THE ATTACK KILLCHAIN

MALWARE ANALYSIS AND INCIDENT FORENSICS

M.Sc. in Cyber Security

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

WHAT ARE WE TALKING ABOUT?

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel | More | Search

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts | Health | World News TV | More

Technology

Yahoo 'state' hackers stole data from 500 million users

23 September 2016 | Technology

Share

Yahoo says "state-sponsored" hackers stole data on about 500 million users in what could be the largest publicly disclosed cyber-breach in history.

Top Stories

US accuses Russia of Aleppo 'barbarism'

5 hours ago

Swiss approve new surveillance law

6 hours ago

Miami baseball star dies in boat crash

3 hours ago

Features & Analysis

Still missing

The search for Mexican students two

WHAT ARE WE TALKING ABOUT?

“

We are aware of a claim. We are committed to protecting the security of our users' information and we take any such claim very seriously. Our security team is working to determine the facts. Yahoo works hard to keep our users safe, and we always encourage our users to create strong passwords, or give up passwords altogether by using Yahoo Account Key, and use different passwords for different platforms.

The “Paranoids,” the internal name for Yahoo’s security team, often clashed with other parts of the business over security costs. And their requests were often overridden because of concerns that the inconvenience of added protection would make people stop using the company’s products.

But Yahoo’s choices had consequences, resulting in a series of embarrassing security failures over the last four years. Last week, the company disclosed that hackers backed by what it believed was an unnamed foreign government stole the credentials of 500 million users in a breach that went undetected for two years. It was the biggest known intrusion into one company’s network, and the episode is now under investigation by both Yahoo and the Federal Bureau of Investigation.

Yahoo Hacked by Criminals, Not State Sponsor, Security Firm Says

by Brian Womack
brianwomack

September 29, 2016 – 12:07 AM CEST

WHAT ARE WE TALKING ABOUT?

HACKREAD
SECURITY IS A MYTH

Search ...

HACKING NEWS | TECH | CYBER CRIME | HOW TO | CYBER EVENTS | SECURITY | SURVEILLANCE | GAMING | SCIENCE

YOU ARE AT: Home » Cyber Crime » Brian Krebs site hit with 665 Gbps DDoS attack; Largest Internet has ever seen

DON'T MISS STORIES *FOLLOW HACKREAD* Like Follow Subscribe Follow

briankrebs
@briankrebs

Follow

Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL

3:02 AM - 21 Sep 2016

Brian Krebs site hit with 665 Gbps DDoS attack; Largest Internet has ever seen

By Waqas on September 21, 2016 *Email* *@hackread* CYBER ATTACKS CYBER CRIME

SUBSCRIBE TO OU

Enter your email...

POPULAR POSTS

DARK NET R
ATTACKING I
September

ARMENIAN H
MILITARY DA
September

HACKER GE
MILITARY DA
September

WHAT ARE WE TALKING ABOUT?

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by **Anna-senpai**.)

Anna-senpai

L33t Member

L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so i
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

WHAT ARE WE TALKING ABOUT?

Mirai today:

US authorities take down a Mirai-variant botnet tied to DDoS threat

An FBI-led operation to disrupt a China-linked botnet comes months after a similar operation in January linked to Volt Typhoon.

Published Sept. 19, 2024

- The FBI disrupted a massive state-linked botnet that compromised more than 260,000 devices worldwide in order to hack critical infrastructure providers in the U.S. and other countries, FBI Director Christopher Wray announced in a speech Wednesday during the Aspen Cyber Summit.
- The botnet was linked to a threat group known as Flax Typhoon, which has targeted critical manufacturing, IT, telecom, government and other organizations in Taiwan, the U.S. and other countries since 2021.
- The botnet compromised thousands of small office/home office routers, digital video cameras, internet-protocol cameras and network-attached storage devices. Almost half of the compromised devices were

Beware the Unpatchable: Corona Mirai Botnet Spreads via Zero-Day

Kyle Lefton, Larry Cashdollar, and Aline Eliovich

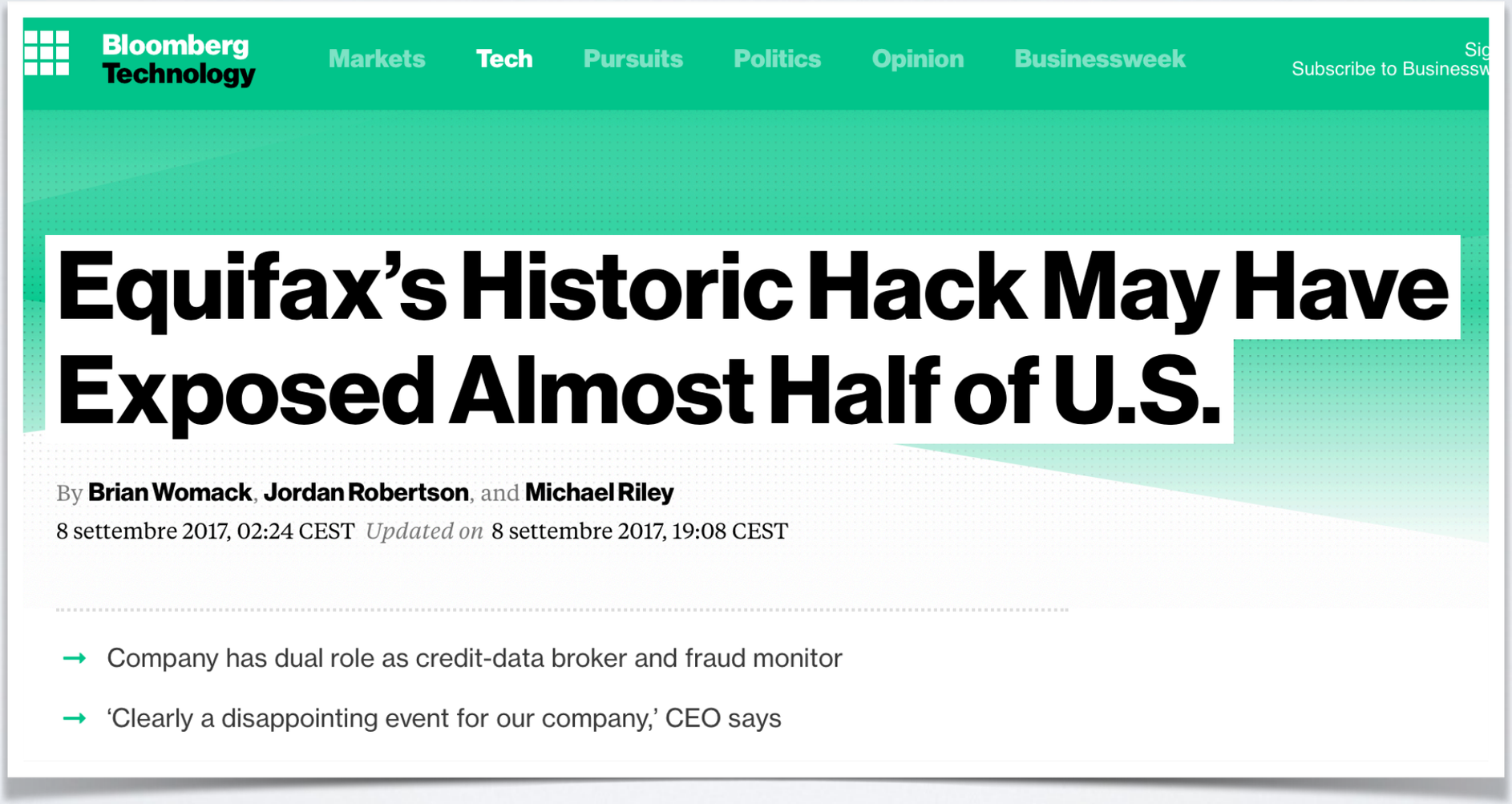
August 28, 2024

Executive summary

- The Akamai Security Intelligence and Response Team (SIRT) has observed a botnet campaign that is abusing several previously exploited vulnerabilities, as well as a zero-day vulnerability discovered by the SIRT.
- CVE-2024-7029 (discovered by Aline Eliovich) is a command injection vulnerability found in the brightness function of AVTECH closed-circuit television (CCTV) cameras that allows for remote code execution (RCE).
- Once injected, the botnet spreads a Mirai variant with string names that reference the COVID-19 virus that has been seen since at least 2020.

WHAT ARE WE TALKING ABOUT?

- September 2017 - The Equifax data breach exposes extremely sensitive data from 143 million consumers
  - hackers exploited a known vulnerability in an unpatched server



Bloomberg Technology

Markets Tech Pursuits Politics Opinion Businessweek

Sig
Subscribe to Businessw

Equifax's Historic Hack May Have Exposed Almost Half of U.S.

By **Brian Womack**, **Jordan Robertson**, and **Michael Riley**

8 settembre 2017, 02:24 CEST *Updated on* 8 settembre 2017, 19:08 CEST

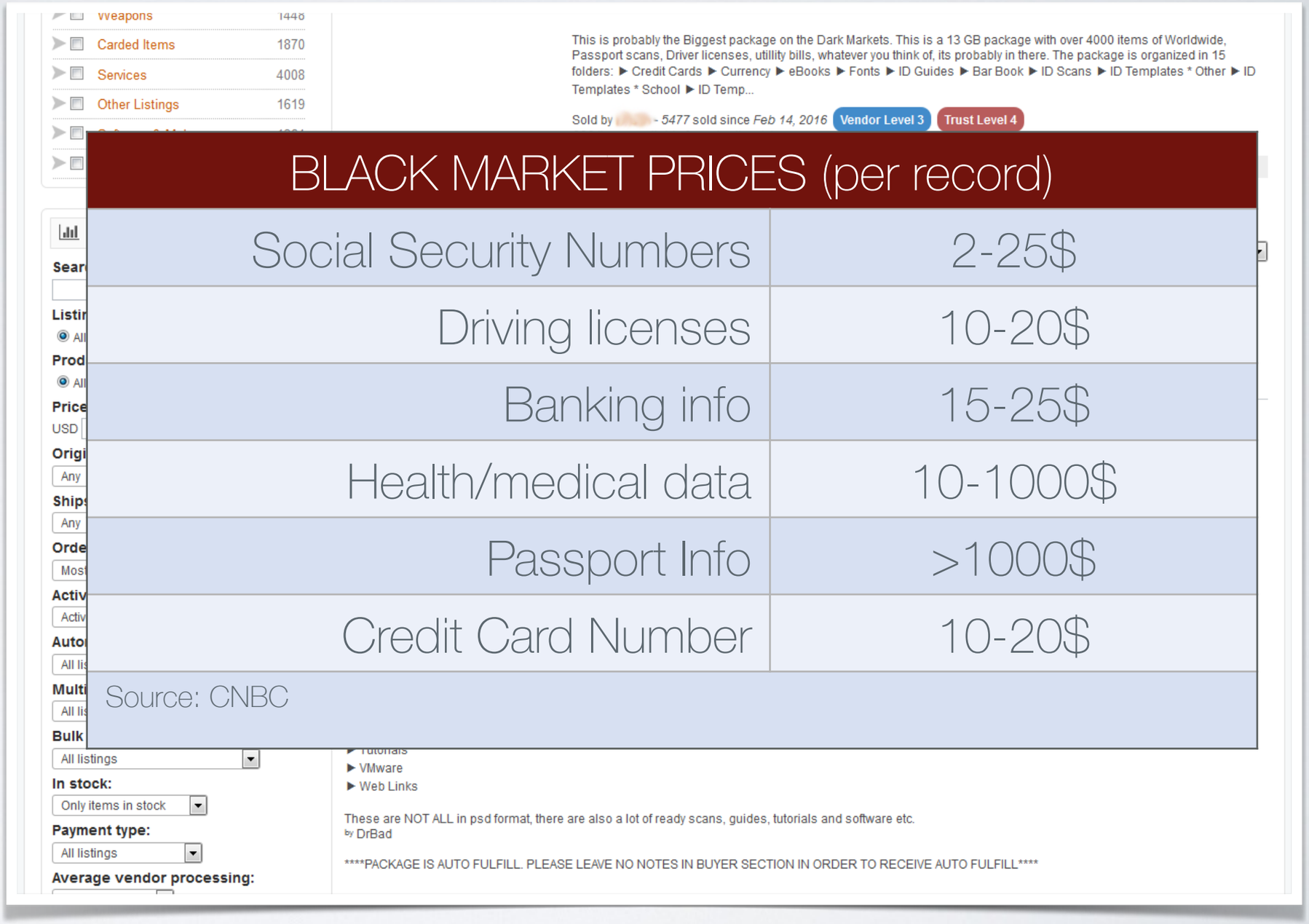
→ Company has dual role as credit-data broker and fraud monitor

→ 'Clearly a disappointing event for our company,' CEO says

WHAT ARE WE TALKING ABOUT?

The *data breach* market is flourishing

- Black markets provide advanced tools for data search.
- Prices are extremely variable depending on the specific product.



BLACK MARKET PRICES (per record)	
Social Security Numbers	2-25$
Driving licenses	10-20$
Banking info	15-25$
Health/medical data	10-1000$
Passport Info	>1000$
Credit Card Number	10-20$

Source: CNBC

WHAT ARE WE TALKING ABOUT?

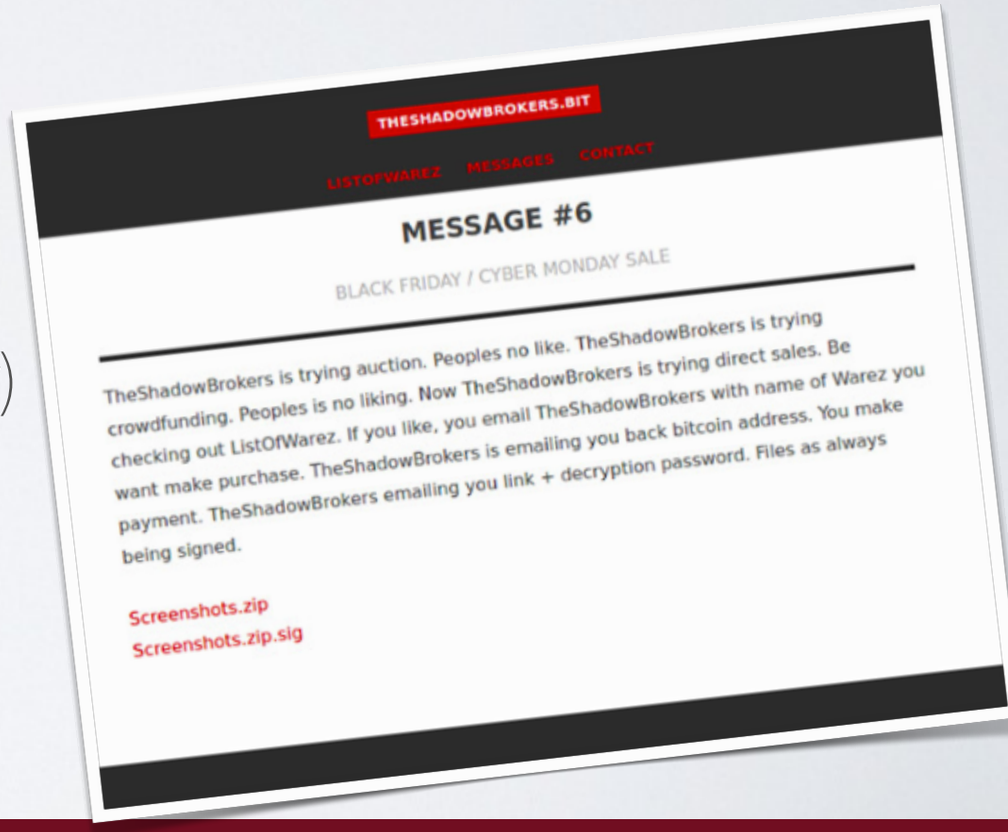
August 2016:

- An hacker group named “Shadow Brokers” setups an auction for a SW pkg.
- They claim the pag contains several advanced tools for system penetration
- Source: The Equation Group (NSA)

The auction goes on for a few weeks with no success

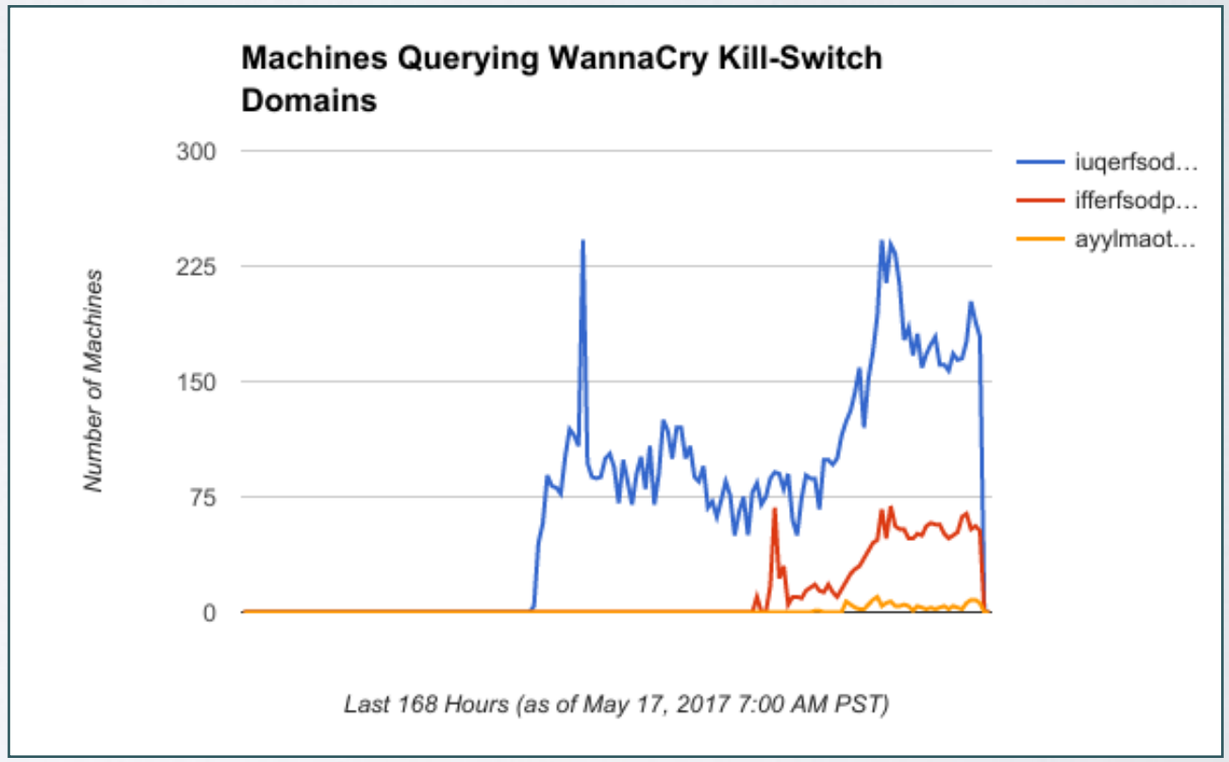
- Evasive action?
- The SW is released publicly (14/4/17)
- Contains executable code for several attacks.
  A few of these were previously unknown (0-day)

The SW structure makes the claim about the source credible.



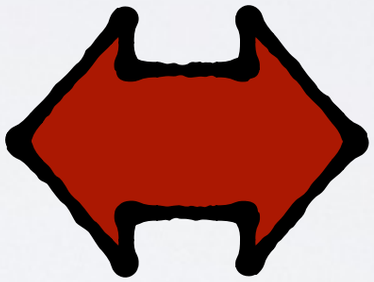
WHAT ARE WE TALKING ABOUT?

- May 2017 - Wannacry spreads infecting thousands of PCs
  - uses EternalBlue, an exploit leaked from NSA
  - spreads widely, but shows little care in its design



WHAT ARE WE TALKING ABOUT?

- Extremely advanced technologies are within easy reach of any criminal with enough budget

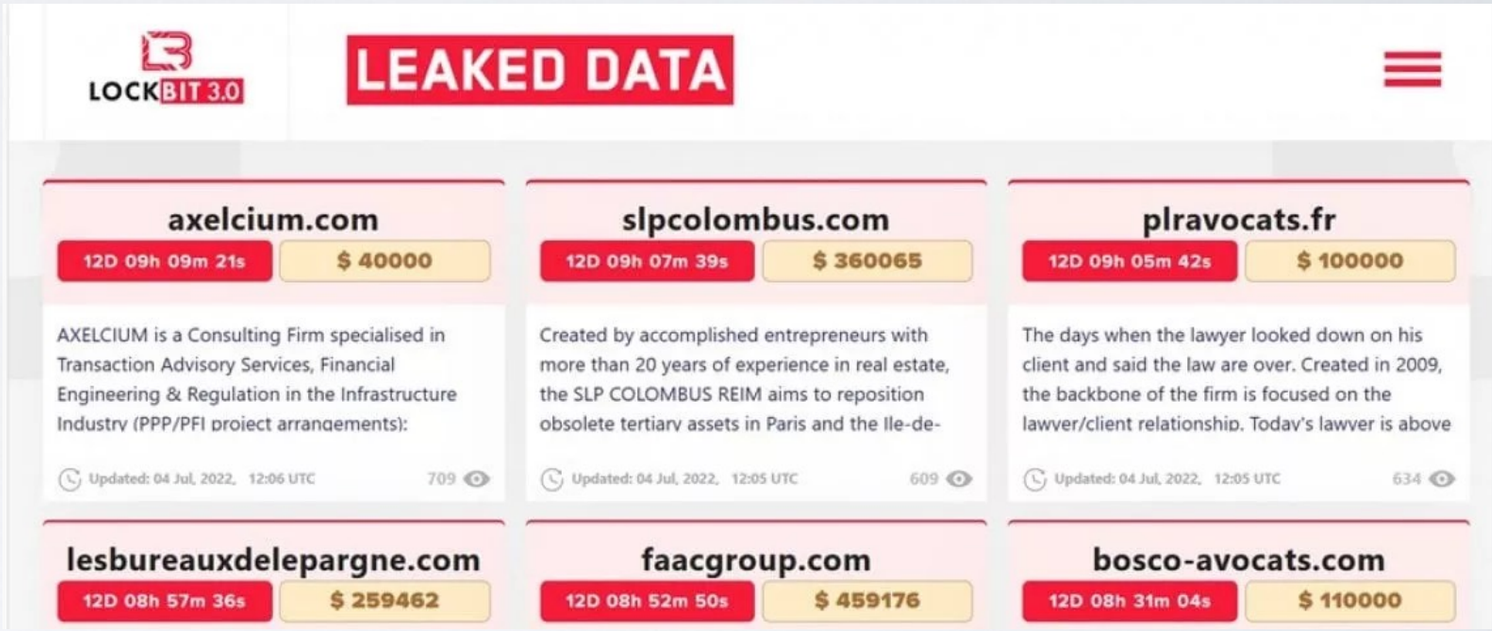


WHAT ARE WE TALKING ABOUT?

- August 2017 - FDA recalls pacemaker devices that were found vulnerable to hacking

WHAT ARE WE TALKING ABOUT?

- Lockbit
  - Ransomware-as-a-service (RaaS) since 2019
  - Third iteration of the software platform
  - Triple extortion tactic
    - through encryption
    - threat to publish sensitive data
    - create pressure using tactics like DDoS or chasing end-users
- Business oriented
  - Bug bounty program
  - Customer care
  - Trust-based model



WHAT ARE WE TALKING ABOUT?

2020: with Solarwinds/SUNBURST supply chain security becomes a crucial issue

- The Orion software, produced by Solarwinds, gets compromised.
- The SUNBURST backdoor is automatically injected in tens of thousands of systems.
  - SUNBURST allows remote access and lateral movements
    - Used to load the TEADROP memory dropper and then install a COBALTSTRIKE beacon module.

2021: CVE-2021-44228 vulnerability in log4j

- The usage of open software is not a security guarantee.

2024: xz Utils attack

- Strongly obfuscated backdoor introduced by a malicious developer infiltrated in the open source community.

WHAT ARE WE TALKING ABOUT?

The topic of this course revolves around CYBER SECURITY

> "*preservation of confidentiality, integrity and availability of information in the Cyberspace*"
> (ISO-27000)

Cyberspace is "*the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*" (NIST)

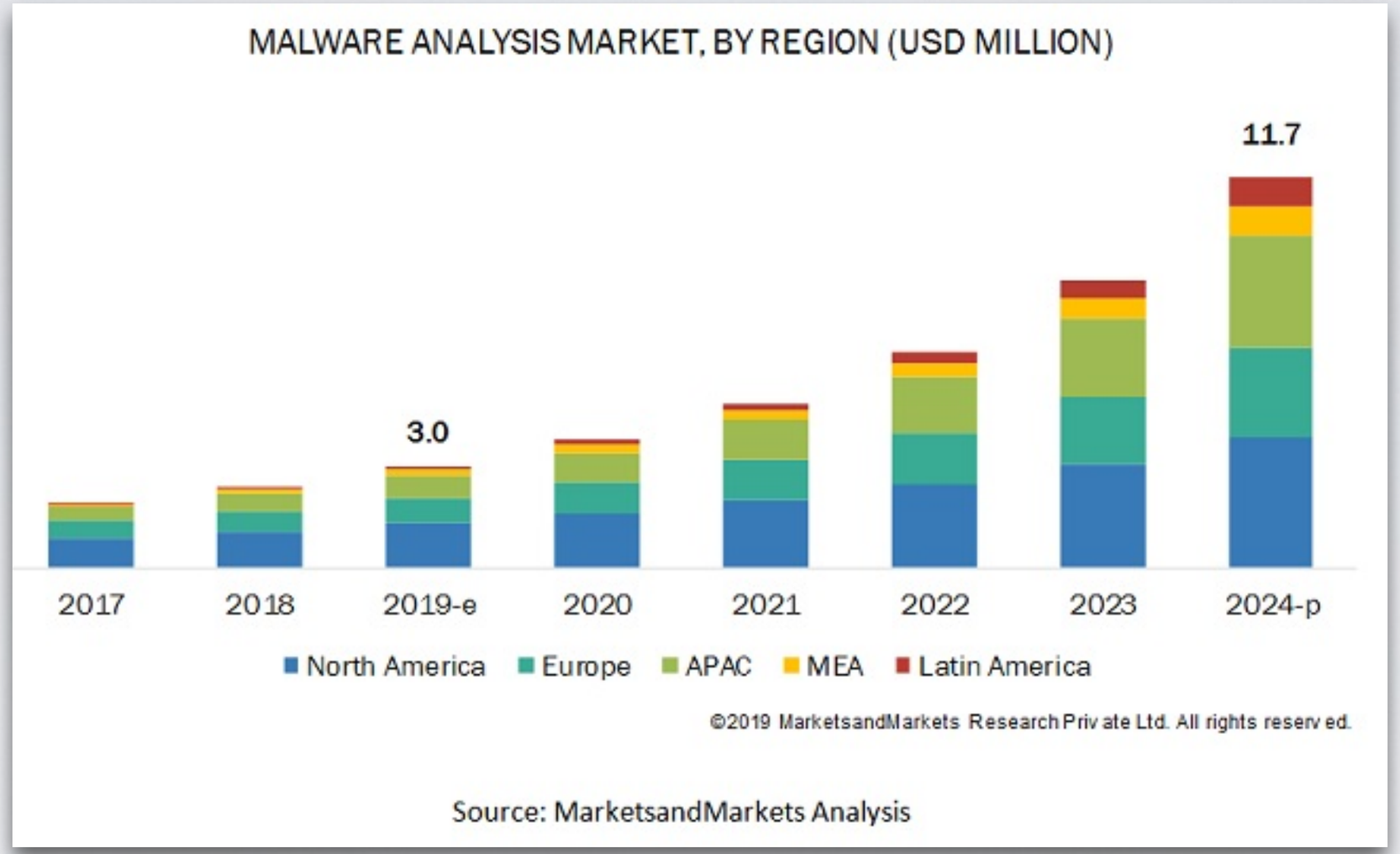
IS THIS RELEVANT?

February 2016 - Obama unveils national cybersecurity action plan

September 2017 - Junker declares Cybersecurity as the second most important challenge that EU will face in the forthcoming years

THE ROLE OF MALWARE

RELEVANT FOR THE JOB MARKET?



https://www.marketsandmarkets.com/Market-Reports/malware-analysis-market-10876513.html

THE 5Ws OF A CYBER ATTACK

WHO?

Targets

- Single users
- Industries
  - Financial
  - Health
  - Energy
  - IT
  - Manufacture
- Public agencies
- MIL & Defense

THE 5Ws OF A CYBER ATTACK

WHO?

Threats

- Hackers
- Activists
- Undercover operations
- Industrial espionage
- Cyberterrorists
- Cyberwarfare

WAIT…CYBERWHAT?

Securing Your Future with Two-Factor Authentication

Do you really know who's accessing your most sensitive networked information assets? Unfortunately, security built on static, reusable passwords has proven easy for hackers to beat.

RSA SecurID® two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator)—providing a much more reliable level of user authentication than reusable passwords.

- The only solution that automatically changes your password every 60 seconds
- 20-year history of outstanding performance and innovation

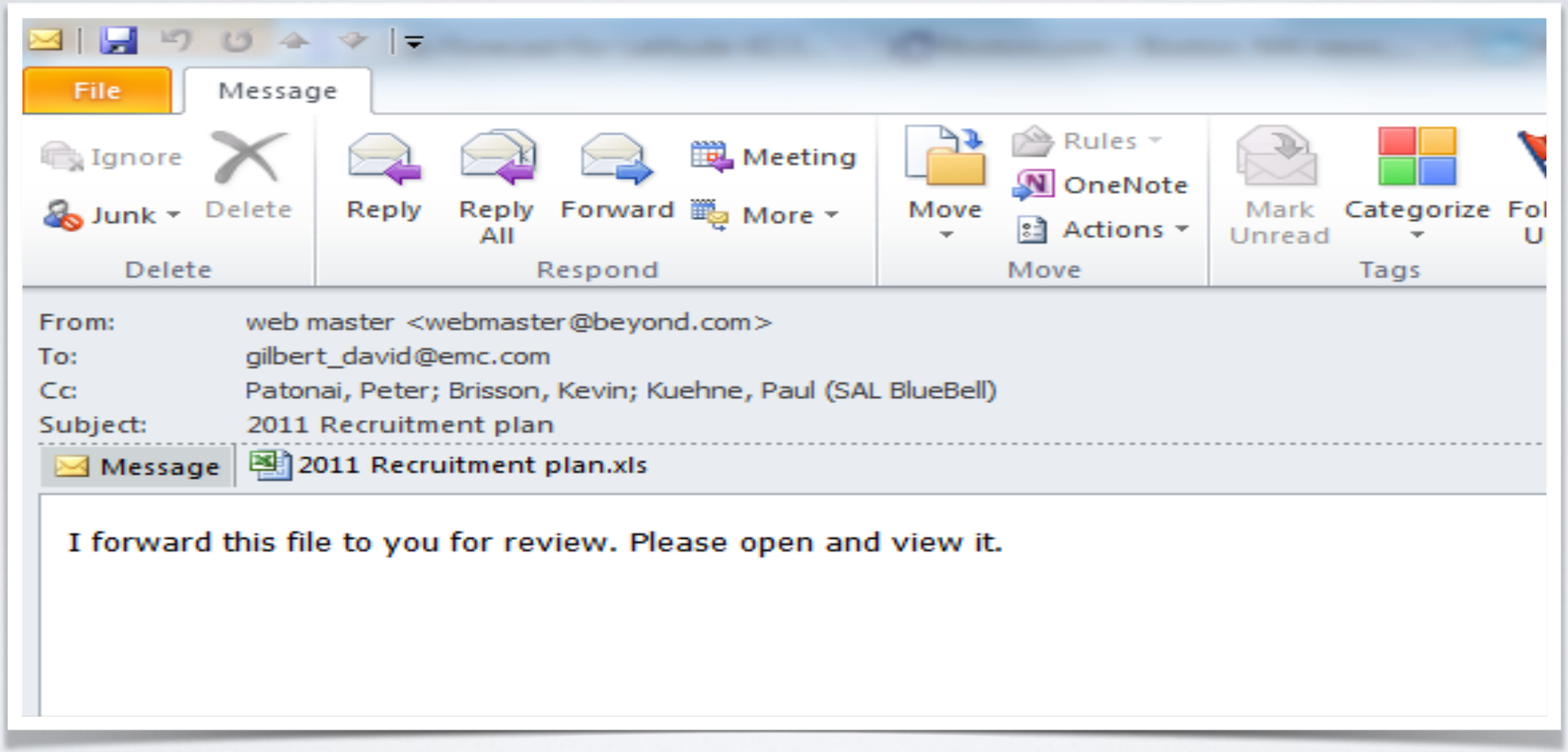
Special Offer

- Evaluate RSA SecurID

Weekly Webinar

RSA invites you to connect with SecurID technical experts for a

WAIT…CYBERWHAT?



WAIT…CYBERWHAT?

RSA hack targeted Flash vulnerability

The mid-March hack that affected RSA was made possible by an Adobe Flash vulnerability, the computer security company has disclosed.On Friday, Uri Rivner, RSA's head of new technologies for consumer identity protection, detailed the methods used to penetrate RSA.

By Jack Clark for Mapping Babel | April 2, 2011 -- 13:11 GMT (14:11 BST) | Topic: Storage

The mid-March hack that affected RSA was made possible by an Adobe Flash vulnerability, the computer security company has disclosed.

On Friday, Uri Rivner, RSA's head of new technologies for consumer identity protection, detailed the methods used to penetrate RSA. The attack, which RSA disclosed on March, saw hackers steal information about RSA's SecureID authentication tokens, which are used to perform two-factor authentication for users of various networks.

WAIT…CYBERWHAT?

Arthur W. Coviello, Jr.

To Our Customers:

On March 17, 2011, RSA publicly disclosed that it had detected a very sophisticated cyber attack on its systems, and that certain information related to the RSA SecurID® product had been extracted. We immediately published best practices and our prioritized remediation steps, and proactively reached out to thousands of customers to help them implement those steps. We remain convinced that customers who implement these steps can be confident in their continued security, and customers in all industries have given us positive feedback on our remediation steps.

Certain characteristics of the attack on RSA indicated that the perpetrator's most likely motive was to obtain an element of security

WAIT…CYBERWHAT?

U.S. Department of Defense
Office of the Assistant Secretary of Defense (Public Affairs)

Speech

On the Web:
http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1369
Media contact: +1 (703) 697-5131/697-5132

Public contact:
http://www.defense.gov/landing/comment.aspx
or +1 (703) 571-3343

Economic Club of Chicago
As Delivered by Secretary of Defense Robert M. Gates, Chicago, IL, Thursday, July 16, 2009

Consider that by 2020, the United States is projected to have nearly 2,500 manned combat aircraft of all kinds. Of those, nearly 1,100 will be the most advanced fifth generation F-35s and F-22s. China, by contrast, is projected to have no fifth generation aircraft by 2020. And by 2025, the gap only widens. The U.S. will have a[n] ately 1,700 of the most advanced fifth generation fighters versus a handful of comparable aircraft for the Chinese. Nonethele[ss] portray this scenario as a dire threat to America's national security.

WAIT…CYBERWHAT?

WAIT…CYBERWHAT?

WAIT…CYBERWHAT?

WAIT…CYBERWHAT?

WAIT…CYBERWHAT?

WAIT…CYBERWHAT?

Cyberwarfare is a reality of any modern conflict.

> The war in Ukraine follows this pattern. The Russian military poured across the Ukrainian border on February 24, 2022, with a combination of troops, tanks, aircraft, and cruise missiles. But the first shots were in fact fired hours before when the calendar still said February 23. They involved a cyberweapon called "Foxblade" that was launched against computers in Ukraine. Reflecting the technology of our time, those among the first to observe the attack were half a world away, working in the United States in Redmond, Washington.

Microsoft, "Defending Ukraine: Early Lessons from the Cyber War", https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

THE 5Ws OF A CYBER ATTACK

WHO?

Other actors

- Research
  - academia
  - agencies
  - individuals
- Security firms and experts
- White-hat hackers
- CERTs and government agencies
- MIL & Defense

THE 5Ws OF A CYBER ATTACK

WHAT?

Activities of interest:

- Data theft
- Machine control
- Financial fraud
- Disruption of operation
- Defacing
- Physical damage

THE 5Ws OF A CYBER ATTACK

WHY?

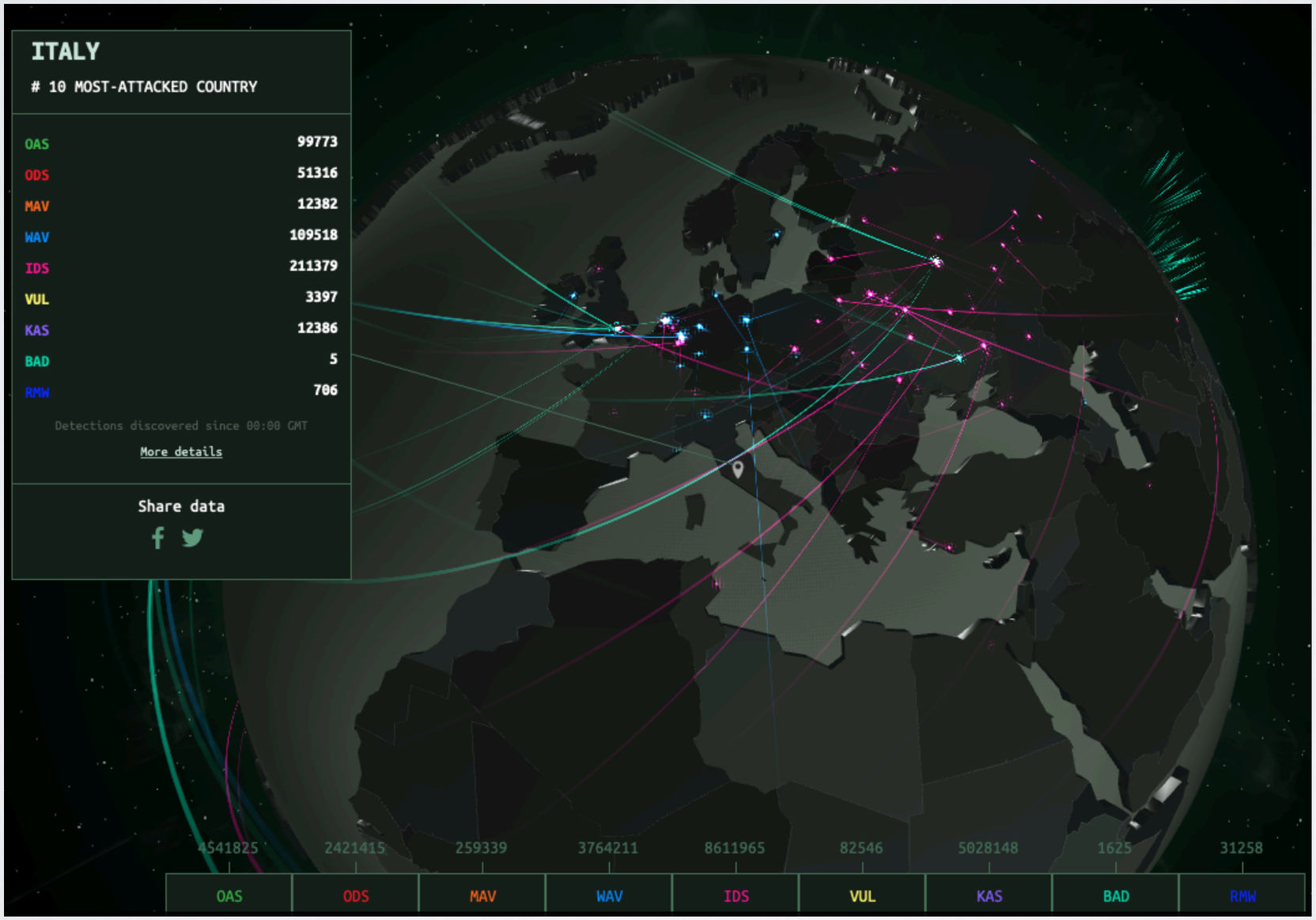
Motivations:

- Financial gain
- Politics/ Hacktivism
- Doxing
- Terrorism / Cyberwarfare
- Revenge

THE 5Ws OF A CYBER ATTACK

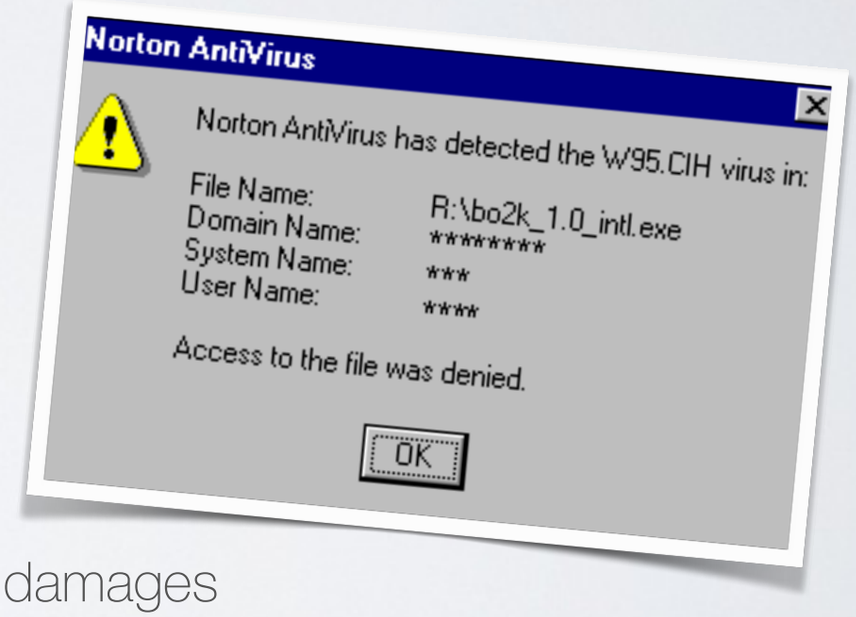
WHEN? WHERE?

https://cybermap.kaspersky.com



THE EVOLUTION OF MALWARE

- 1998 - CIH (aka Chernobyl)
  - Developed by a taiwanese student (Cheng Ing-Hau)
    - as a challenge against bold claims of antiviral efficiency by antivirus software developers
  - CIH spreads under the Portable Executable file format under Windows 9x, ME
  - The size of the virus is around 1 kilobyte (but infected files don't grow)
  - Payload
    - overwrites the first megabyte of space on available HDs causing the SO to hang
    - tries to overwrite the Flash BIOS causing permanent hardware damage
  - Spread
    - CIH infected 60 million computers and caused $1.6 billion in damages



THE EVOLUTION OF MALWARE

- 1998 - First distributed denial of service attack
- 2001 - Code Red
  - Targeted U.S. government websites, it was seen as a potential cyber-attack by terrorists or a foreign government
  - White House website was shut down temporarily
  - Exploited a flaw in the Microsoft Internet Information server, which allowed it to vandalize websites
  - Red infected 359,000 computers at its peak, on June 19

THE EVOLUTION OF MALWARE

- 2003 - Slammer
  - Fastest-spreading computer virus EVER
    - more than 75000 hosts (90% of targets) were infected in less than 10 minutes
    - In approximately 3 minutes, the worm achieved its full scanning rate
    - it was then limited by available bandwidth
  - Exploiting a buffer-overflow vulnerability in computers on the Internet running Microsoft's SQL Server or Microsoft SQL Server Desktop Engine (MSDE)
  - It contained no dangerous payload
  - But it completely saturated available bandwidth causing a DDoS blocking Bank of America ATMs, a 911 ER system in Washington state and an Ohio nuclear plant

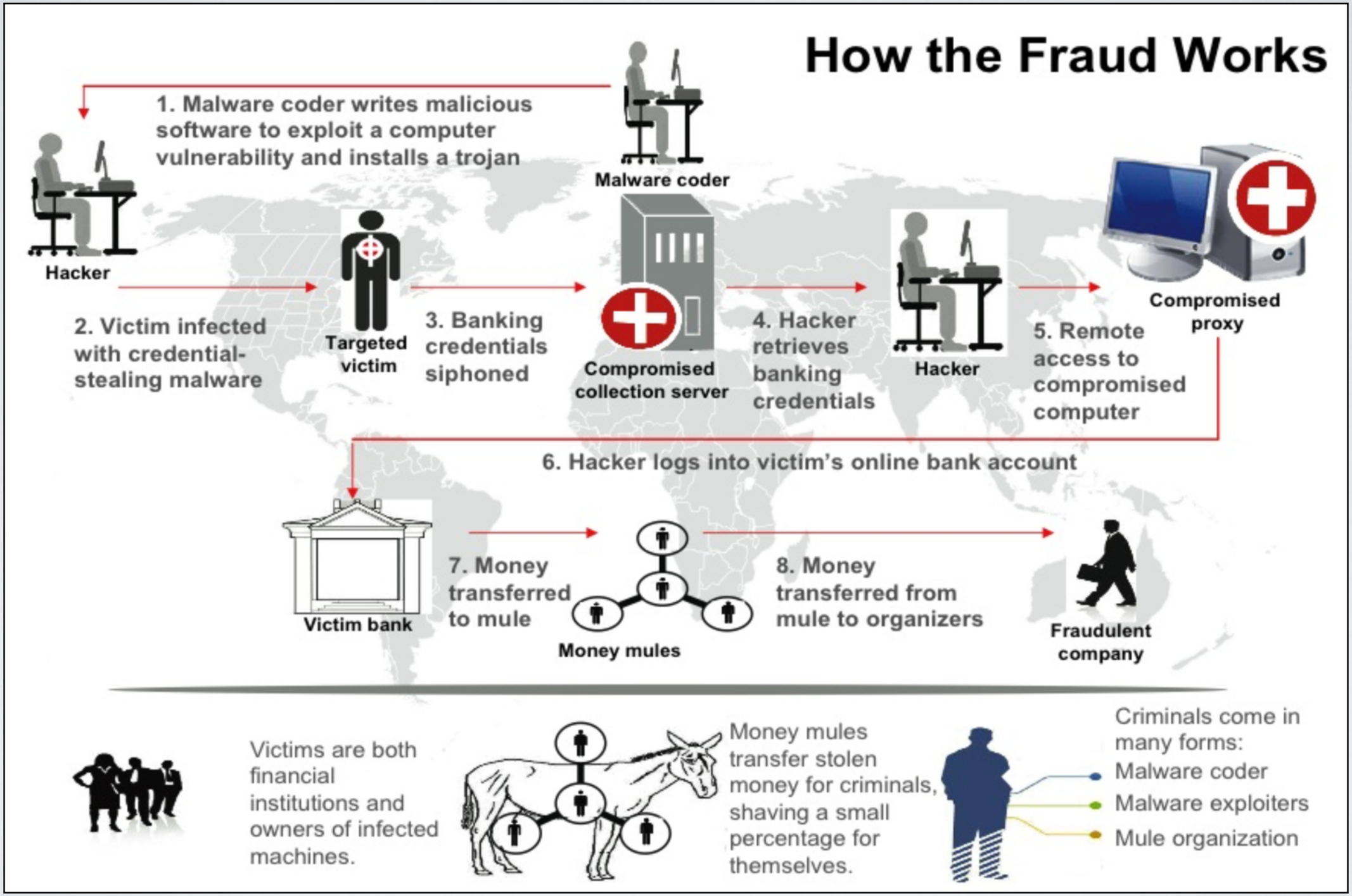
THE EVOLUTION OF MALWARE

- 2004 - MyDoom
  - First serious example of worm spreading through spam
  - Payloads
    - A DDoS attack toward www.sco.com
    - A backdoor
- 2005 - Poison Ivy
  - First example of RAT (Remote access Trojan)
  - gave attacker full access to computer for
    - surveillance
    - data exfiltration

THE EVOLUTION OF MALWARE

- 2007 - Zeus
  - Designed to install key loggers on victims' machines and steal bank passwords
  - Delivered through phishing techniques
  - Installs and hide with a trusted certificate
  - Provides hidden access to the infected machine
  - At that time represented the largest botnet on the Internet: some 3.6 million PCs are said to be infected in the U.S. alone

THE EVOLUTION OF MALWARE



THE EVOLUTION OF MALWARE

- 2008 - Agent.btz
  - Data stealing software
  - Transmission via thumb drives
  - The first drive was left in the parking lot of a US military base
  - First example of spyware?

THE EVOLUTION OF MALWARE

- 2010 - Stuxnet
  - First example of cyber-weapon with unprecedented complexity
  - Developed to hamper the uranium enrichment process in Iran
  - Delivered via thumb drives (unconfirmed)
  - Payload
    - Infected SCADA appliances controlling centrifuges
    - It forced centrifuges to spin outside suggested bounds for long periods
    - Meanwhile it reported safe working conditions to monitoring consoles
  - It delayed enrichment process between 18 and 24 months (unconfirmed)
  - Developed by US and Israeli governments (unconfirmed)

THE EVOLUTION OF MALWARE

- 2010 - Digitar
  - First time the target of the attack was a root certification authority
  - Several servers of the CA were owned
  - Hackers were able to issue hundreds of valid certificates
  - The Diginotar CA was blacklisted to avoid possible consequences
  - Diginotar filed for bankruptcy a few months later

THE EVOLUTION OF MALWARE

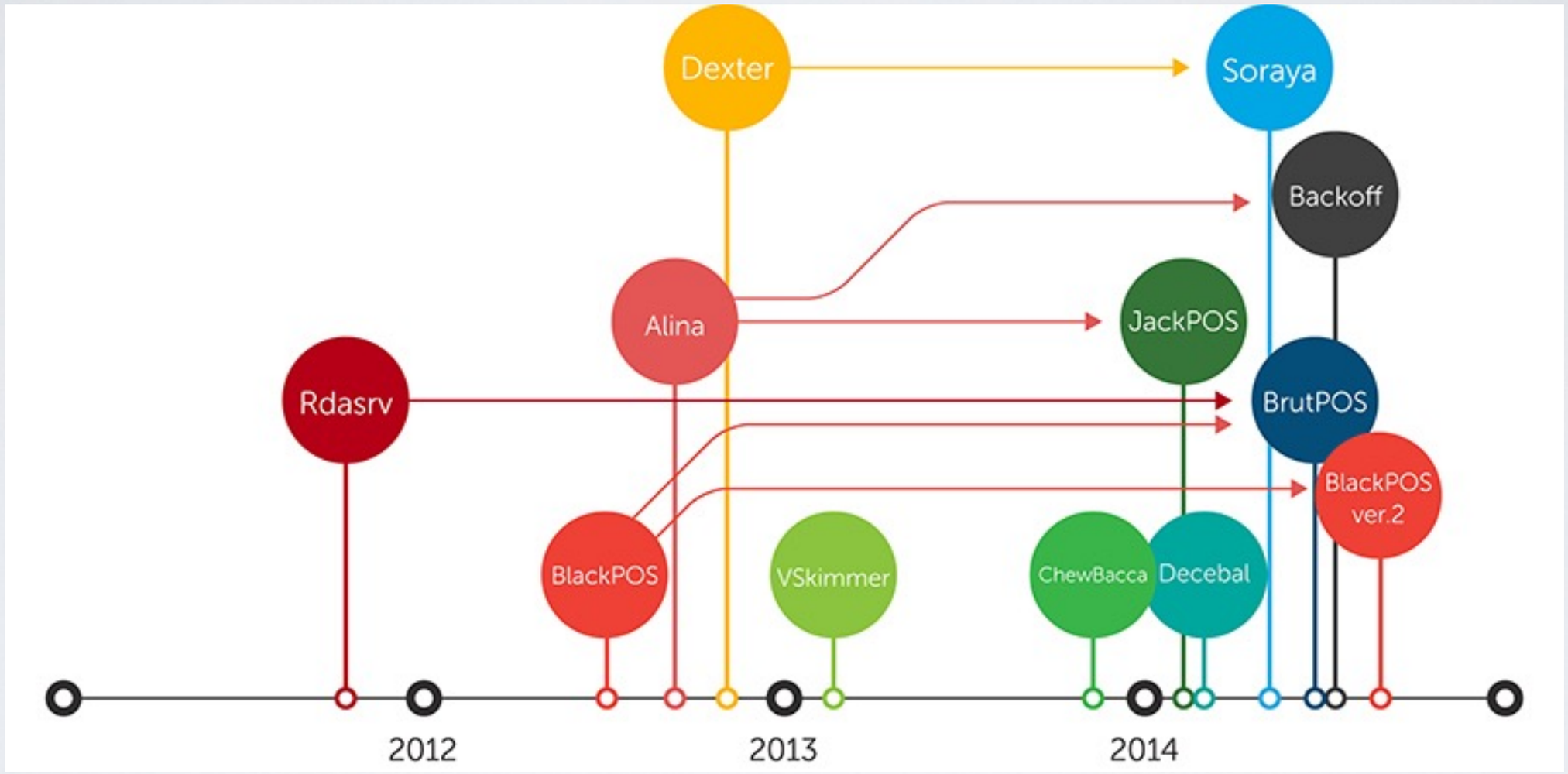
- 2012 - Flame
  - Extremely complex and modular malware
  - Used to perform targeted cyber-espionage
  - Majority of targets were in Iran
  - Flame was signed with a fraudulent certificate purportedly from the Microsoft Enforced Licensing Intermediate PCA certificate authority
  - Exploited an MD5 collision to build a trustable certificate

THE EVOLUTION OF MALWARE

- 2017 - Wannacry, NotPetya
  - Growth of ransomware
  - Use of advanced exploits (EternalBlue against unpatched SMB stack)
  - NotPetya used in large-scale attack against Ukraine
    - Its ransomware nature was modified to transform it in a destructive malware.

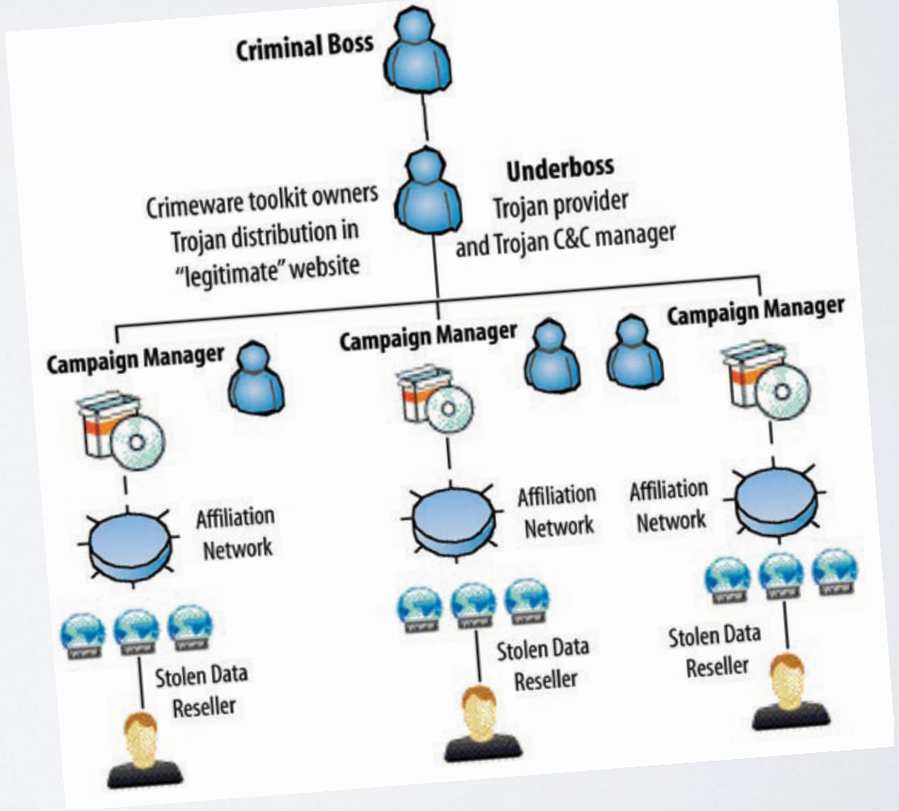
THE EVOLUTION OF CYBERATTACKS

- A growing trend towards POS malware



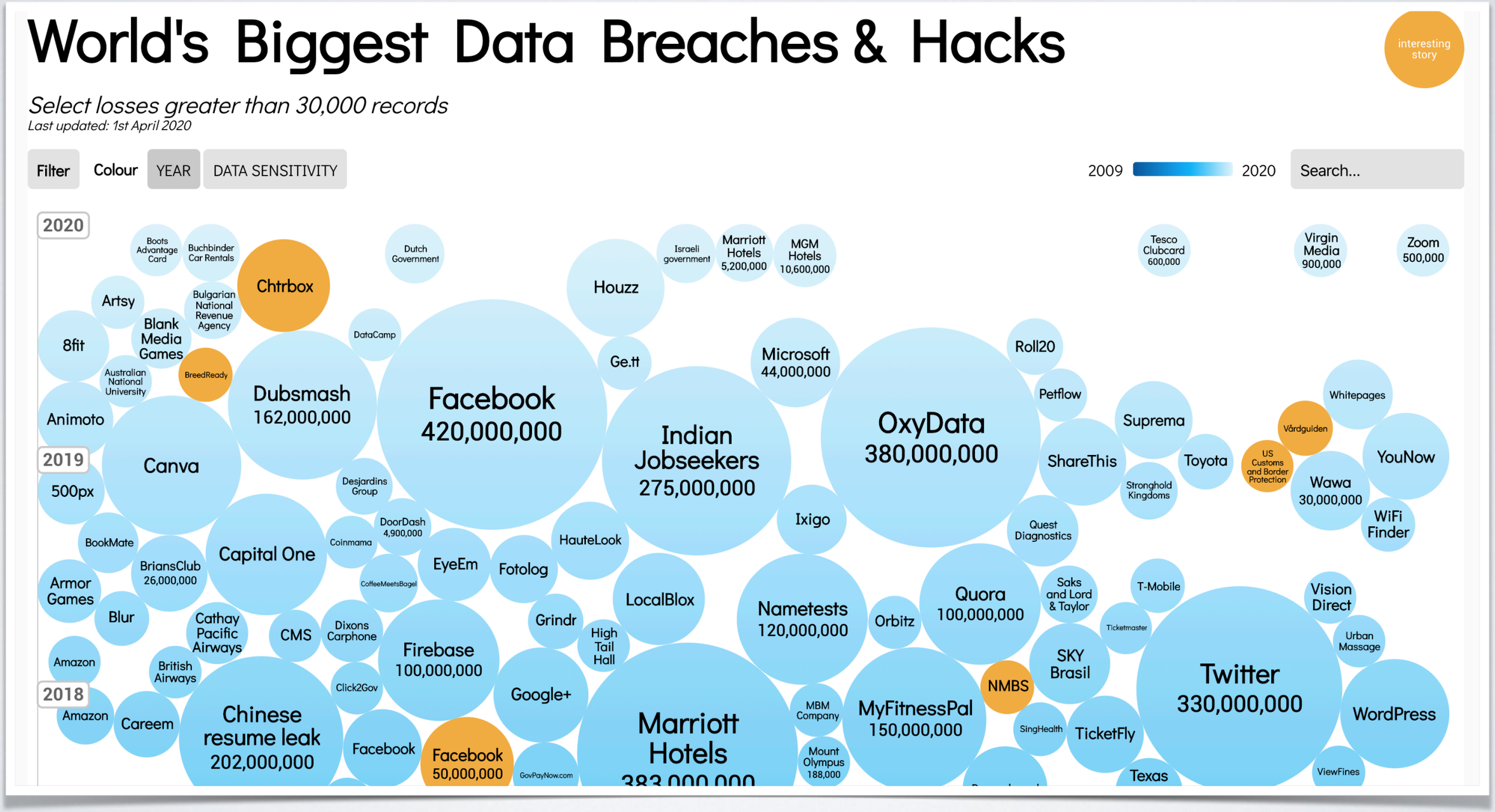
THE EVOLUTION OF CYBERATTACKS

- Evolution of the attacker:
  - nerdy teen
  - full-fledged experts (hackers)
  - structured criminal organizations
- More than the attacker, his motivations evolved
  - “I’m a hacker…cool eh ?”
  - Demonstration, protest, attract media, etc.
  - Increased knowledge
  - Profit
  - Espionage, monitoring, etc.



THE EVOLUTION OF CYBERATTACKS

- A growing trend http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

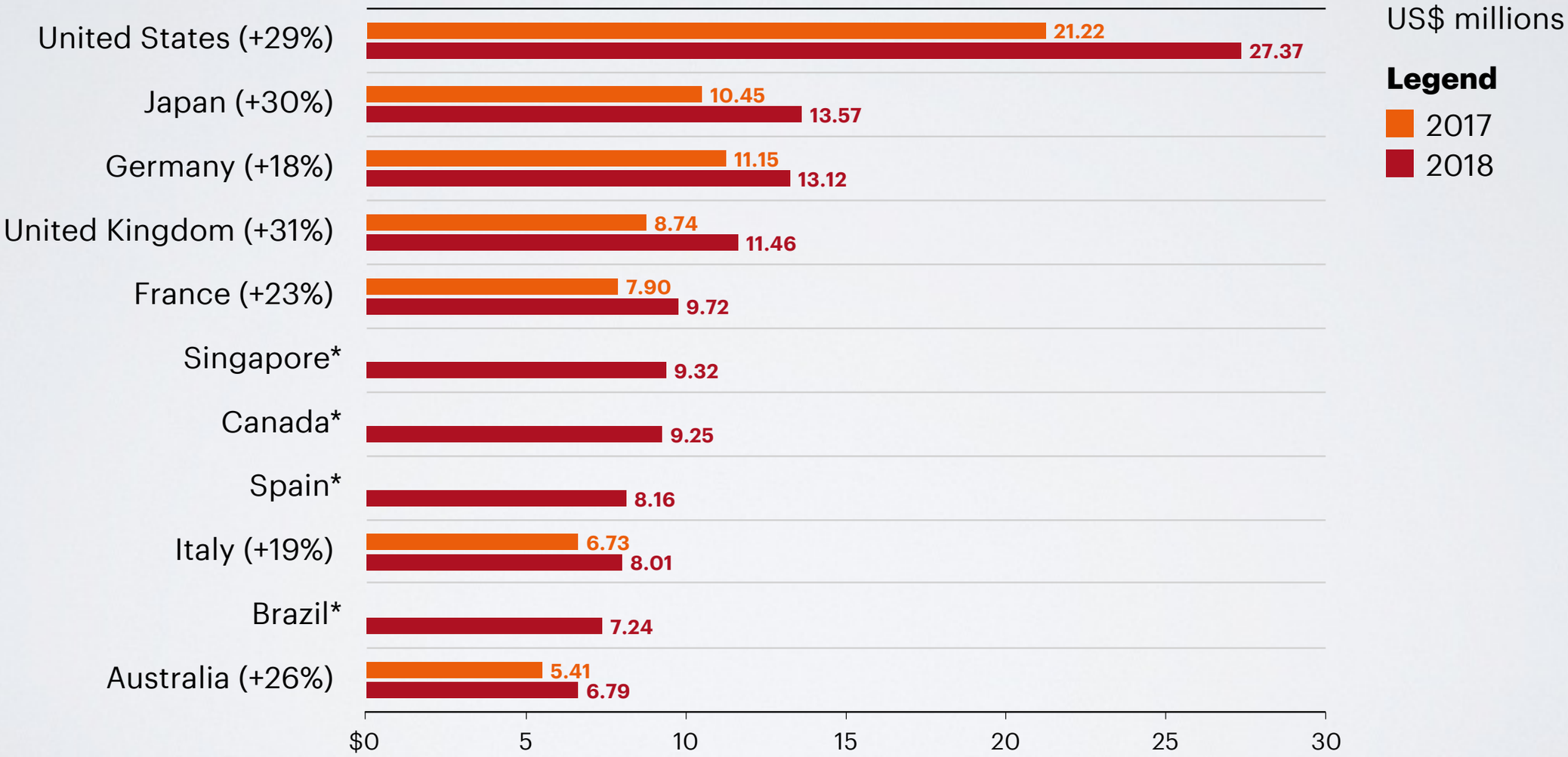


THE EVOLUTION OF CYBERATTACKS

- With growing costs (Accenture 2019)

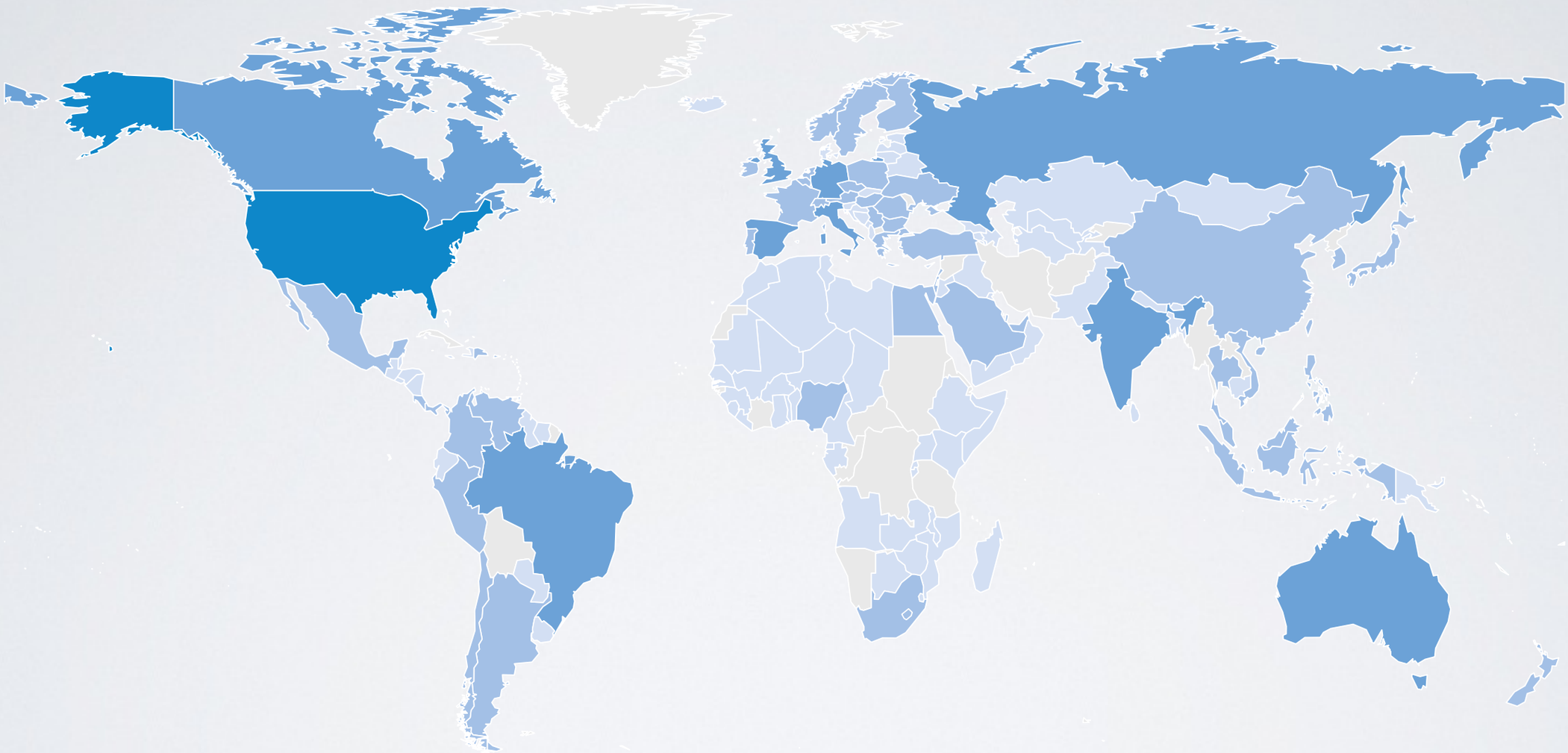
FIGURE 4

The average annual cost of cybercrime by country



THE EVOLUTION OF CYBERATTACKS

- What about today? Demographics



Verizon - 2018 data breach investigation report

THE EVOLUTION OF CYBERATTACKS

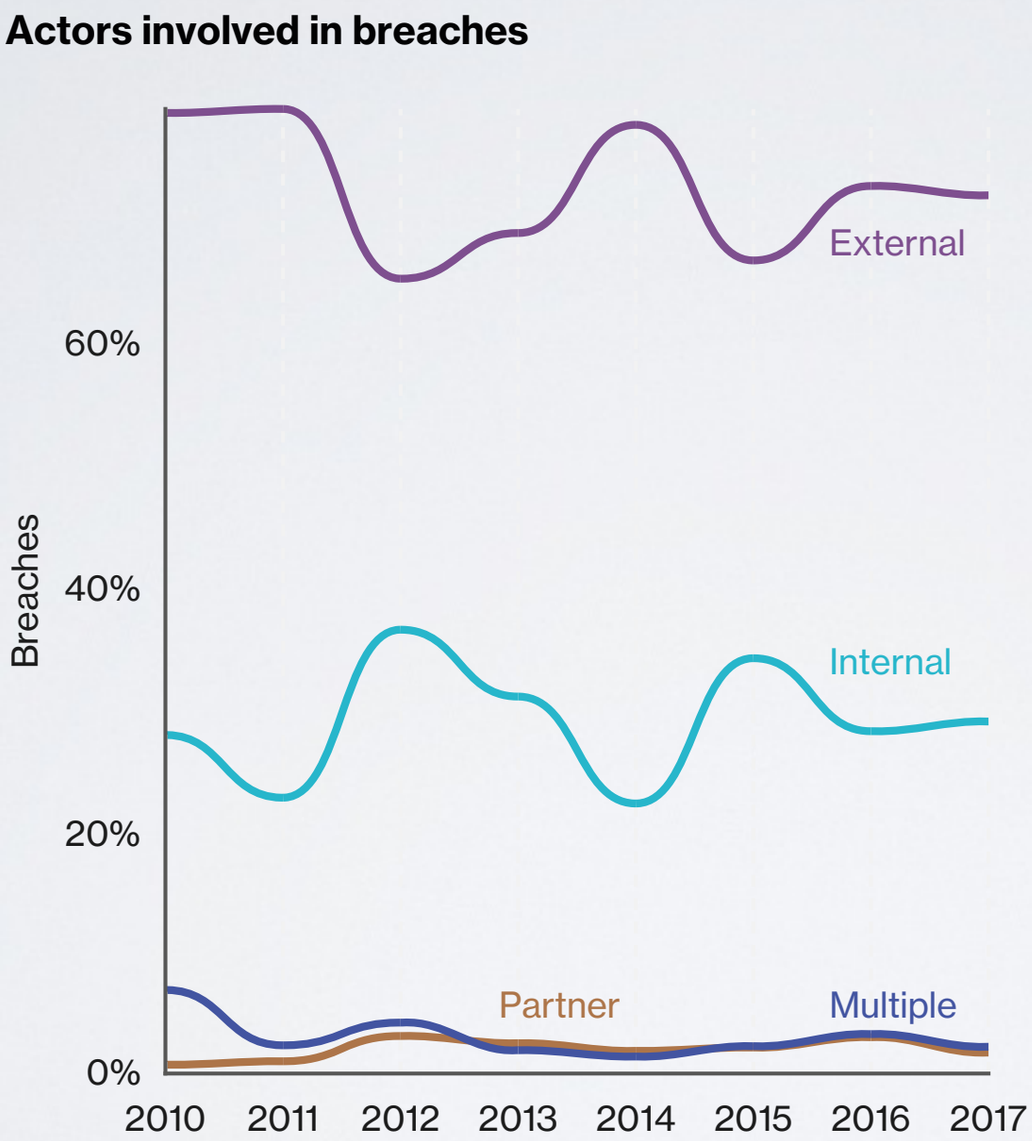
- What about today? Targets

	Incidents				Breaches			
	Large	Small	Unknown	Total	Large	Small	Unknown	Total
Accommodation (72)	40	296	32	368	31	292	15	338
Administrative (56)	7	15	11	33	5	12	1	18
Agriculture (11)	1	0	4	5	0	0	0	0
Construction (23)	2	11	10	23	0	5	5	10
Education (61)	42	26	224	292	30	15	56	101
Entertainment (71)	6	19	7,163	7,188	5	17	11	33
Financial (52)	74	74	450	598	39	52	55	146
Healthcare (62)	165	152	433	750	99	112	325	536
Information (51)	54	76	910	1,040	29	50	30	109
Management (55)	1	0	1	2	0	0	0	0
Manufacturing (31–33)	375	21	140	536	28	15	28	71
Mining (21)	3	3	20	26	3	3	0	6
Other Services (81)	5	11	46	62	2	7	26	35
Professional (54)	158	59	323	540	24	39	69	132
Public (92)	22,429	51	308	22,788	111	31	162	304
Real Estate (53)	2	5	24	31	2	4	14	20
Retail (44–45)	56	111	150	317	38	86	45	169
Trade (42)	13	5	13	31	6	4	2	12
Transportation (48–49)	15	9	35	59	7	6	5	18
Utilities (22)	14	8	24	46	4	3	11	18
Unknown	1,043	9	17,521	18,573	82	3	55	140
Total	**24,505**	**961**	**27,842**	**53,308**	**545**	**756**	**915**	**2,216**

Verizon - 2018 data breach investigation report

THE EVOLUTION OF CYBERATTACKS

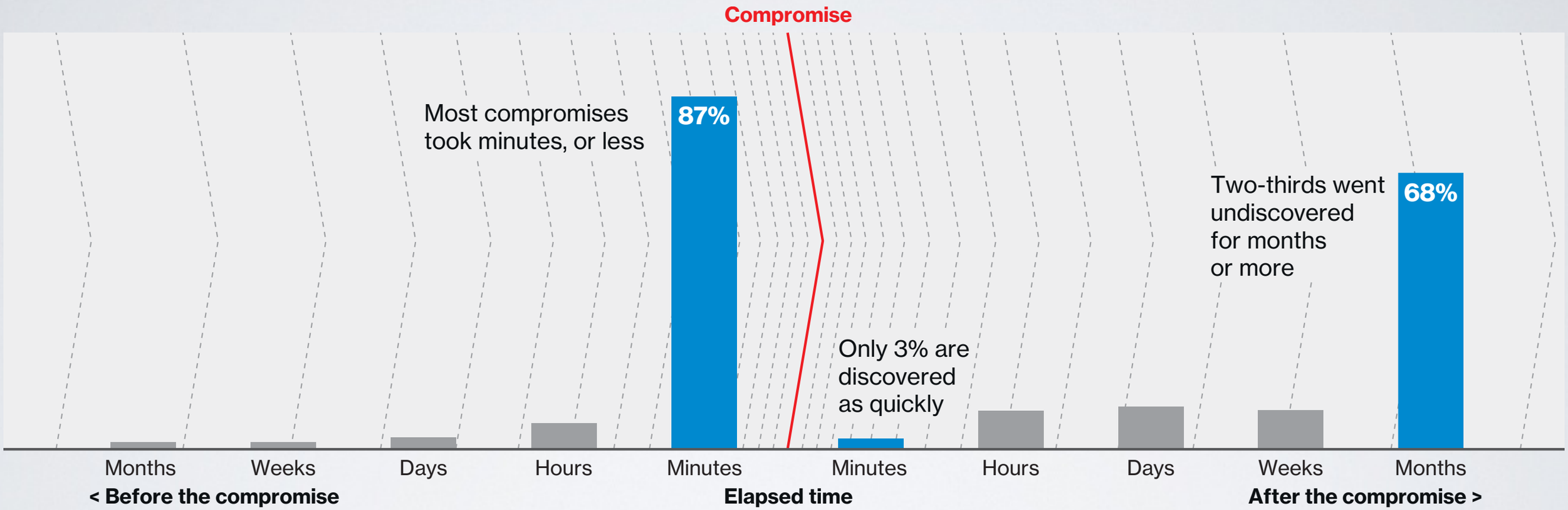
- What about today? Origin



Verizon - 2018 data breach investigation report

THE EVOLUTION OF CYBERATTACKS

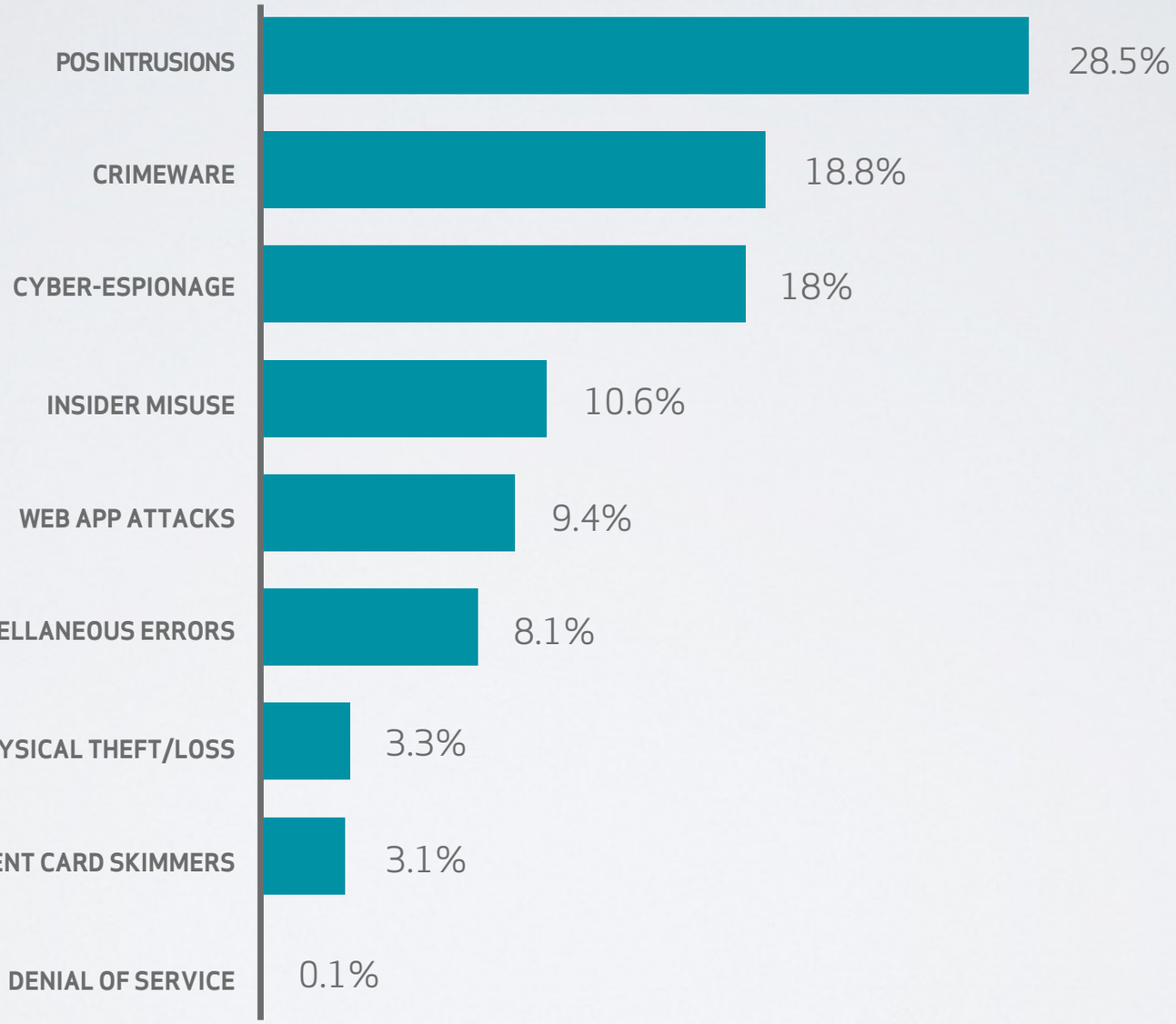
- What about today? Asymmetry



Verizon - 2018 data breach investigation report

THE EVOLUTION OF CYBERATTACKS

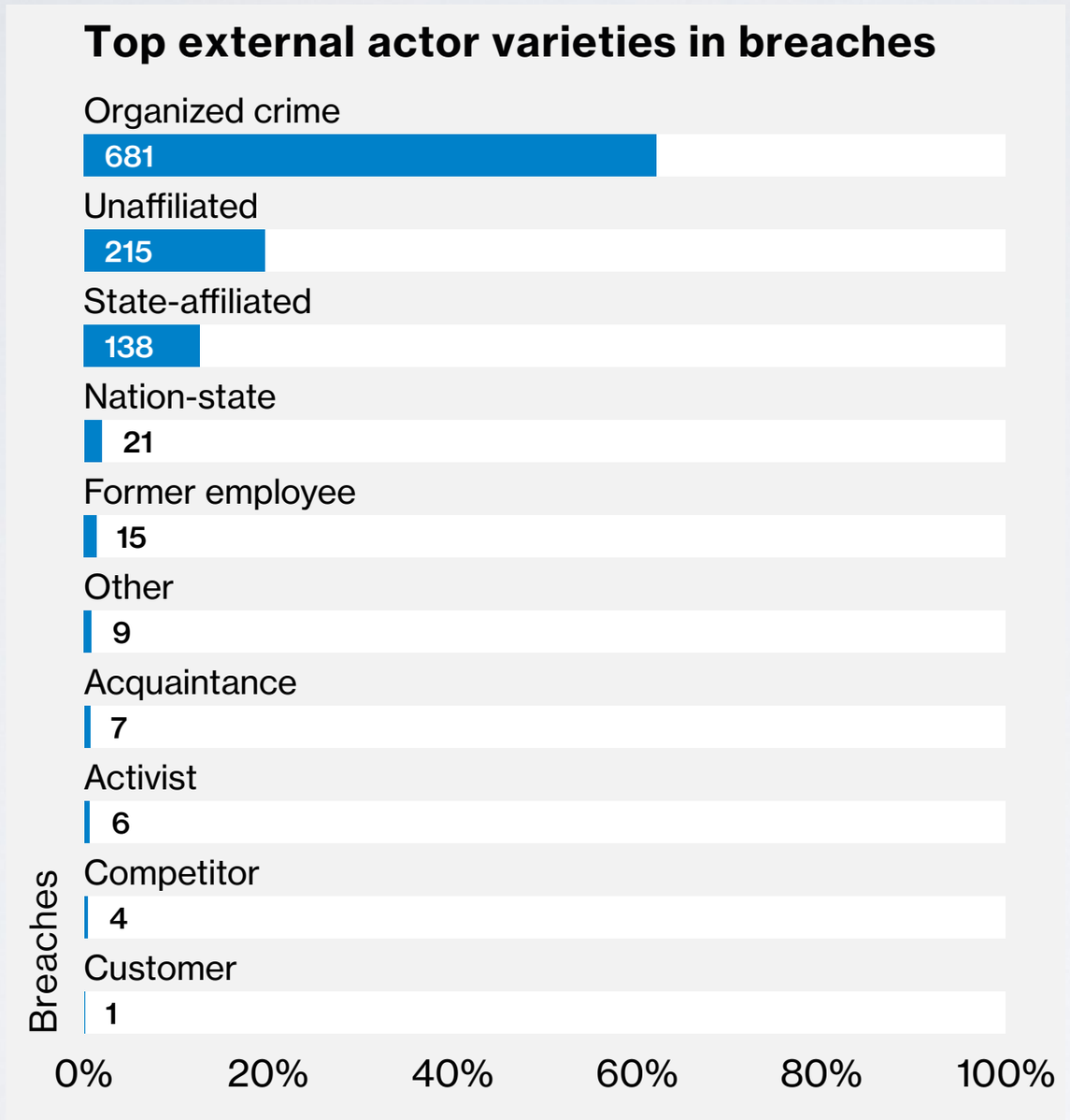
- What about today? Attack methodology



Verizon - 2014 data breach investigation report

THE EVOLUTION OF CYBERATTACKS

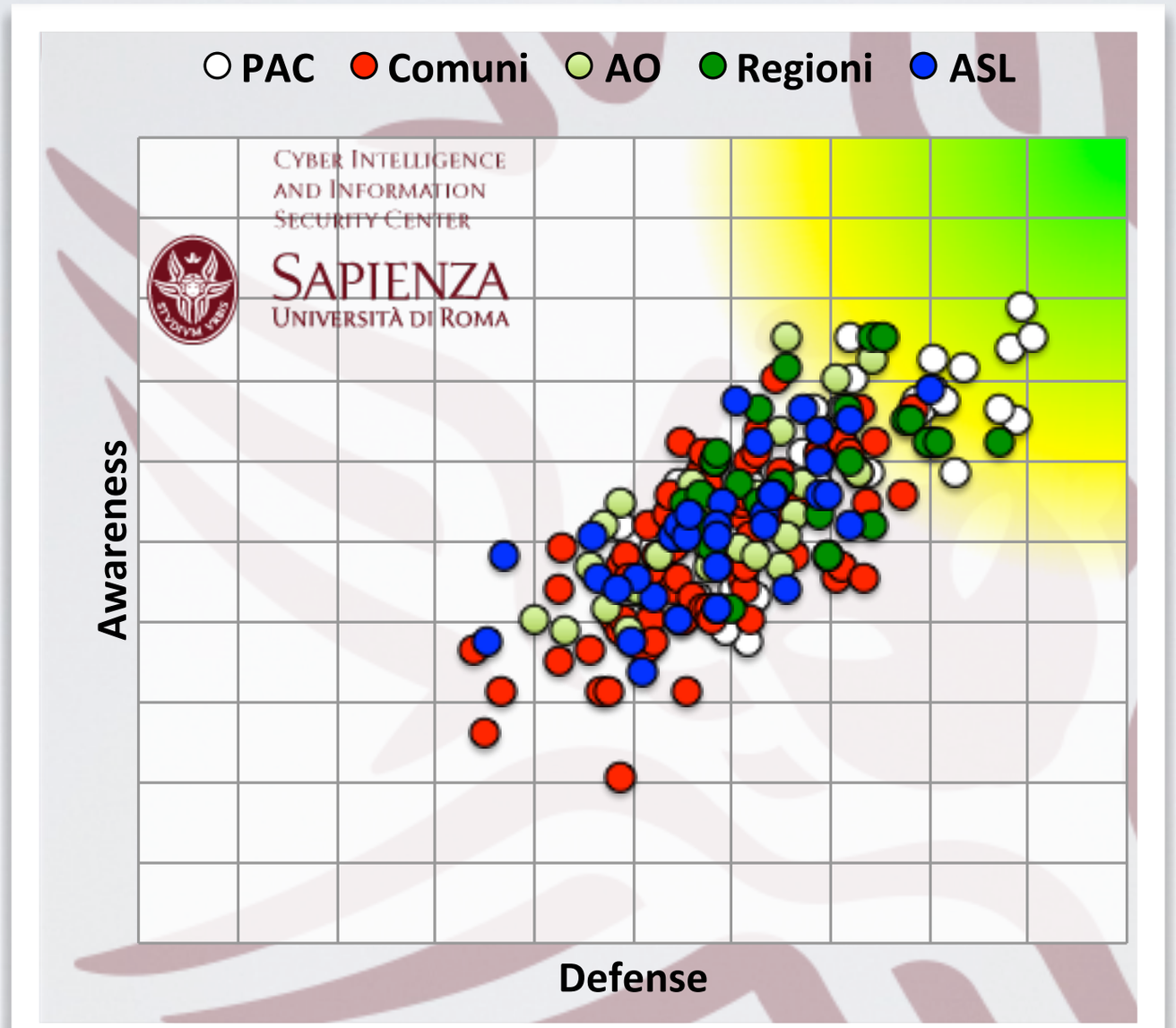
- What about today? Actors



Verizon - 2018 data breach investigation report

THE EVOLUTION OF CYBERATTACKS

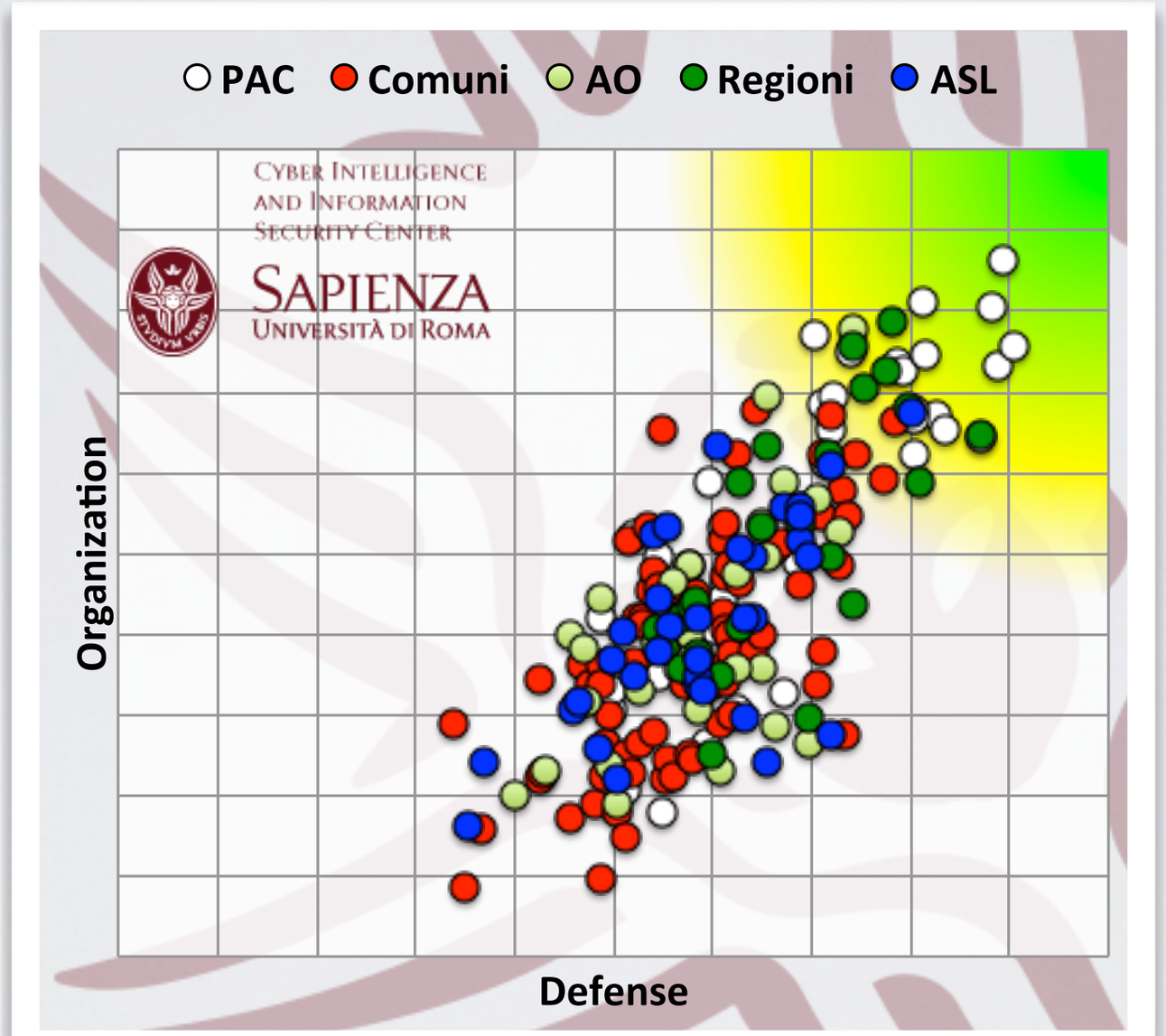
- Is awareness useful?



CIS - 2014 Italian Cyber Security Report

THE EVOLUTION OF CYBERATTACKS

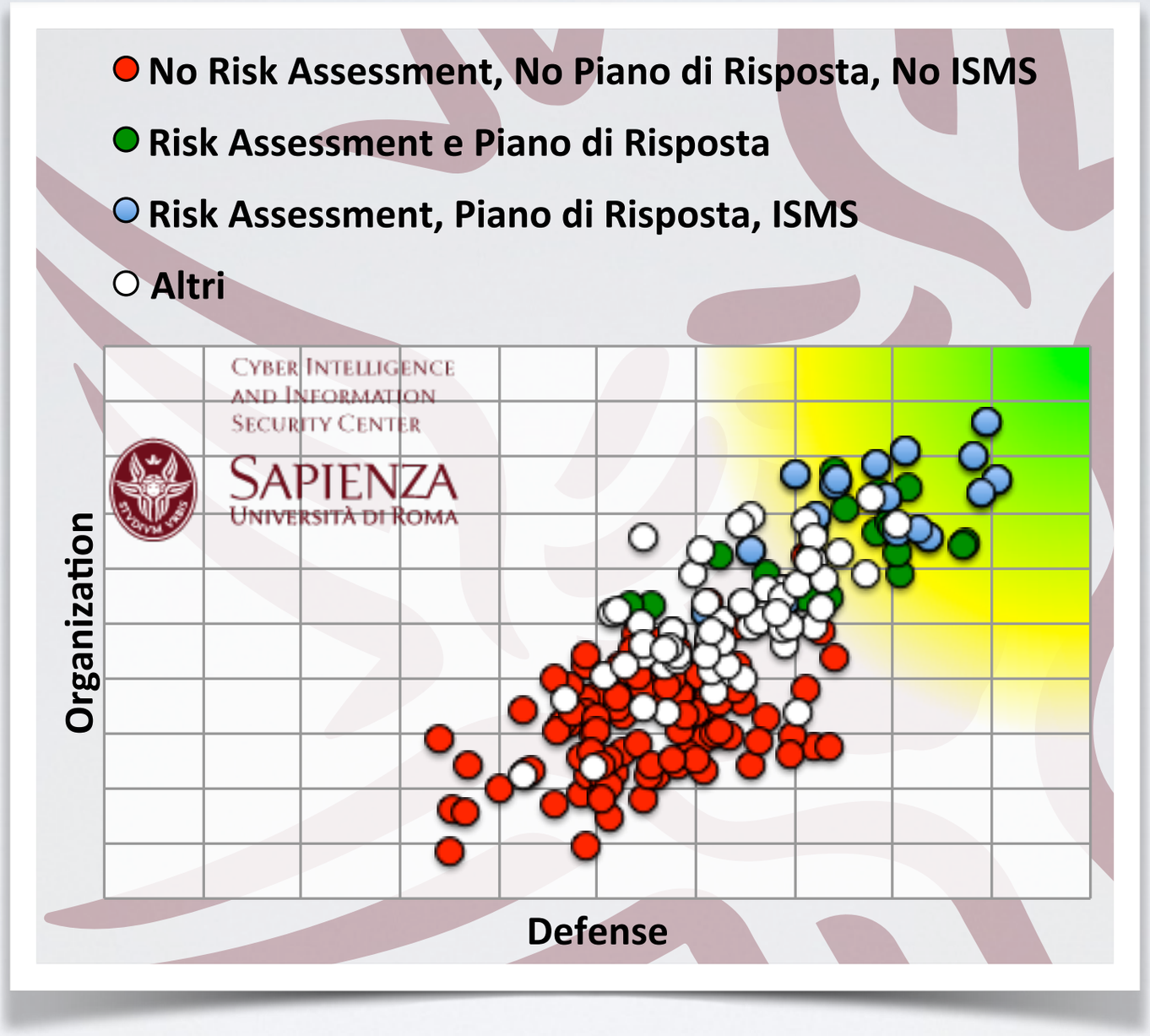
- Is organization useful?



CIS - 2014 Italian Cyber Security Report

THE EVOLUTION OF CYBERATTACKS

- Do best practices help?



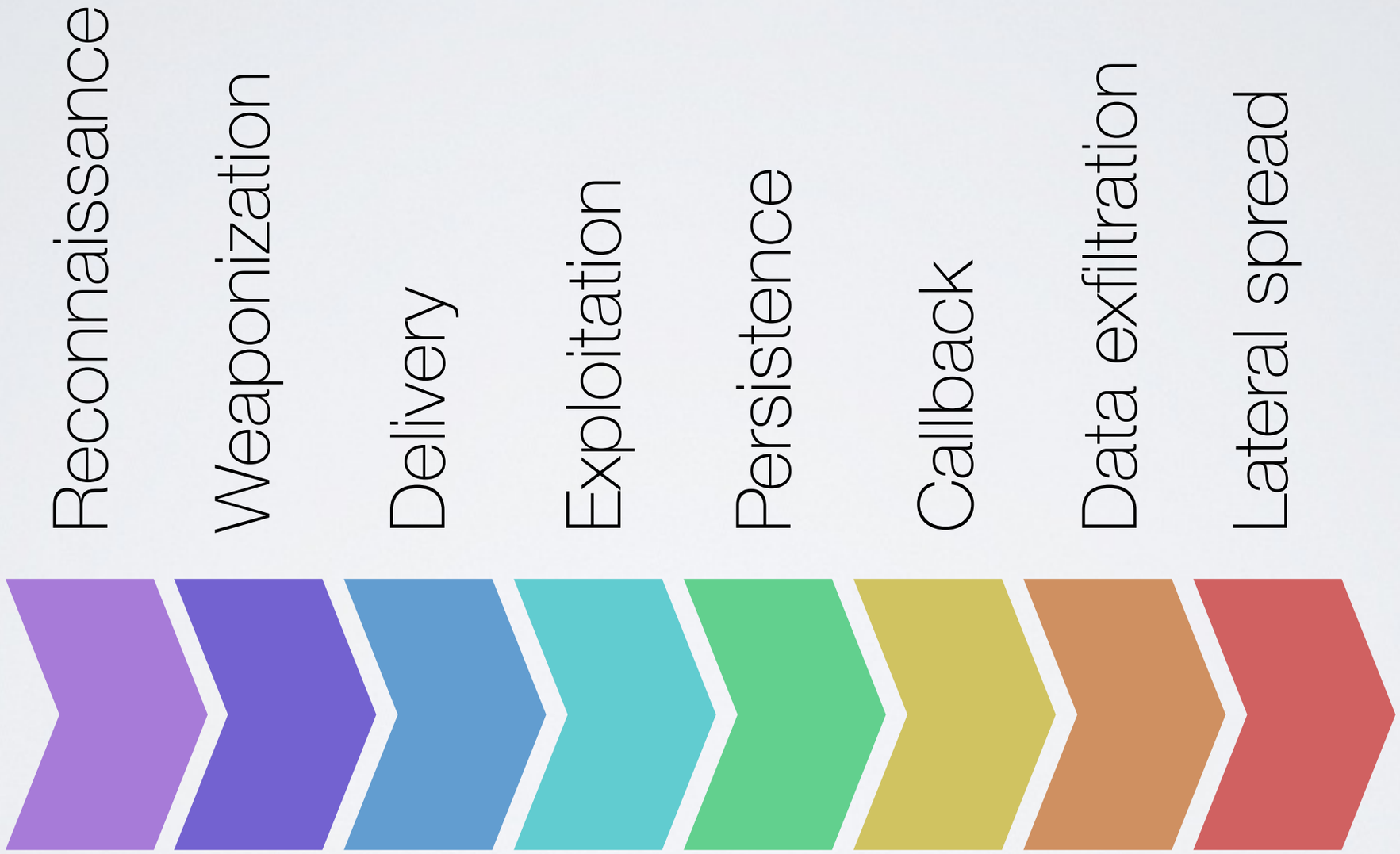
CIS - 2014 Italian Cyber Security Report

ANATOMY OF AN ATTACK

- Most dangerous attacks are today characterised by
  - Precise targeting
    - Mass campaigns vs. precise targeting
  - Full control of target (RAT)
    - Remote access + privilege escalation
    - Multi-step attacks and compromisations
    - The attacker aims to fully control targets
- Long-term persistence (APT)
  - Multiple backdoors
    - Some of them may stay silent to provide backup entrance after target recovery
  - Activity obfuscation
  - Security measure sidesteps + evasion

ANATOMY OF AN ATTACK

- The intrusion “killchain”



ANATOMY OF AN ATTACK

Reconnaissance

- Definition of the target surface
- The attacker looks for the best strategy to apply
- Target profiling
  - Through social media
  - Public data sources
  - Doxing attacks
- Widely underrated phase of an attack

ANATOMY OF AN ATTACK

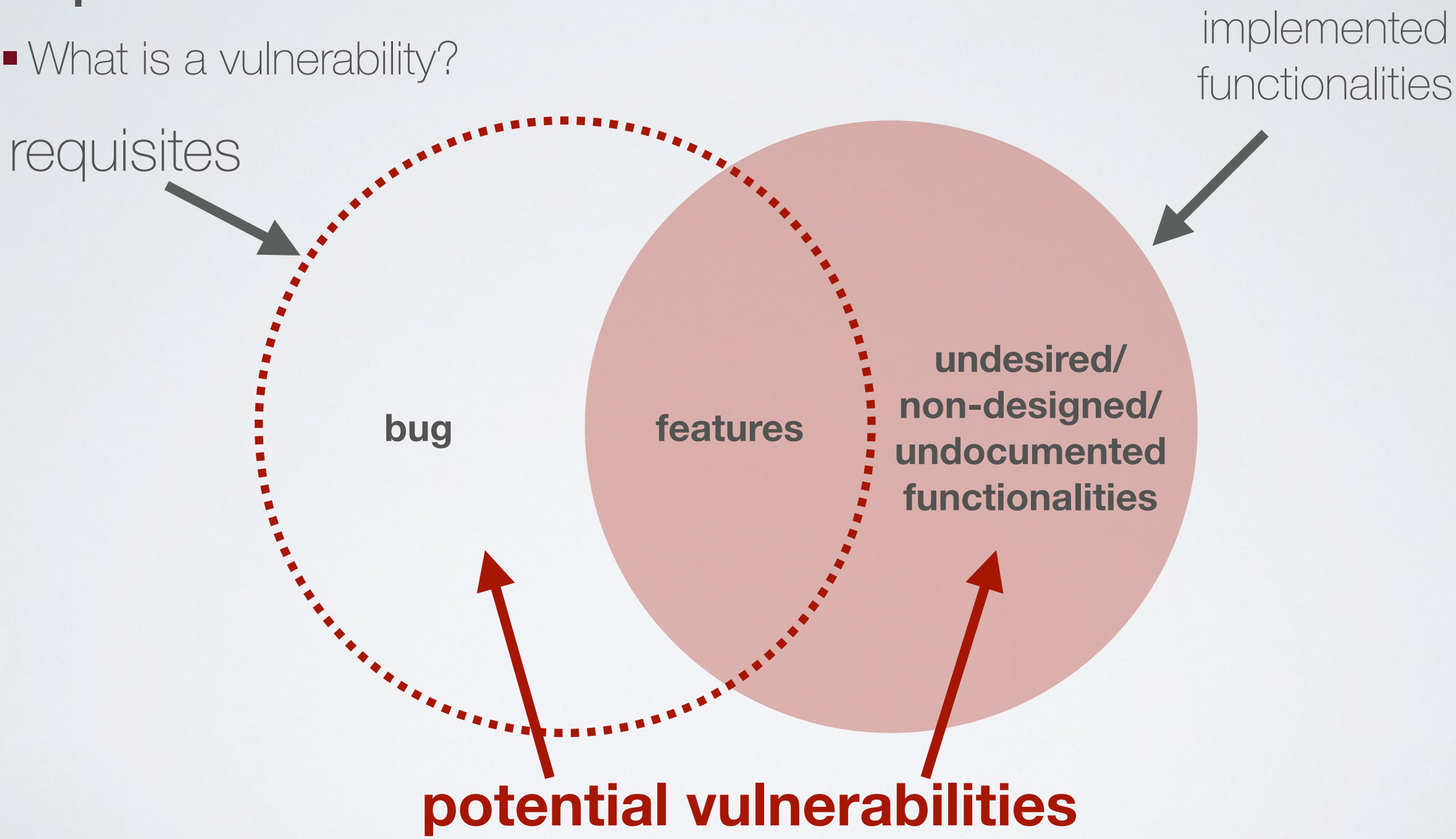
Weaponization

- A theoretical attack (or proof-of-concept) is transformed in running code
- This is the step that requires strong technical skills
- Often “outsourced”
- Unknown vulnerabilities are extremely valuable
  - 0-day exploits
  - Sold for hundreds of $ on black markets
  - Valuable as long as they remain secret

ANATOMY OF AN ATTACK

Weaponization

- What is a vulnerability?



ANATOMY OF AN ATTACK

- New vulnerabilities are discovered every day
- Many of them are already exploited in the wild

Sponsored by DHS/NCCIC/US-CERT

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

NIST National Institute of Standards and Technology

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics | Data Feeds | Statistics | FAQs

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments | Visualizations

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

70170 CVE Vulnerabilities
283 Checklists
249 US-CERT Alerts
4349 US-CERT Vuln Notes
10286 OVAL Queries
103866 CPE Names

Last updated: 5/14/2015 6:34:58 PM

CVE Publication rate: 15.7

Email List

NVD provides four mailing lists to the public. For information and subscription instructions

National Cyber Awareness System

Vulnerability Summary for CVE-2015-3043

Original release date: 04/14/2015

Last revised: 04/22/2015

Source: US-CERT/NIST

Overview

Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in April 2015, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, and CVE-2015-3042.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

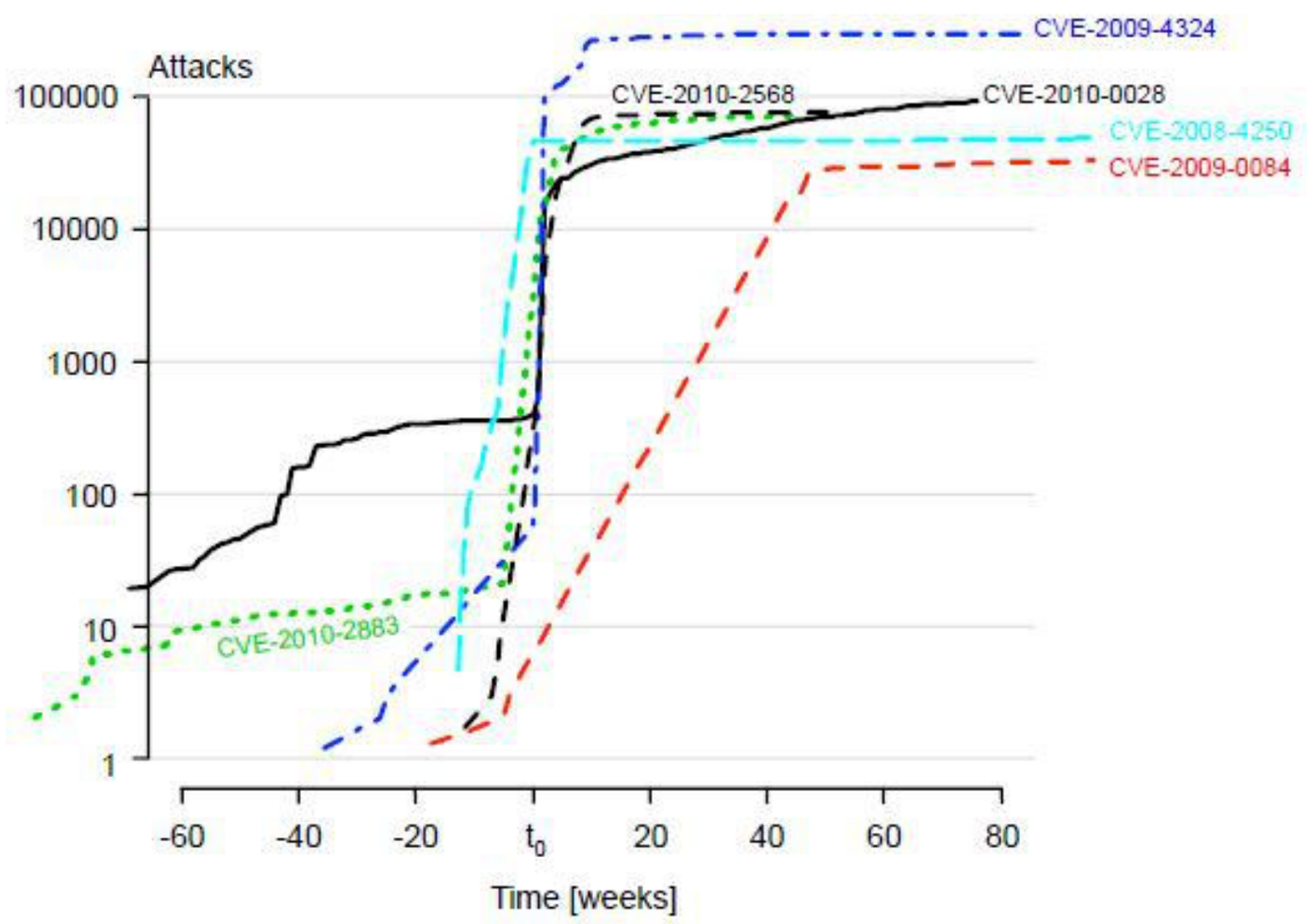
**NOTE: Access Complexity scored Low due to insufficient information

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

ANATOMY OF AN ATTACK

Weaponization

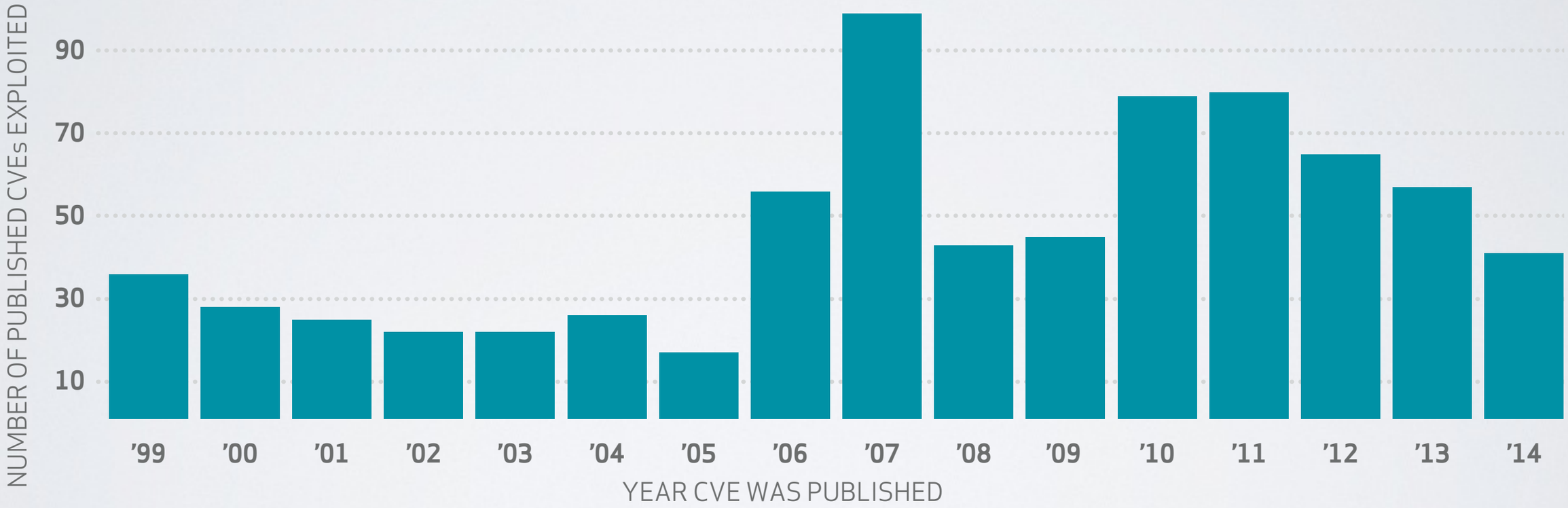


(a) Attacks exploiting zero-day vulnerabilities before and after the disclosure (time = t_0).

ANATOMY OF AN ATTACK

Weaponization

- Old vulnerabilities are still widely exploited

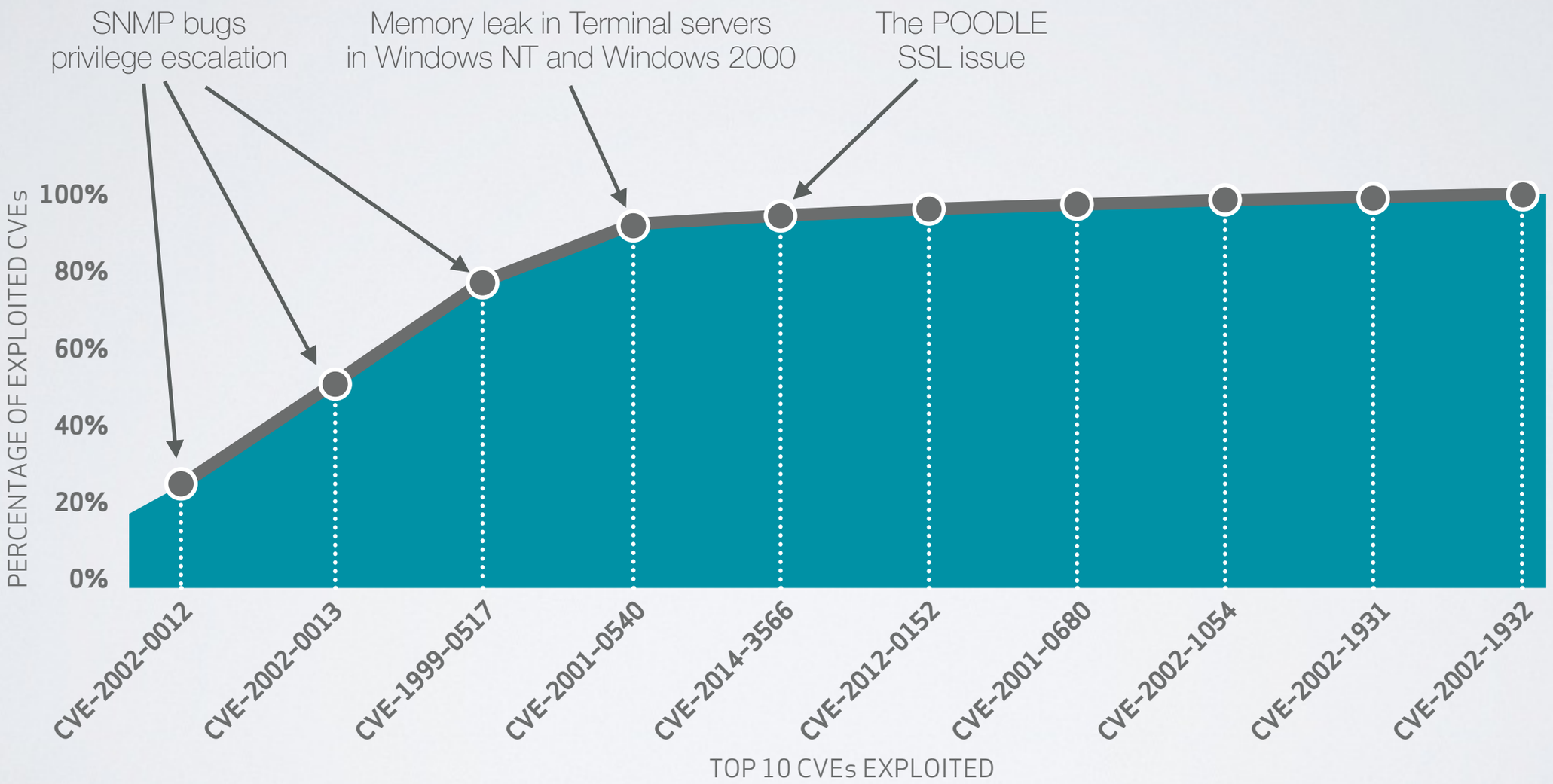


Verizon - 2015 data breach investigation report

ANATOMY OF AN ATTACK

Weaponization

- Few vulnerabilities represent a large fraction of exploits

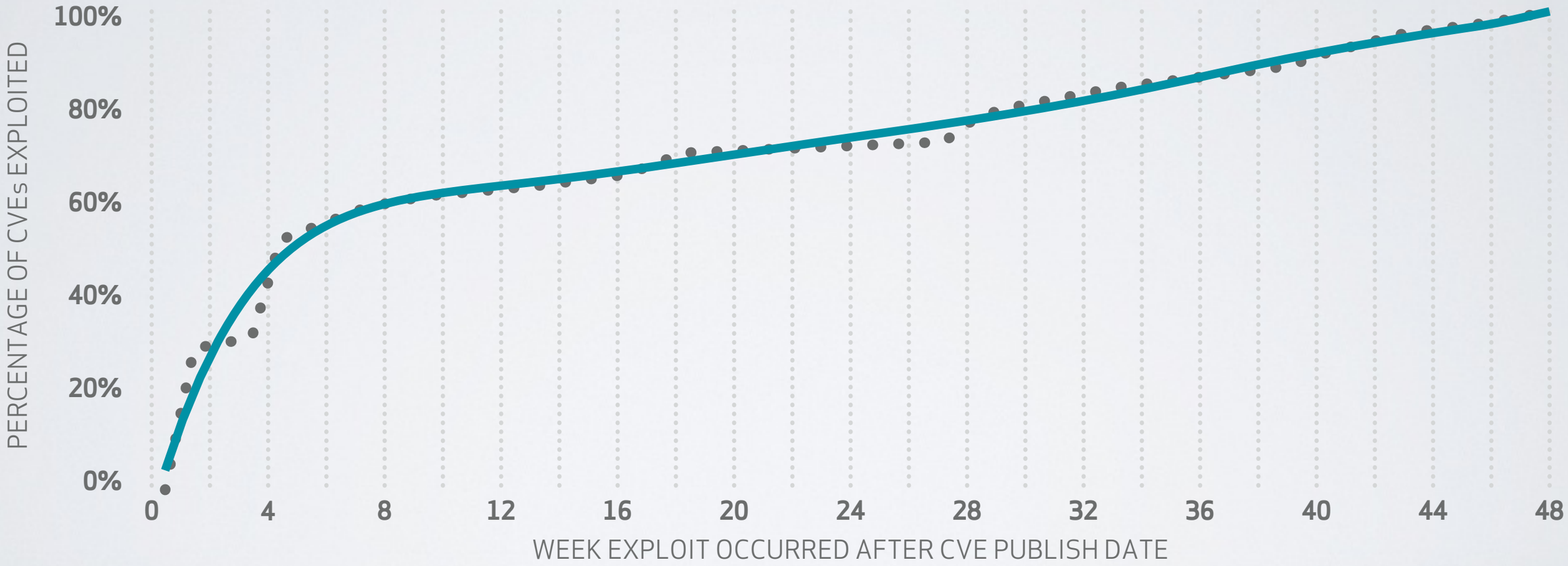


Verizon - 2015 data breach investigation report

ANATOMY OF AN ATTACK

Weaponization

- Time to weaponization is critical



Verizon - 2015 data breach investigation report

ANATOMY OF AN ATTACK

- Example:

FireEye Contact Us: (877) 347-3393 Worldwide

Products Solutions Mandiant Consulting Current Threats

Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack

April 18, 2015 | By Fireeye Labs | Threat Research

FireEye Labs recently detected a limited APT campaign exploiting zero-day vulnerabilities in Adobe Flash and a brand-new one in Microsoft Windows. Using the Dynamic Threat Intelligence Cloud (DTI), FireEye researchers detected a pattern of attacks beginning on April 13th, 2015. Adobe independently patched the vulnerability (CVE-2015-3043) in APSB15-06. Through correlation of technical indicators and command and control infrastructure, FireEye assess that APT28 is probably responsible for this activity.

Microsoft is aware of the outstanding local privilege escalation vulnerability in Windows (CVE-2015-1701). While there is not yet a patch available for the Windows vulnerability, updating Adobe Flash to the latest version will render this in-the-wild exploit innocuous. We have only seen CVE-2015-1701 in use in conjunction with the Adobe Flash exploit for CVE-2015-3043. The Microsoft Security Team is working on a fix for CVE-2015-1701.

Exploit Overview

The high level flow of the exploit is as follows:

1. User clicks link to attacker controlled website
2. HTML/JS launcher page serves Flash exploit
3. Flash exploit triggers CVE-2015-3043, executes shellcode
4. Shellcode downloads and runs executable payload
5. Executable payload exploits local privilege escalation (CVE-2015-1701) to steal System token

The Flash exploit is served from unobfuscated HTML/JS. The launcher page picks one of two Flash files to deliver depending upon the target's platform (Windows 32 versus 64bits).

The Flash exploit is mostly unobfuscated with only some light variable name mangling. The attackers relied heavily on the CVE-2014-0515 Metasploit module, which is well documented. It is ROPless, and

https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html

ANATOMY OF AN ATTACK

Delivery

- the exploit is delivered through a vector
- delivery method
  - phishing
  - spear phishing
  - watering hole

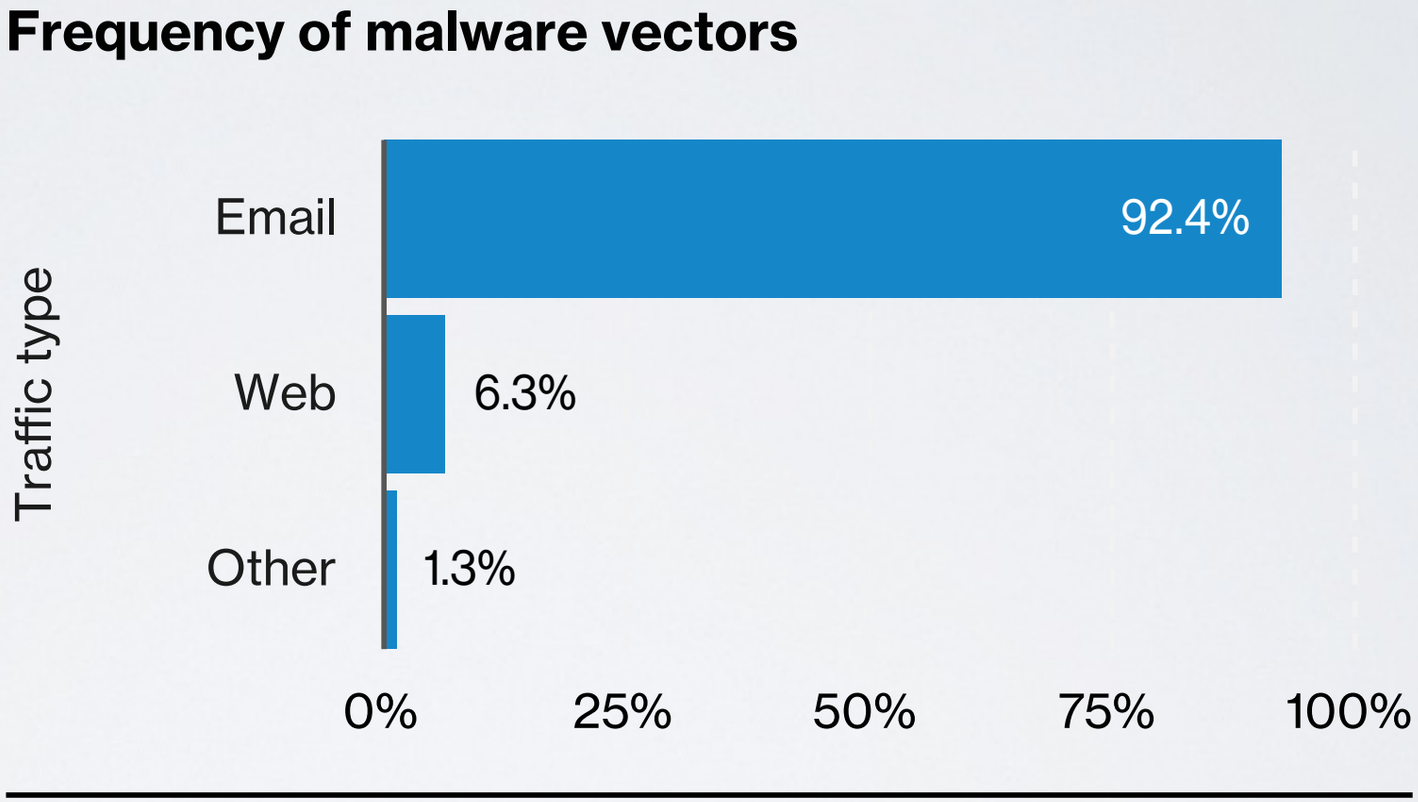


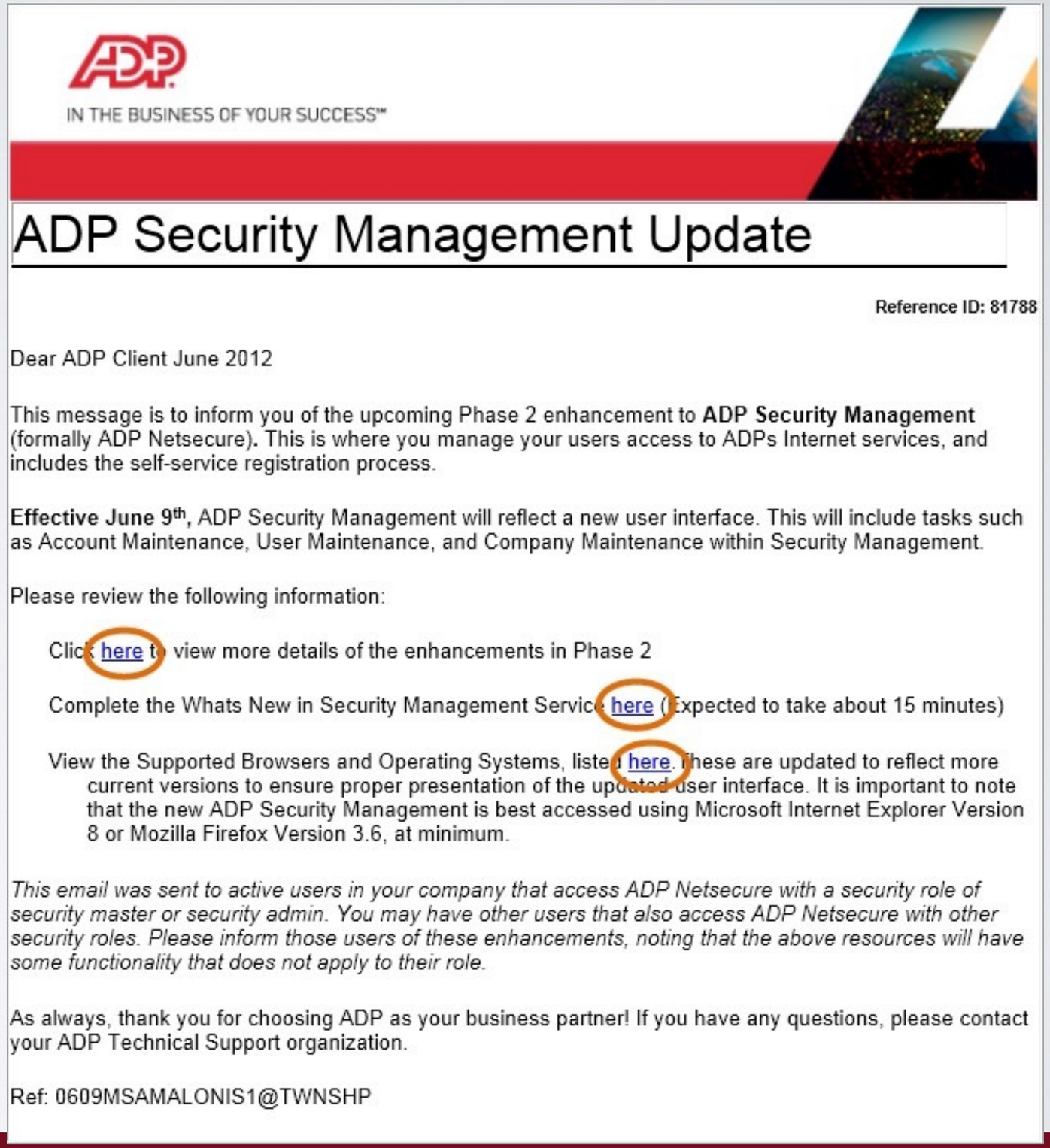
Figure 21. Frequency of malware vectors within detected malware (n=58,987,788)

Verizon - 2018 data breach investigation report

ANATOMY OF AN ATTACK

Delivery

- Spear phishing example



IN THE BUSINESS OF YOUR SUCCESS℠

ADP Security Management Update

Reference ID: 81788

Dear ADP Client June 2012

This message is to inform you of the upcoming Phase 2 enhancement to **ADP Security Management** (formally ADP Netsecure)**.** This is where you manage your users access to ADPs Internet services, and includes the self-service registration process.

Effective June 9th, ADP Security Management will reflect a new user interface. This will include tasks such as Account Maintenance, User Maintenance, and Company Maintenance within Security Management.

Please review the following information:

Click here to view more details of the enhancements in Phase 2

Complete the Whats New in Security Management Service here (Expected to take about 15 minutes)

View the Supported Browsers and Operating Systems, listed here. These are updated to reflect more current versions to ensure proper presentation of the updated user interface. It is important to note that the new ADP Security Management is best accessed using Microsoft Internet Explorer Version 8 or Mozilla Firefox Version 3.6, at minimum.

This email was sent to active users in your company that access ADP Netsecure with a security role of security master or security admin. You may have other users that also access ADP Netsecure with other security roles. Please inform those users of these enhancements, noting that the above resources will have some functionality that does not apply to their role.

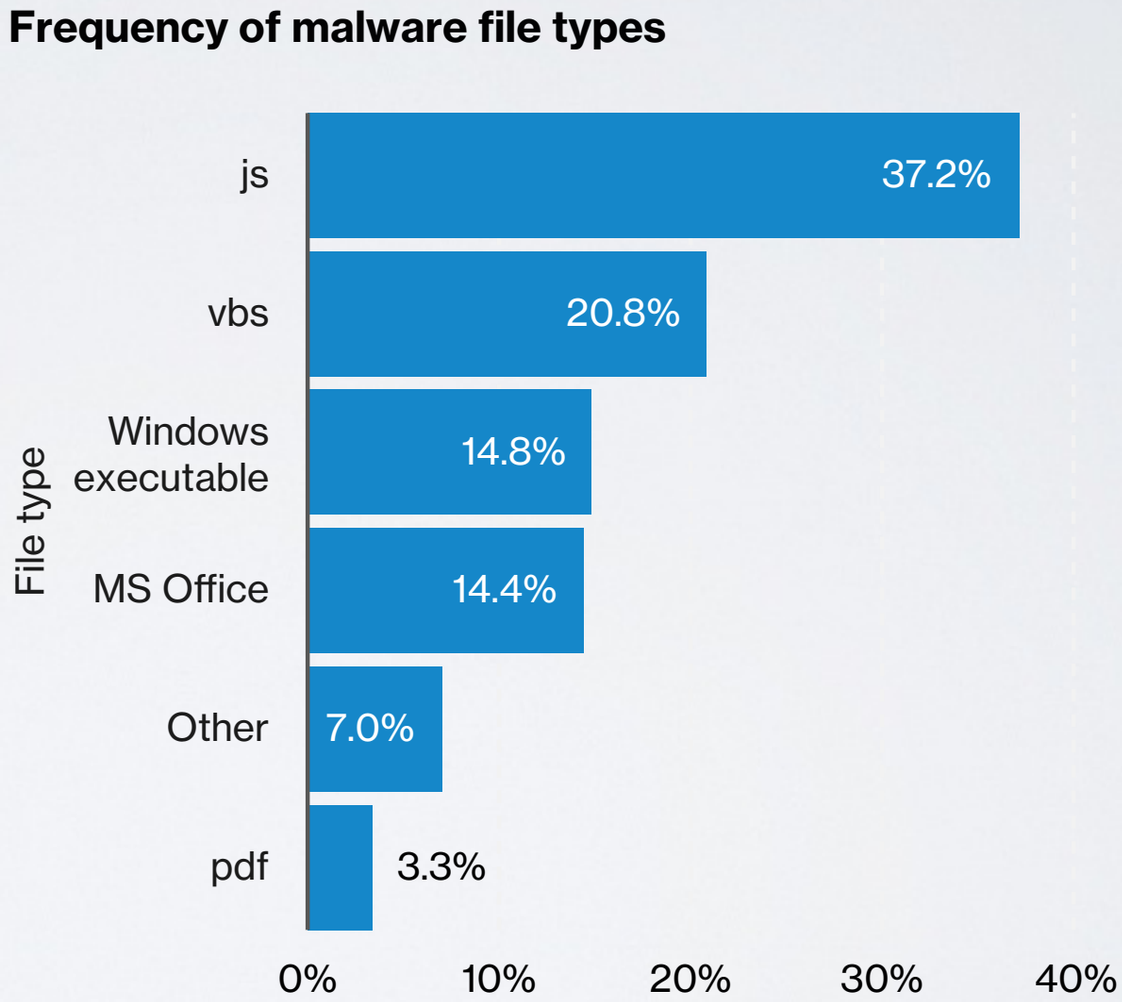
As always, thank you for choosing ADP as your business partner! If you have any questions, please contact your ADP Technical Support organization.

Ref: 0609MSAMALONIS1@TWNSHP

ANATOMY OF AN ATTACK

Delivery

- the exploit is delivered through a vector
- delivery method
- delivery vector
  - EXE
  - ZIP
  - DOC, XLS, etc.
  - PDF
  - Javascript
  - Flash
  - …



ANATOMY OF AN ATTACK

Exploit

- attack method
  - 0-day exploit
  - known software vulnerability
  - misconfiguration
  - bad user behavior

ANATOMY OF AN ATTACK

Installation

- Payload download
- Payload must be obfuscated while it trespasses boundary security
  - Secure channels
  - Code obfuscation and polymorphism
  - Encryption
  - Steganography
- Use your imagination (tweets, Facebook messages, etc.)

ANATOMY OF AN ATTACK

Callback

- After installation the payload cleans up what remains of the infiltration procedure
- It may leverage local exploit to escalate local privileges
- Detecting the intrusion from this moment may be extremely difficult
- The payload contact a C&C server to
  - receive further instructions
  - download modules
- The communication is obfuscated as well

ANATOMY OF AN ATTACK

- Example: downloader.BMP.exe
  - uses steganography to encrypt commands in a BMP file header

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	42	4D	36	2C	02	00	00	00	00	00	36	00	00	00	28	00	BM6œ 6 (
00000010	00	00	25	02	00	00	40	00	00	00	01	00	18	00	00	00	% @
00000020	00	00	00	9C	01	00	00	00	00	00	00	00	00	00	00	00	œ
00000030	00	00	00	00	00	00	F6	42	36	65	22	31	F7	73	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	01	01	01	00	00	01	01	00	01	
00000060	01	00	01	01	00	00	00	01	01	00	00	01	00	01	00	01	
00000070	01	00	00	01	00	01	00	01	01	01	00	00	00	00	00	00	
00000080	01	01	01	00	01	00	00	00	01	01	00	00	01	00	00	00	
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

ANATOMY OF AN ATTACK

- Example: TROJAN.MSIL.BERBOMTHUM.AA
  - uses steganography to hide commands in JPG images
  - pictures are distributed through social accounts (Twitter)

Commands	Description
/print	Screen capture
/processos	Retrieve list of running processes
/clip	Capture clipboard content
/username	Retrieve username from infected machine
/docs	Retrieve filenames from a predefined path such as (desktop, %AppData% etc.)

ANATOMY OF AN ATTACK

Data exfiltration

- Any information in a single PC is potentially valuable
  - Passwords
  - private encryption keys
  - Documents
  - Information about the surrounding network
- Once the malware obtained administration privileges it can do whatever you may imagine:
  - install and use further software
  - impersonate you
  - act as a proxy
  - monitor the surrounding environment with your webcam

ANATOMY OF AN ATTACK

Lateral spread

- Your PC may just be an access point to a larger network
- The attacker will take his time and explore his surrounding to infiltrate further resources
- The attacker is there to stay as long as possible

ANATOMY OF AN ATTACK

Reconnaissance → days/months

Weaponization → days/months

Delivery → minutes/hours

Exploitation → milliseconds

Persistence → years

Callback → years

Data exfiltration → years

Lateral spread → years