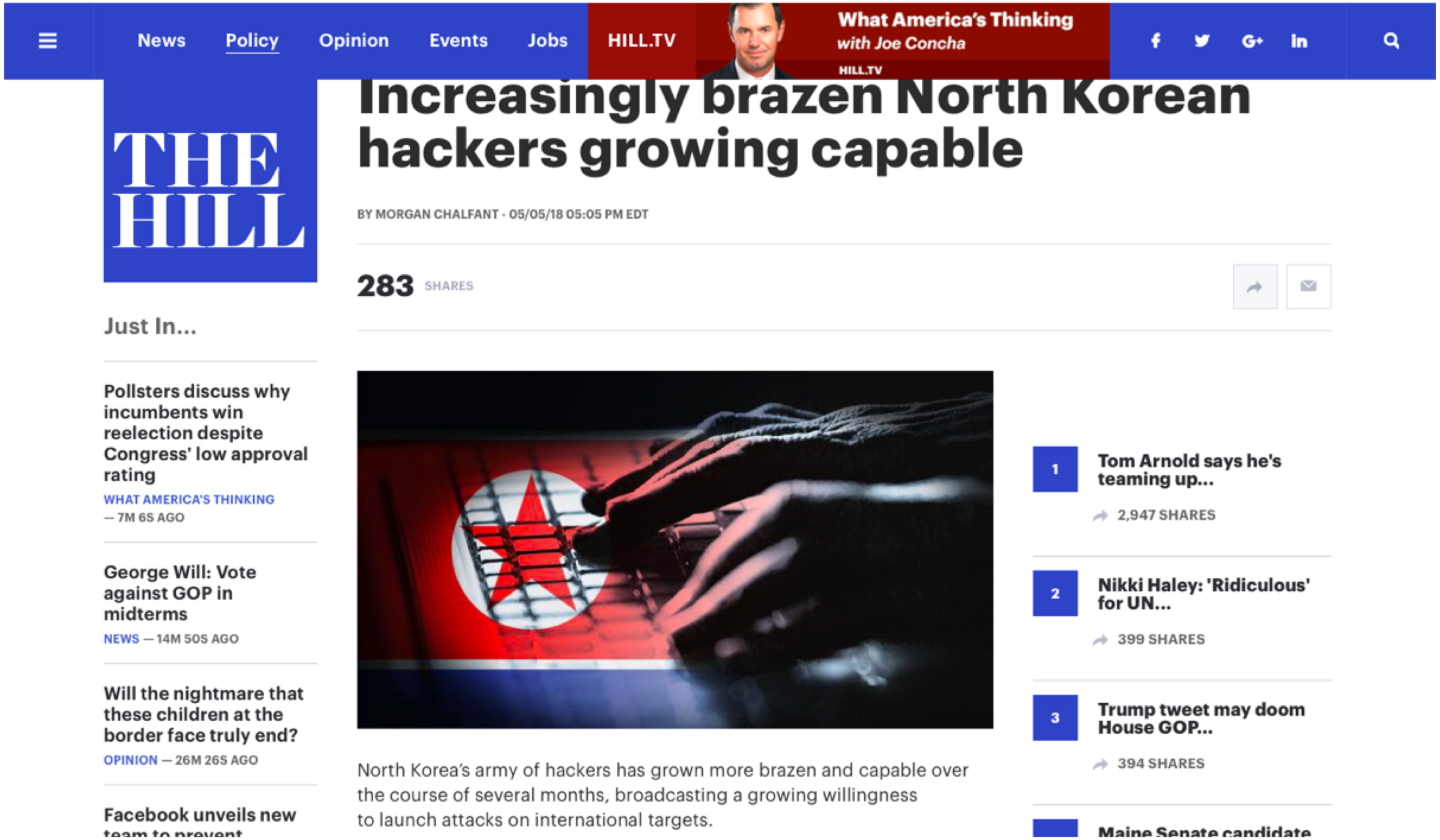
Chip and No Signature: What's Behind the Move?

0 Comments

Leveraging SaaS to Fill the Skills Gap

0 Comments

…and state actors are also getting stronger



Increasingly brazen North Korean hackers growing capable

BY MORGAN CHALFANT - 05/05/18 05:05 PM EDT

283 SHARES

North Korea's army of hackers has grown more brazen and capable over the course of several months, broadcasting a growing willingness to launch attacks on international targets.

Just In...

Pollsters discuss why incumbents win reelection despite Congress' low approval rating
WHAT AMERICA'S THINKING — 7M 6S AGO

George Will: Vote against GOP in midterms
NEWS — 14M 50S AGO

Will the nightmare that these children at the border face truly end?
OPINION — 26M 26S AGO

Facebook unveils new team to prevent

1 Tom Arnold says he's teaming up...
2,947 SHARES

2 Nikki Haley: 'Ridiculous' for UN...
399 SHARES

3 Trump tweet may doom House GOP...
394 SHARES

Maine Senate candidate

In physical world, prevention is better than cure..

SECURE
PROTECT
PREVENT
ESSEX.POLICE.UK/SECURE
PFCC
POLICE, FIRE AND CRIME COMMISSIONER FOR ESSEX
ESSEX POLICE
Protecting and serving Essex

BURGLAR ENTRY BREAKDOWN
22% Back Door
2% Second Floor
23% First Floor Window
34% Front Door
9% Garage
4% Unlocked Entrance
Almost 1 in 8 burglars enter a home through an unlocked door, window or other opening without force.
Homes without security systems are up to
3 TIMES
more likely to be targets. 60% of convicted burglars say they avoid homes with alarm systems.
PREVENTION TIP
Consider installing a security system and keep it active.
PREVENTION TIP
Take a few moments to make sure your windows and doors are closed and locked before leaving home.
BURGLARY PREVENTION TIPS
CHICAGO
24 HOUR 7 DAYS
LOCKSMITHS
312.878.2715

How to Keep the Burglar Out

What the burglar looks for:
- Signs that the home is unoccupied.
- Easy access, use the locks you have on all doors and windows.

House Numbers: House numbers should be visible from the street, numbers not script, and of a contrasting color.

Lights: Front, back and by garages are recommended. Motion detector lights are an alternative to lights being on all the time. Interior-timed lighting devices should be utilized when not home.

Windows: Glass is vulnerable to attack. Fortunately, burglars are reluctant to break windows because of the noise and windows are often visible from the street and other residences.

Garage: Never leave unlocked, especially if it has a connecting door to the house. Lock away tools and ladders so that a thi cannot use them. Attached garages prov visual cover for a burglar

ks: Use dead bolt locks having a hrow are recommended. Be sure se a high security strike plate with crews.

Basement Windows: Often overlooked basement windows should be secured prevent them from being forced open. Window locks should not be vulnerable glass is broken.

ubs: Should be kept low enough hey do not block possible points of y or to conceal a potential attacker.

Doors: Solid core wood doors with frames that cannot be spread apart with a pry bar are recommended.

Burglar Alarm Signs: Be sure to prominently display all signs and decals.

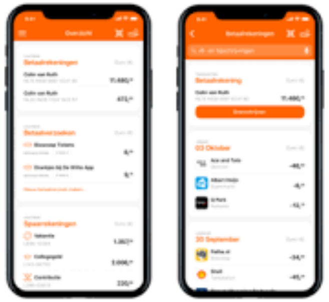
Spare Keys: Never leave a spare key in a hiding place outside your home. Burglars know all the hiding places. Leave one with a trusted neighbor.

…and real effect is that we chase away some burglars..

- Most visible security measures work only to chase a thief away and make them go to the neighbor’s house
- Most security measures only work in slightly delaying the time to break in and act for psychological effect on the buyer
- We have accepted the risk of a burglary once every x years and can live with it..
- Most major (non-financial) infrastructure in Europe is hardly protected

In the digital world it’s very different…

- Deterring burglars doesn’t work…
  - Easy for hackers to remain anonymous
  - chance of being caught is minimal
  - ’scaling’ is easy for criminals
  - Many governments don’t cooperate with finding criminals
- ’Hardening’ is possible to some extent, but ‘Firewalls’ don’t work anymore
- Education and awareness are a first step (GDPR publicity helped a bit)
- More and more devices and systems connected and become more vulnerable
  - More applications with user access
  - More and more mobile applications used
  - Customers expect fast response and no delays for security checks

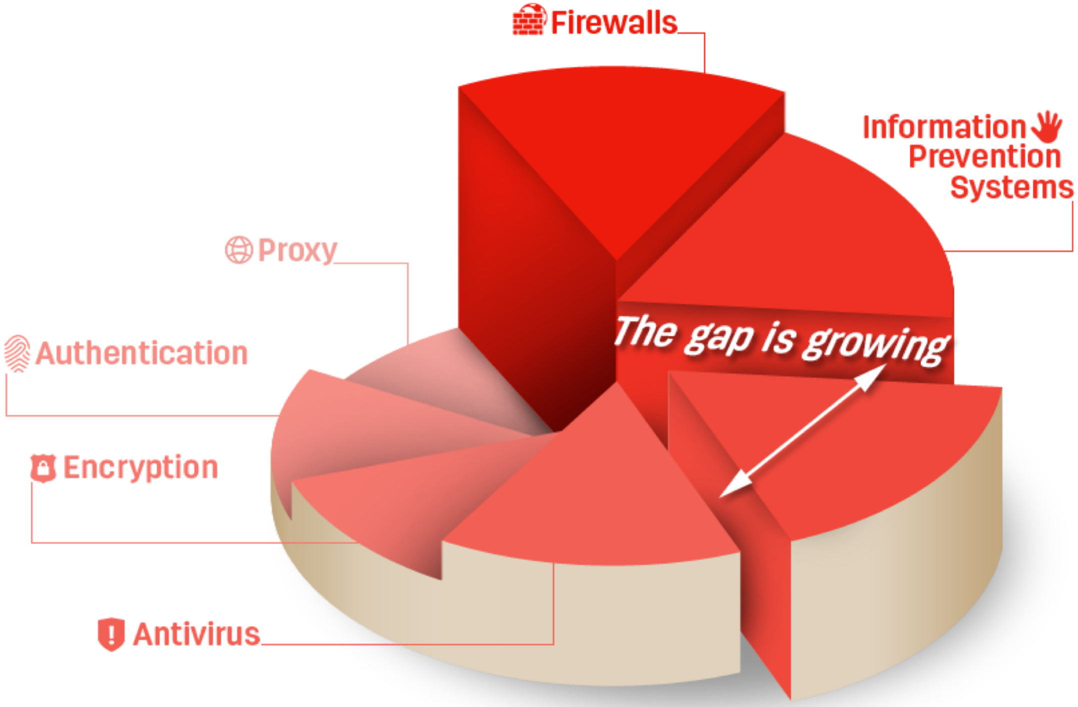


How do we harden against attacks?

Firewalls have trouble with encrypted traffic

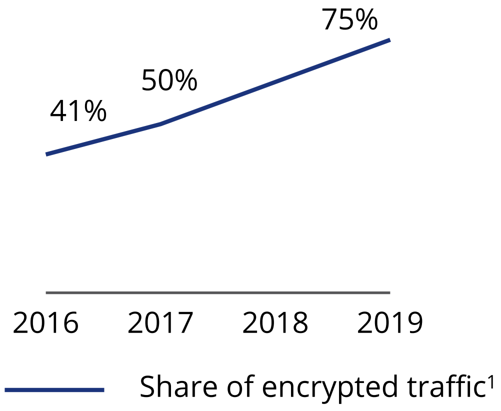
Authentication methods still underdeveloped

→ ***Need network detection and end-point detection***

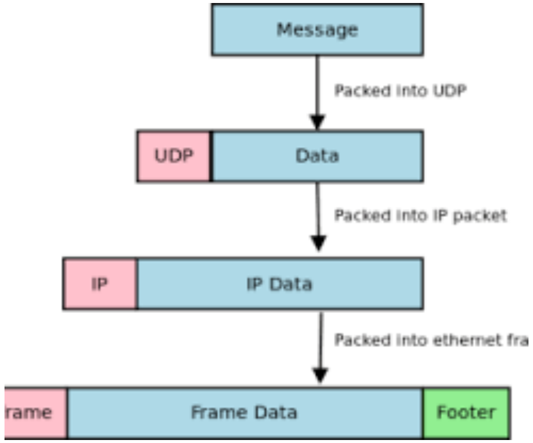


The nature of the Internet also makes prevention very difficult

- Internet Protocol Packets roam around the world freely
- Source cannot be confirmed with certainty: we don’t know WHO is behind any info..
- No central network management or supervision
- Encryption makes it actually more difficult to secure



Gartner 2018



Tanenbaum et al. Network management

New problem is not malware itself, but how long it goes undetected

Average presence

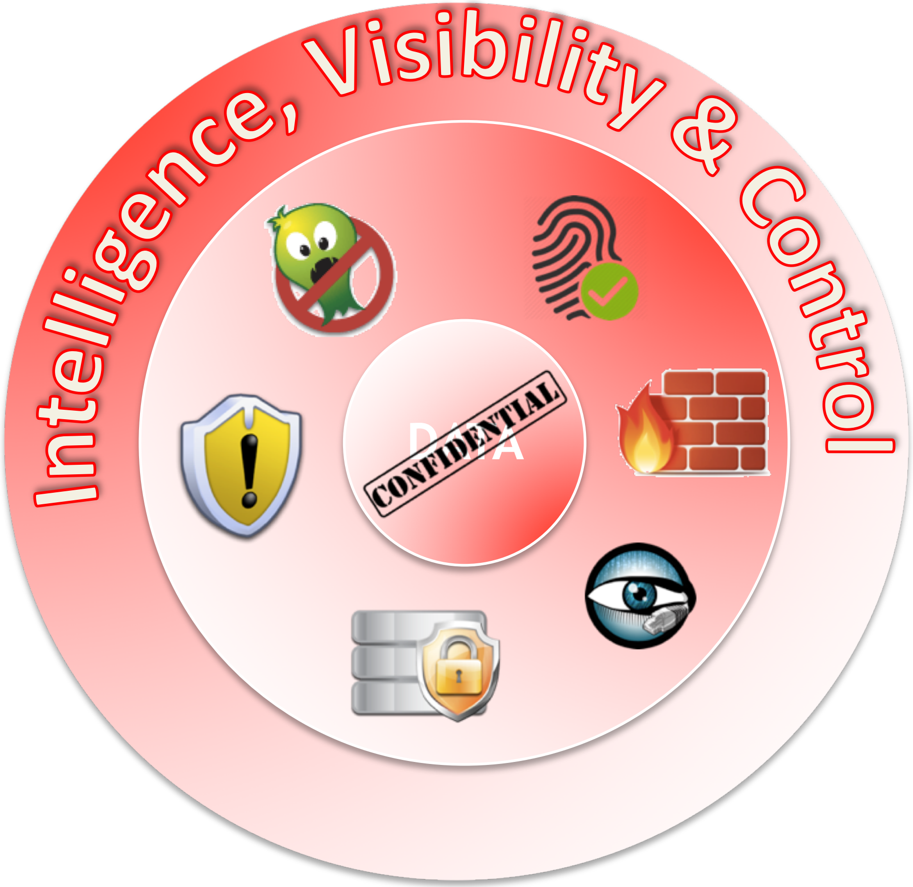
229 DAYS

New malware per day

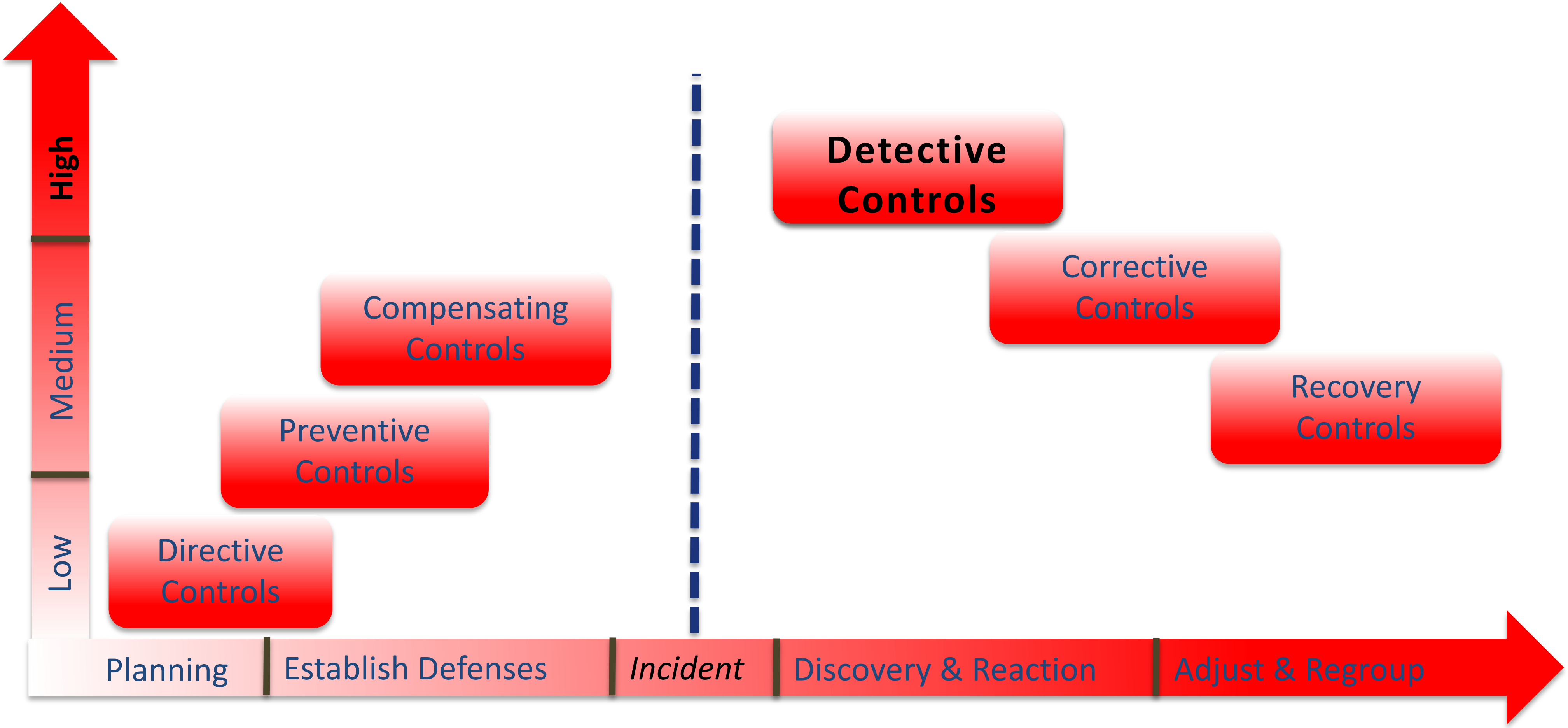
390.000+

Discovered externally

67%



… so rapid detection becomes of key importance..



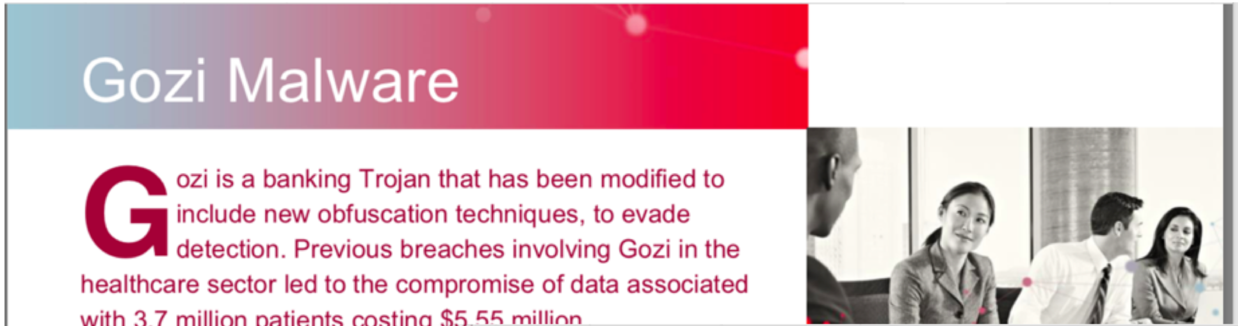
Who are the hackers? - examples of traditional ones

Anonymous
well known group of hackers with members around the world
Guy Fawkers masks
Against corporates, organisations and governments
Ddos attacks against Mastercard / Visa as they blocked Wikileaks web site.
Hacked IS supporters after the attacks in Paris and Orlando (2016)

Solo
Real name Gary McKinnon
Scottish nerd believing in UFO’s and life out of space
Cracked

Kevin Mitnick
Hacked intelligence services including FBI
includes social engineering

..smarter and more aggressive..



Gozi Malware

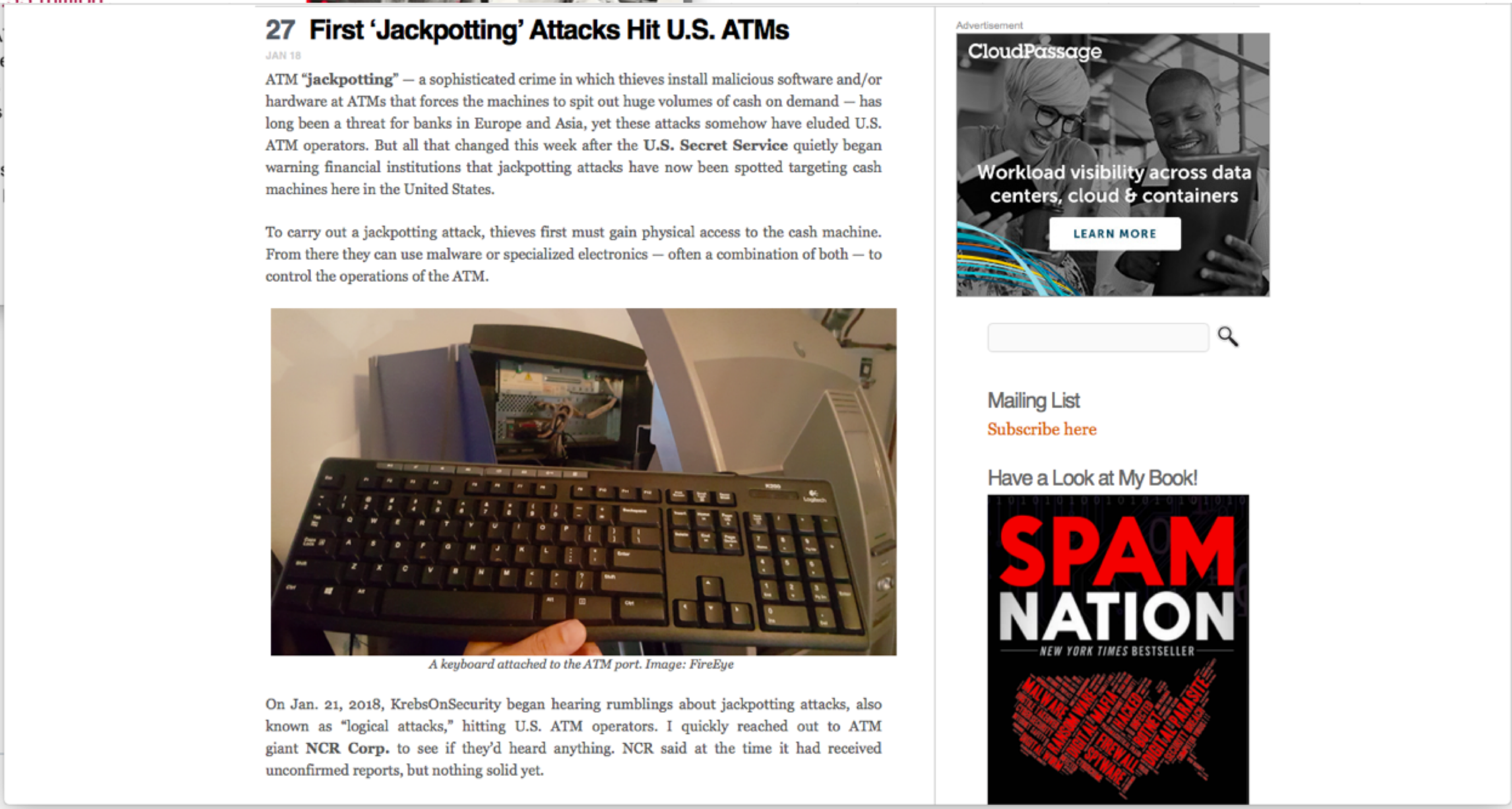
Gozi is a banking Trojan that has been modified to include new obfuscation techniques, to evade detection. Previous breaches involving Gozi in the healthcare sector led to the compromise of data associated with 3.7 million patients costing $5.55 million

CGI's Advanced Threat Investigation (A
various sources, and has been able to ide
that exfiltrates data from victim's machines
login credentials and further credentials
applications.

Gozi has further functionality including s
functions. The Gozi malware strand is also

ANALYSIS OF THE GOZI SAMPLE

Sample received



27 First 'Jackpotting' Attacks Hit U.S. ATMs

JAN 18

ATM "**jackpotting**" — a sophisticated crime in which thieves install malicious software and/or hardware at ATMs that forces the machines to spit out huge volumes of cash on demand — has long been a threat for banks in Europe and Asia, yet these attacks somehow have eluded U.S. ATM operators. But all that changed this week after the **U.S. Secret Service** quietly began warning financial institutions that jackpotting attacks have now been spotted targeting cash machines here in the United States.

To carry out a jackpotting attack, thieves first must gain physical access to the cash machine. From there they can use malware or specialized electronics — often a combination of both — to control the operations of the ATM.

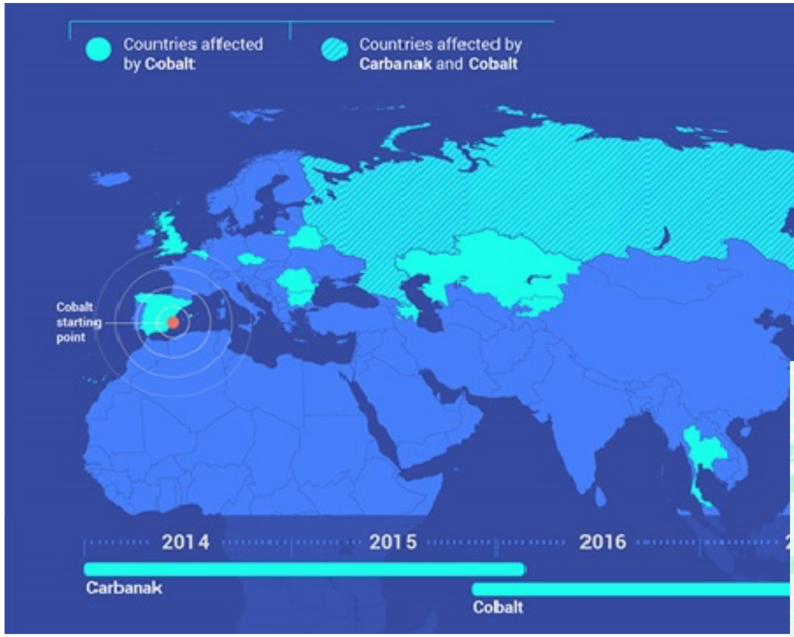
A keyboard attached to the ATM port. Image: FireEye

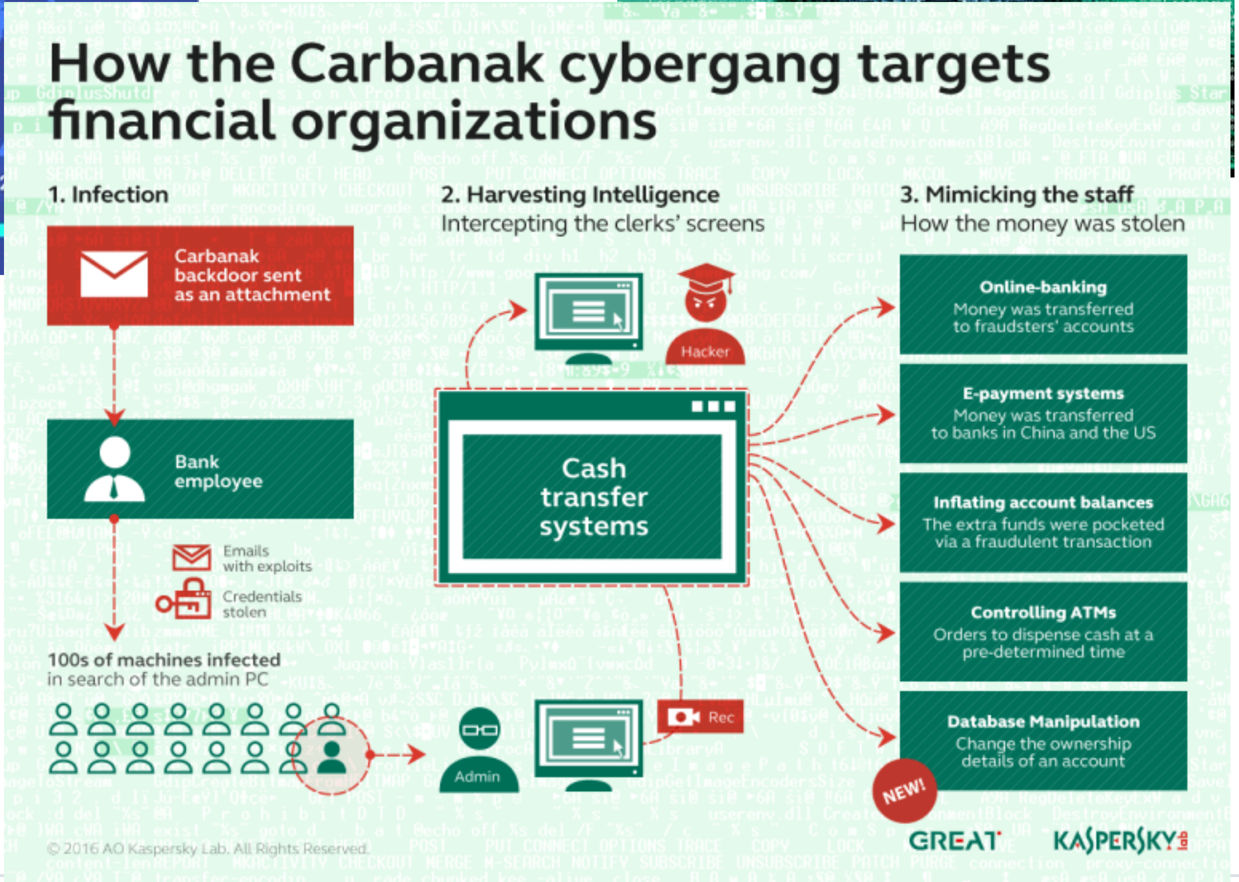
On Jan. 21, 2018, KrebsOnSecurity began hearing rumblings about jackpotting attacks, also known as "logical attacks," hitting U.S. ATM operators. I quickly reached out to ATM giant **NCR Corp.** to see if they'd heard anything. NCR said at the time it had received unconfirmed reports, but nothing solid yet.

Mailing List
Subscribe here

Have a Look at My Book!

Example: ‘man in the middle attack’


Countries affected by Cobalt
Countries affected by Carbanak and Cobalt
Cobalt starting point
2014
2015
2016
Carbanak
Cobalt



How the Carbanak cybergang targets financial organizations

1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected in search of the admin PC

Admin

2. Harvesting Intelligence

Intercepting the clerks' screens

Hacker

Cash transfer systems

Rec

3. Mimicking the staff

How the money was stolen

Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

Inflating account balances
The extra funds were pocketed via a fraudulent transaction

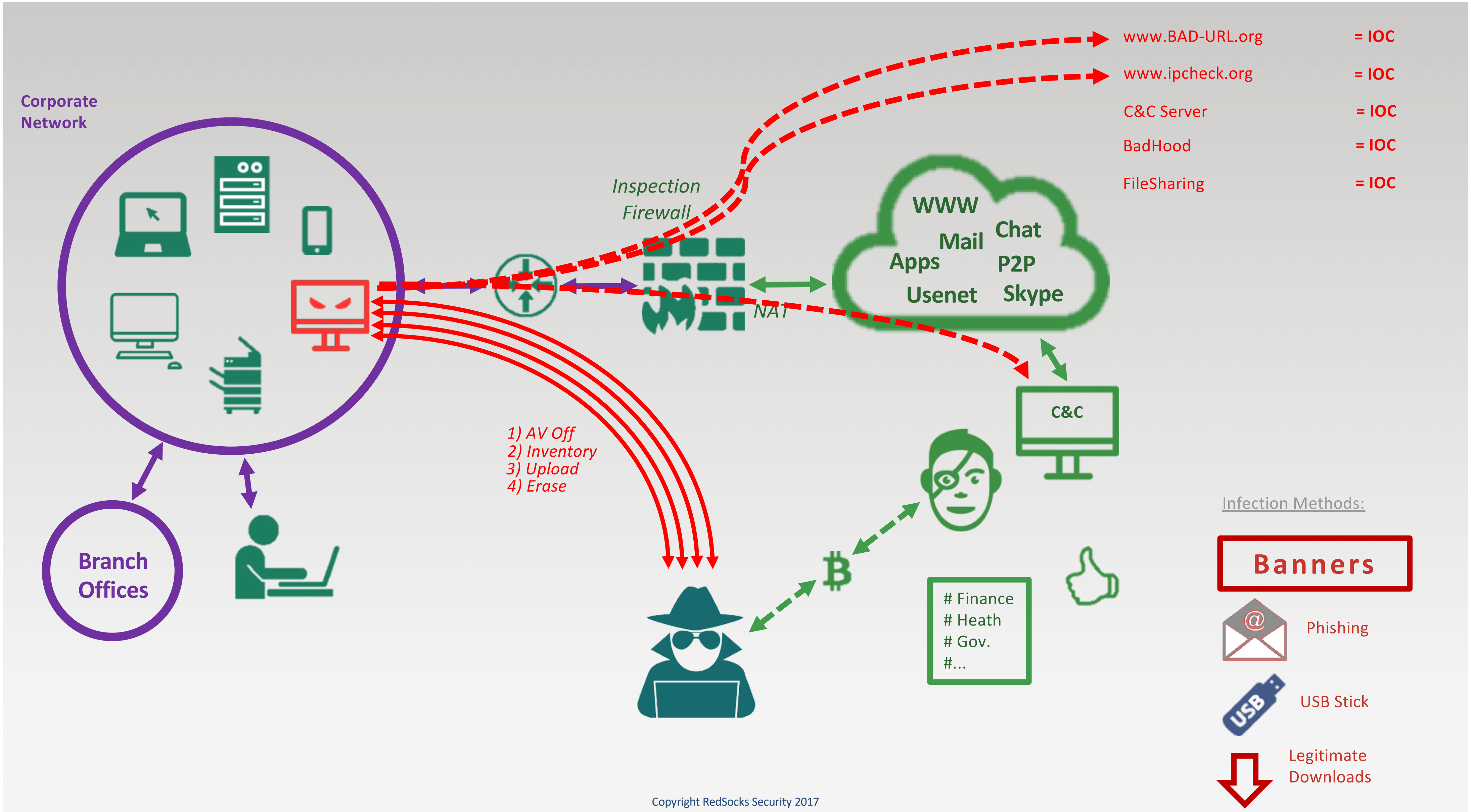
Controlling ATMs
Orders to dispense cash at a pre-determined time

Database Manipulation
Change the ownership details of an account

NEW!

GREAT KASPERSKY lab

Malware Infection; how does it work?



Corporate Network

Inspection Firewall

NAT

WWW

Mail

Chat

Apps

P2P

Usenet

Skype

www.BAD-URL.org	= IOC
www.ipcheck.org	= IOC
C&C Server	= IOC
BadHood	= IOC
FileSharing	= IOC

C&C

1) AV Off
2) Inventory
3) Upload
4) Erase

Branch Offices

# Finance
# Heath
# Gov.
#...

Infection Methods:

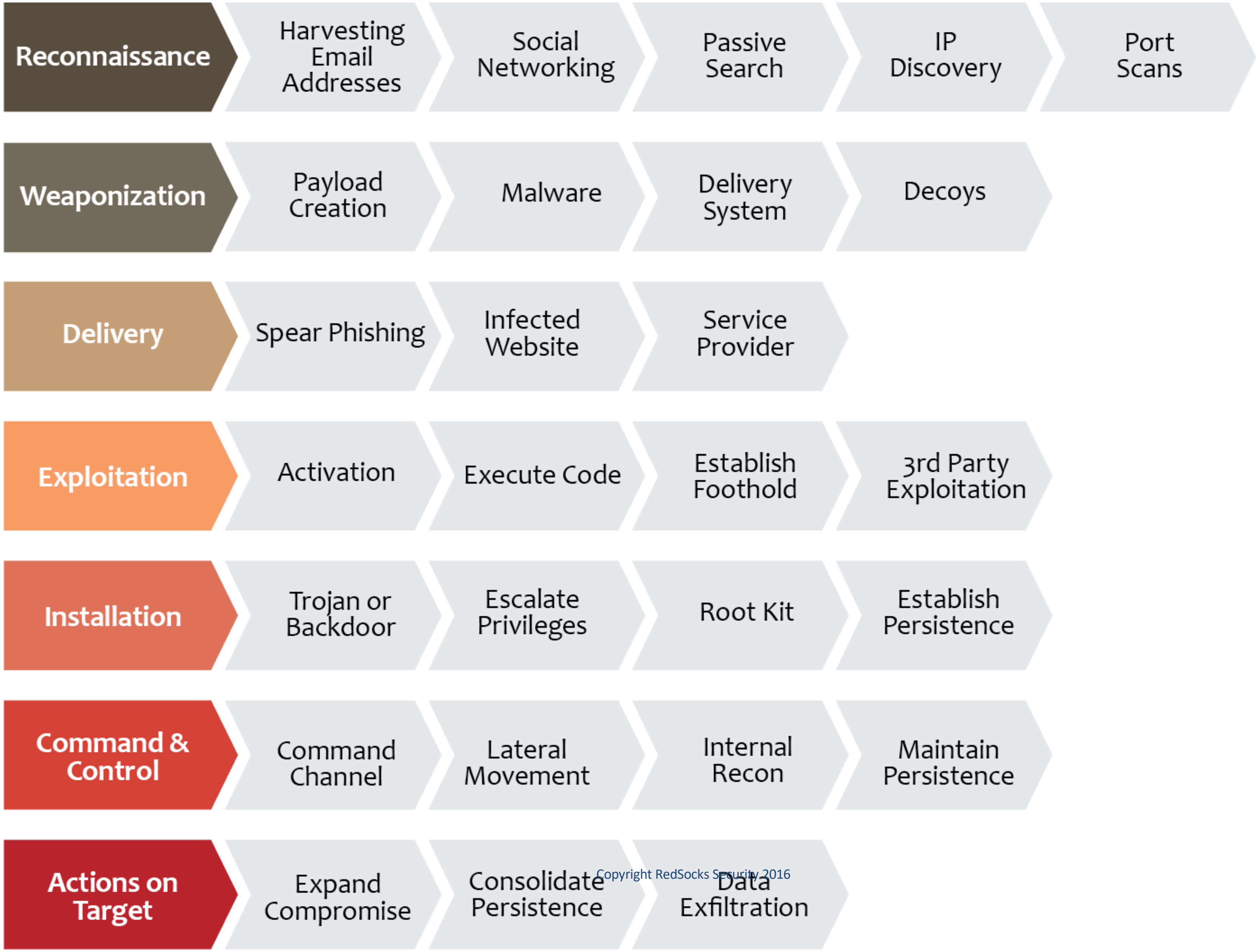
Banners

Phishing

USB Stick

Legitimate Downloads

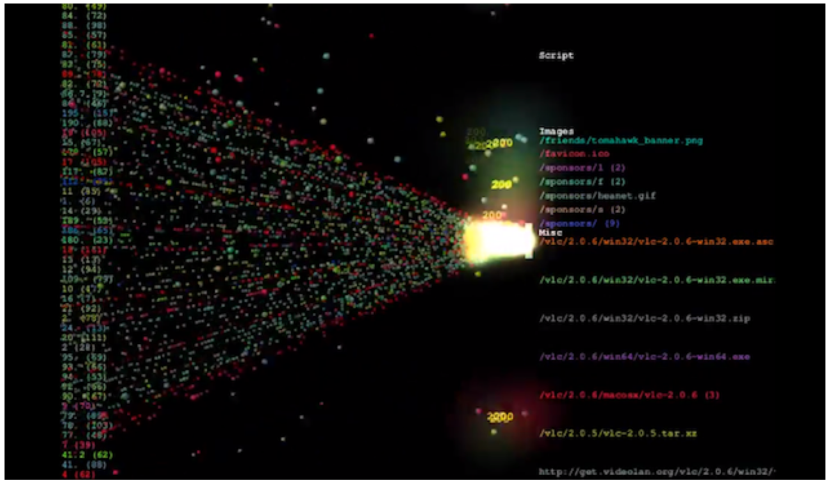
Attacks are built up over several months… called the ‘kill chain’



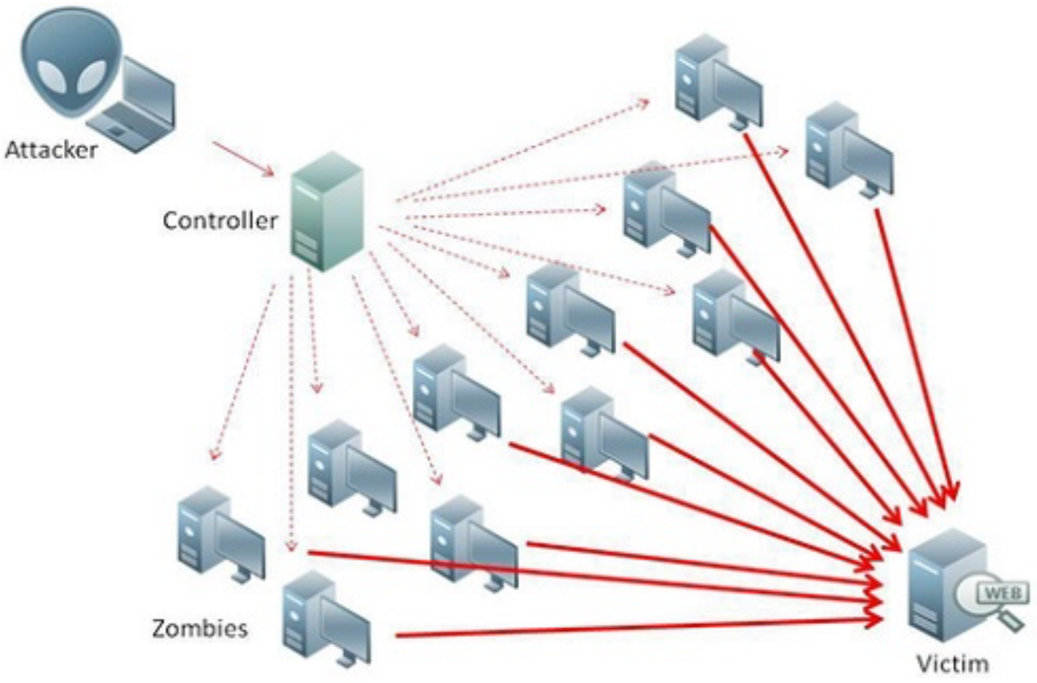
Reconnaissance	Harvesting Email Addresses	Social Networking	Passive Search	IP Discovery	Port Scans
Weaponization	Payload Creation	Malware	Delivery System	Decoys	
Delivery	Spear Phishing	Infected Website	Service Provider		
Exploitation	Activation	Execute Code	Establish Foothold	3rd Party Exploitation	
Installation	Trojan or Backdoor	Escalate Privileges	Root Kit	Establish Persistence	
Command & Control	Command Channel	Lateral Movement	Internal Recon	Maintain Persistence	
Actions on Target	Expand Compromise	Consolidate Persistence	Data Exfiltration		

In particular in the last few years it has become easier to DDos

- > 1 Bn IoT devices connected
- > 1 Million IoT devices infected and in control as ‘botnets’
- Attacks can be made different each time, such that they can’t be uncovered quickly nor prevented
- Many cheap services available: *Stressers*
- Anonymizing tools available (*spoofing)*



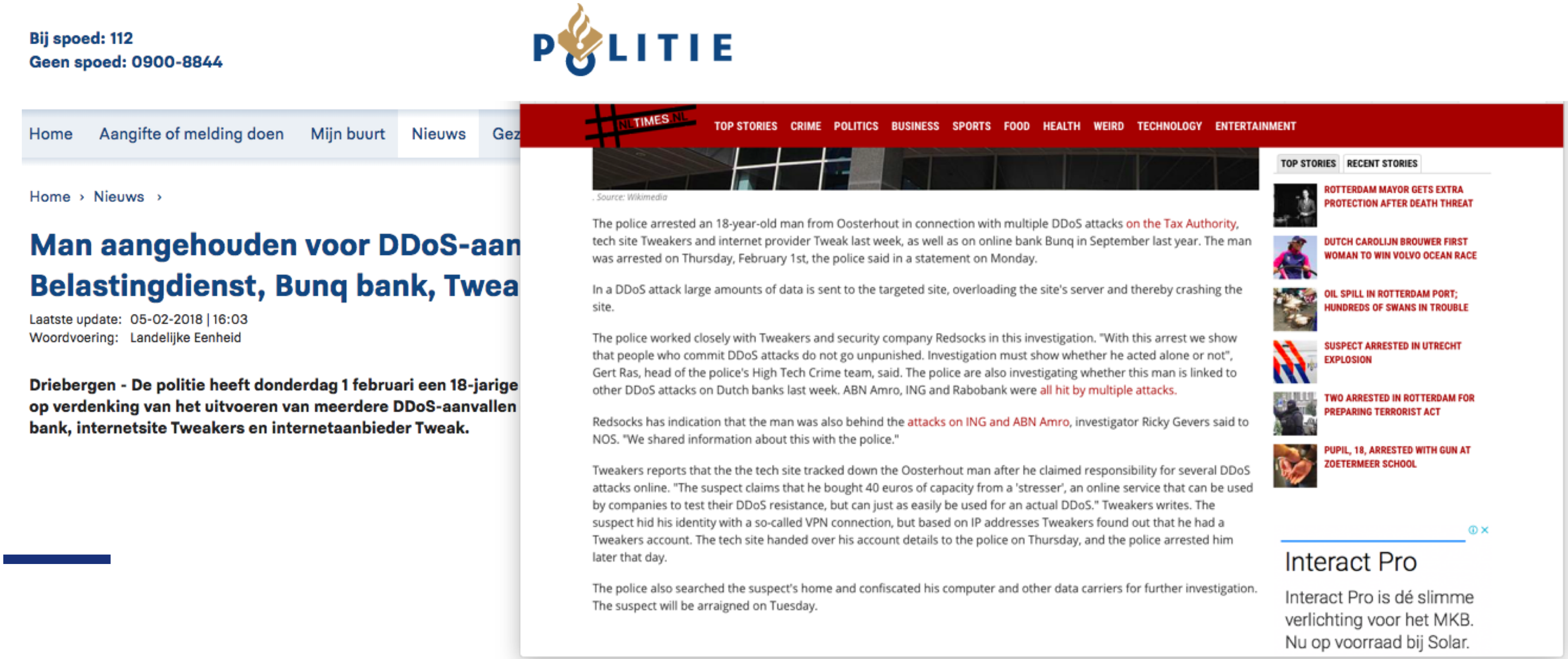
```
Script

Images
/friends/tomahawk_banner.png
/favicon.ico
/sponsors/l (2)
/sponsors/f (2)
/sponsors/heanet.gif
/sponsors/s (2)
/sponsors/ (9)
Misc
/vlc/2.0.6/win32/vlc-2.0.6-win32.exe.asc

/vlc/2.0.6/win32/vlc-2.0.6-win32.exe.mir

/vlc/2.0.6/win32/vlc-2.0.6-win32.zip

/vlc/2.0.6/win64/vlc-2.0.6-win64.exe

/vlc/2.0.6/macosx/vlc-2.0.6 (3)

/vlc/2.0.5/vlc-2.0.5.tar.xz

http://get.videolan.org/vlc/2.0.6/win32/
```



Police uses tips and industry knowledge

Just like in physical world: small mistakes happen

Actual criminal: Jelle Schneider (18 years old; at parents’ home in Netherlands)



Home › Nieuws ›

Man aangehouden voor DDoS-aan Belastingdienst, Bunq bank, Twea

Laatste update: 05-02-2018 | 16:03
Woordvoering: Landelijke Eenheid

Driebergen - De politie heeft donderdag 1 februari een 18-jarige op verdenking van het uitvoeren van meerdere DDoS-aanvallen bank, internetsite Tweakers en internetaanbieder Tweak.

. Source: Wikimedia

The police arrested an 18-year-old man from Oosterhout in connection with multiple DDoS attacks on the Tax Authority, tech site Tweakers and internet provider Tweak last week, as well as on online bank Bunq in September last year. The man was arrested on Thursday, February 1st, the police said in a statement on Monday.

In a DDoS attack large amounts of data is sent to the targeted site, overloading the site's server and thereby crashing the site.

The police worked closely with Tweakers and security company Redsocks in this investigation. "With this arrest we show that people who commit DDoS attacks do not go unpunished. Investigation must show whether he acted alone or not", Gert Ras, head of the police's High Tech Crime team, said. The police are also investigating whether this man is linked to other DDoS attacks on Dutch banks last week. ABN Amro, ING and Rabobank were all hit by multiple attacks.

Redsocks has indication that the man was also behind the attacks on ING and ABN Amro, investigator Ricky Gevers said to NOS. "We shared information about this with the police."

Tweakers reports that the the tech site tracked down the Oosterhout man after he claimed responsibility for several DDoS attacks online. "The suspect claims that he bought 40 euros of capacity from a 'stresser', an online service that can be used by companies to test their DDoS resistance, but can just as easily be used for an actual DDoS." Tweakers writes. The suspect hid his identity with a so-called VPN connection, but based on IP addresses Tweakers found out that he had a Tweakers account. The tech site handed over his account details to the police on Thursday, and the police arrested him later that day.

The police also searched the suspect's home and confiscated his computer and other data carriers for further investigation. The suspect will be arraigned on Tuesday.

ROTTERDAM MAYOR GETS EXTRA PROTECTION AFTER DEATH THREAT

DUTCH CAROLIJN BROUWER FIRST WOMAN TO WIN VOLVO OCEAN RACE

OIL SPILL IN ROTTERDAM PORT; HUNDREDS OF SWANS IN TROUBLE

SUSPECT ARRESTED IN UTRECHT EXPLOSION

TWO ARRESTED IN ROTTERDAM FOR PREPARING TERRORIST ACT

PUPIL, 18, ARRESTED WITH GUN AT ZOETERMEER SCHOOL

So how to protect?

- ***Need network detection and end-point detection***

- ***Ensure adequate response***