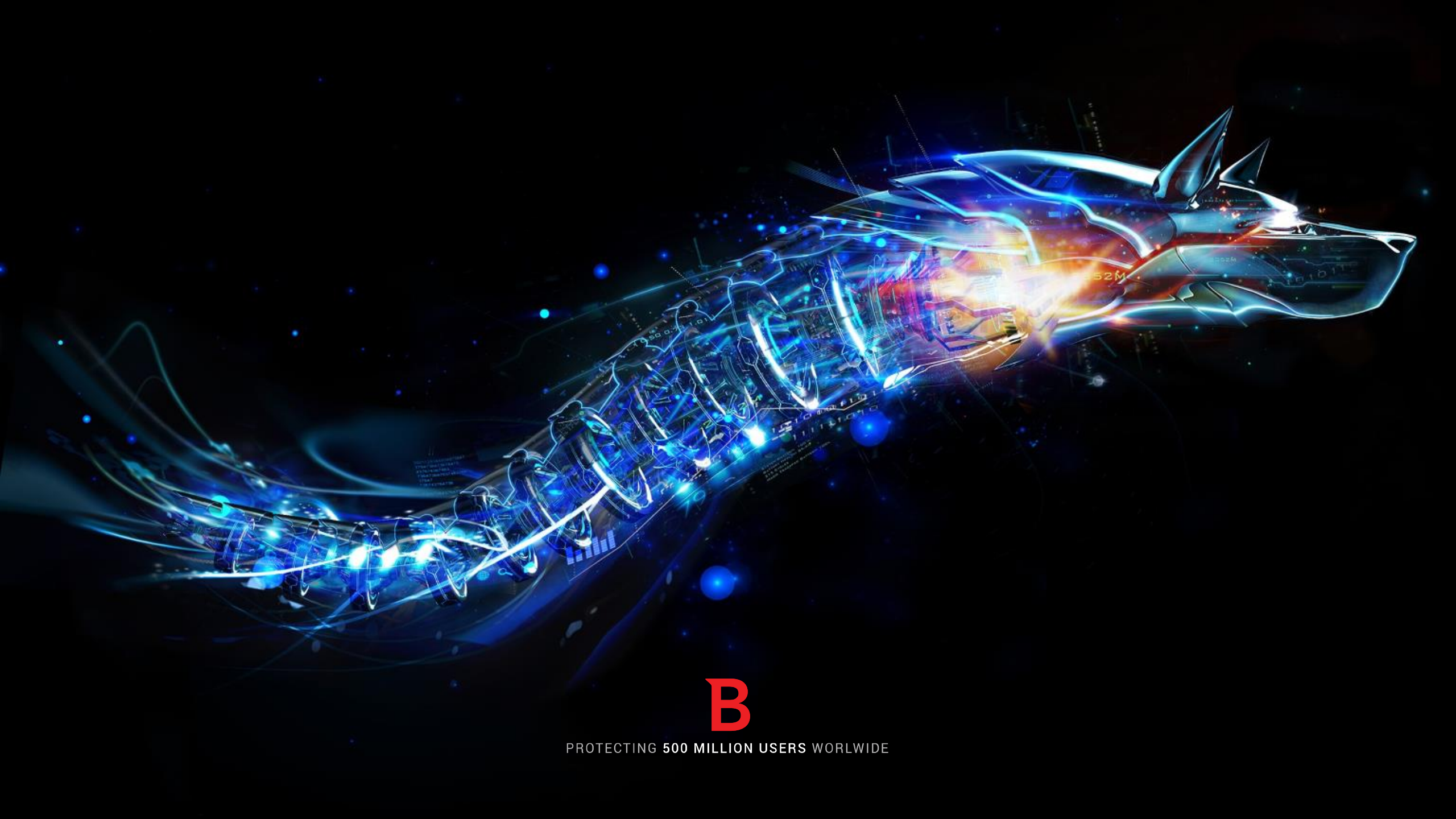

B
PROTECTING 500 MILLION USERS WORLWIDE

Bitdefender

“Unsecurity” and “Risks” in Digital Transformation

MIRCO ROHR

What is a Risk ?

The quantifiable likelihood of loss or less than expected returns.

Examples: currency risk, inflation risk,
economic risk, principal risk, country risk,
Liquidity risk, market risk, prepayment risk, credit risk
business risk, income risk.

A TERRIBLE DAY IN THE LIFE OF A CEO OR…A CIO….OR A CISO

Google

targeted attacks

Toate Imagini Știri Videoclipuri Hărți Mai multe Setări Instrumente

Aproximativ 2.570.000 (de) rezultate (0,45 secunde)

Security

Apple and MS attackers Wild Neutron return with fresh run of attacks

'Skilled and versatile' group bank around to strafe new targets

Google

advanced persistent threats

Toate Imagini Știri Videoclipuri Mai

Aproximativ 2.360.000 (de) rezultate (0,39 secunde)

Home > Security > Cybercrime & Hacking

NEWS

Target CIO resigns following breach

The retailer announces the resignation after data breaches affecting up to 110 million people

JP Morgan's CISO Greg Rattray was asked to leave his position and take up the global cyber partnerships and government strategy.

JUN 15, 2014 @ 09:00 AM 27,281 VIEWS The Little Bl

Target CEO Fired - Can You Be Fired If Your Company Is Hacked?

Eric Basu, CONTRIBUTOR

I offer insight on cyber security issues for businesses and consumers. FULL BIO

Opinions expressed by Forbes Contributors are their own.

A common perspective is that cyber security is primarily the responsibility of the IT department. If a data breach incident occurred, the senior IT executive was the only one to take the fall, and usually only if there was incompetence involved vs. simply bad luck.

MAY 8, 2014 @ 08:42 AM 6,925 VIEWS The Little Black Book

Target's CEO Steps Down Following The Massive Data Breach And Canadian Debacle

RISK ASSESSMENT —

Meet the hackers who break into Microsoft and Apple to steal insider info

Almost 50 companies have been hacked by a shadowy group.

DAN GOODIN - 7/8/2015, 4:00 PM

BAD NEWS….

Huge Financial Loss

Brand Reputation

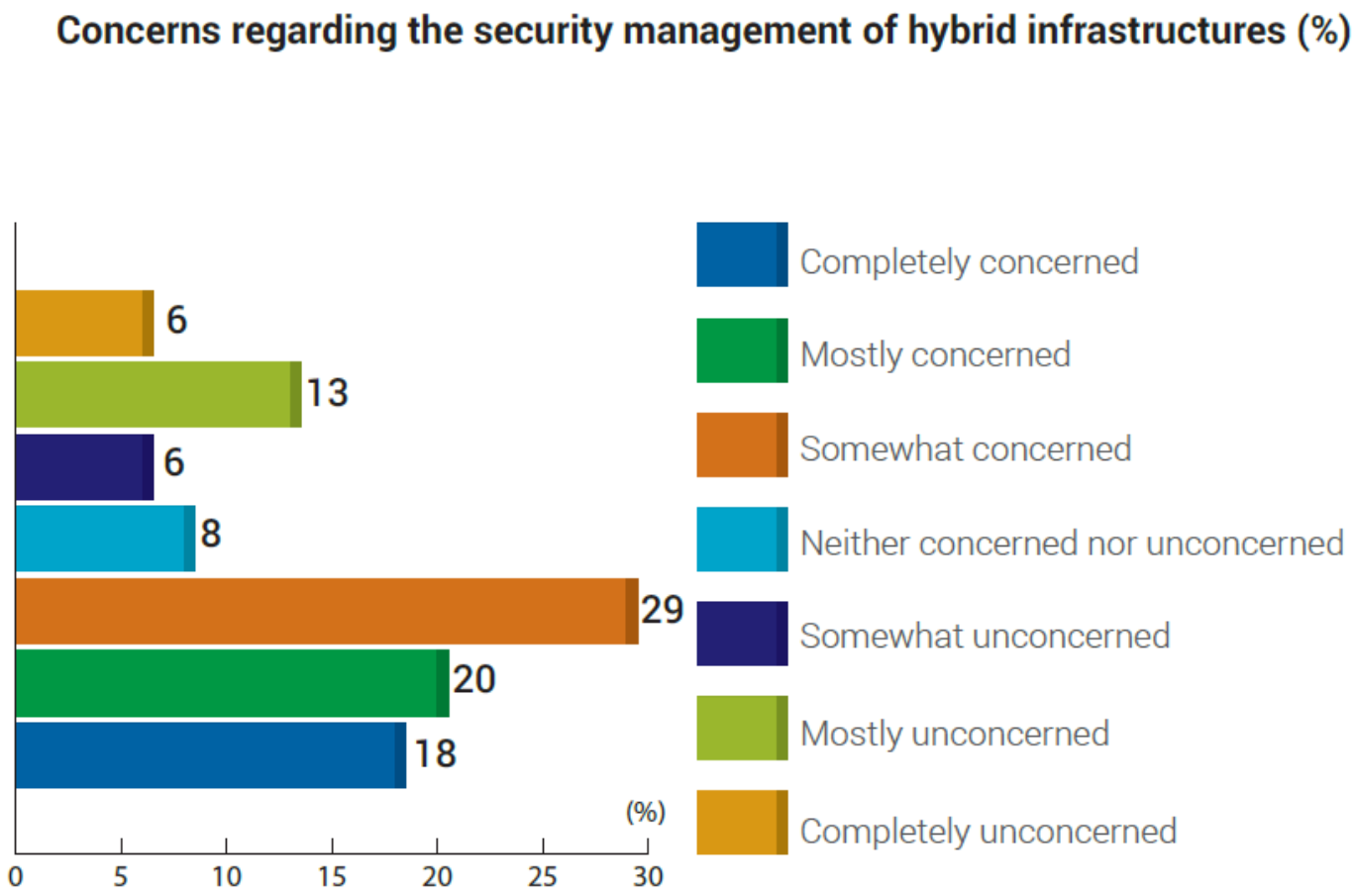
Customer Trust

Loss of Intellectual Property

Business Disruption

C level jobs at risk

HYBRID INFRASTRUCTURE - CONCERNS



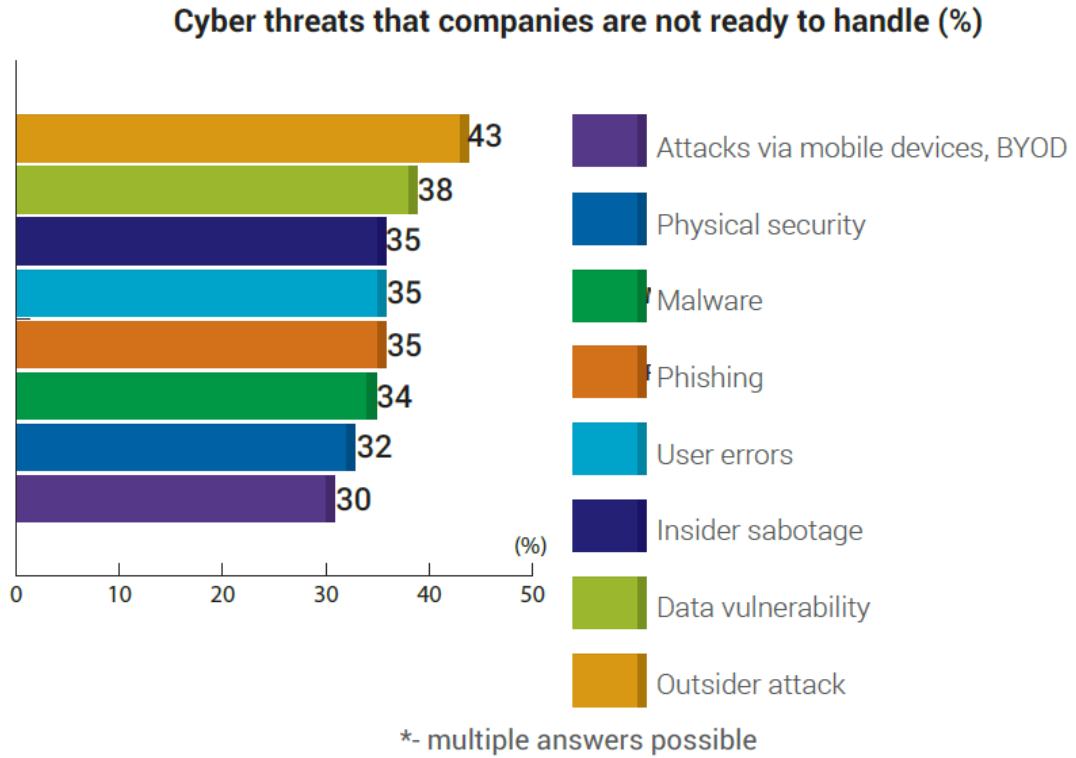
- A Bitdefender study on large companies revealed that 73% of IT decision makers fear having to pay financial compensation in case of a security breach
- while 66% even fear their own job safety.
- Moreover, seven out of 10 IT decision makers are concerned or completely concerned regarding the security management of hybrid infrastructures.

http://download.bitdefender.com/resources/files/News/CaseStudies/study/125/Bitdefender-Whitepaper-VE-A4-en-EN-web.pdf

COMPANIES ARE NOT READY TO HANDLE CYBERTHREATS

Bitdefender's survey shows companies are not prepared to handle:

outsider attack (43%),
data vulnerability (38%),
insider sabotage (35%),
user errors (35%),
and phishing (35%).



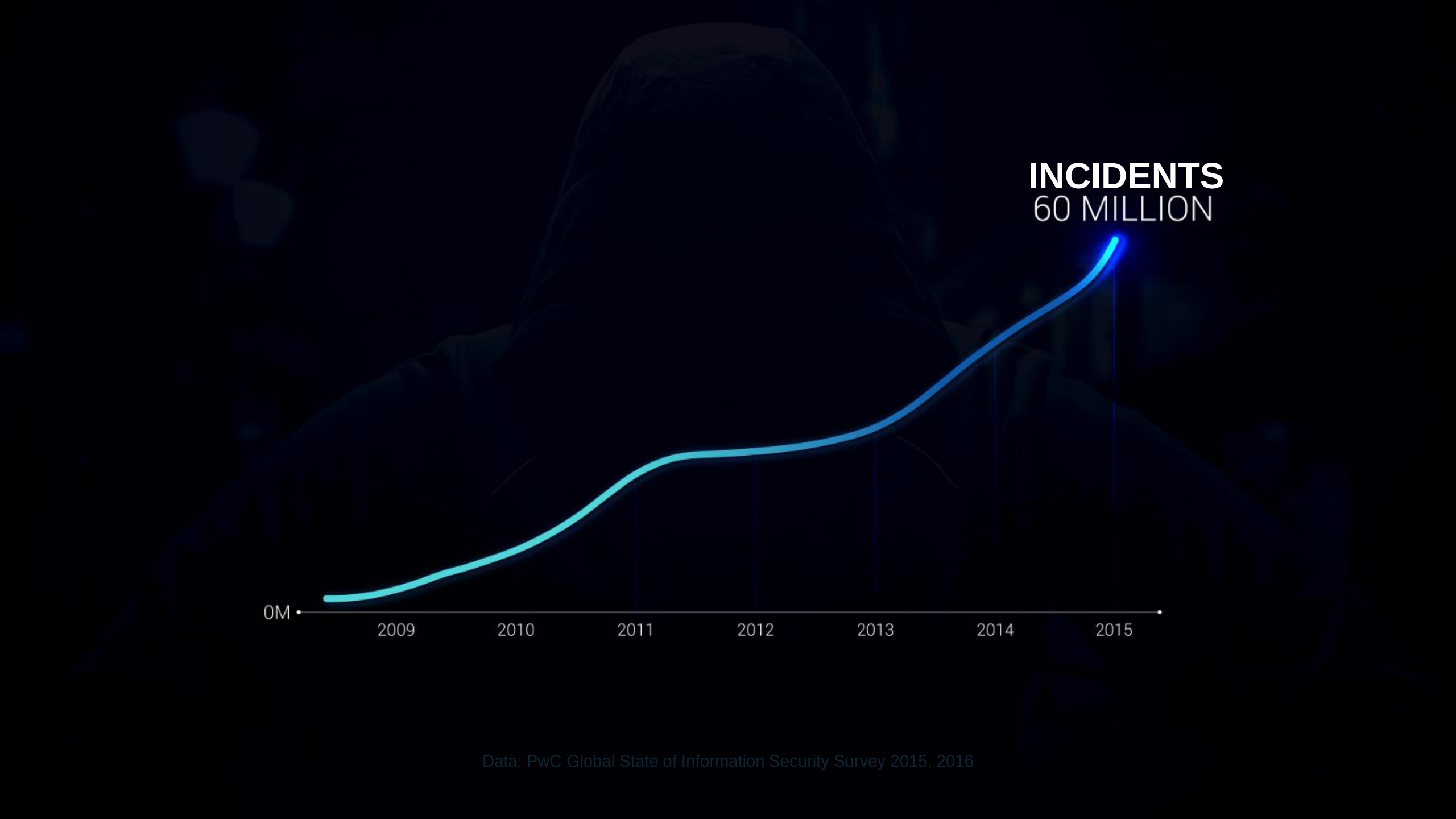
http://download.bitdefender.com/resources/files/News/CaseStudies/study/125/Bitdefender-Whit
VE-A4-en-EN-web.pdf

Outsider attacks and data vulnerability pose a significant risk for all companies and represent the main threats that companies are unprepared to handle, and CIOs are aware that cybercriminals can spend large amounts of time inside organizations without being detected - APTs are often defined as designed to evade detection.


THE WORLD OF
STEALING EVERYTHING

GREED MOTIVATES

“89% of breaches had a financial or espionage motive”

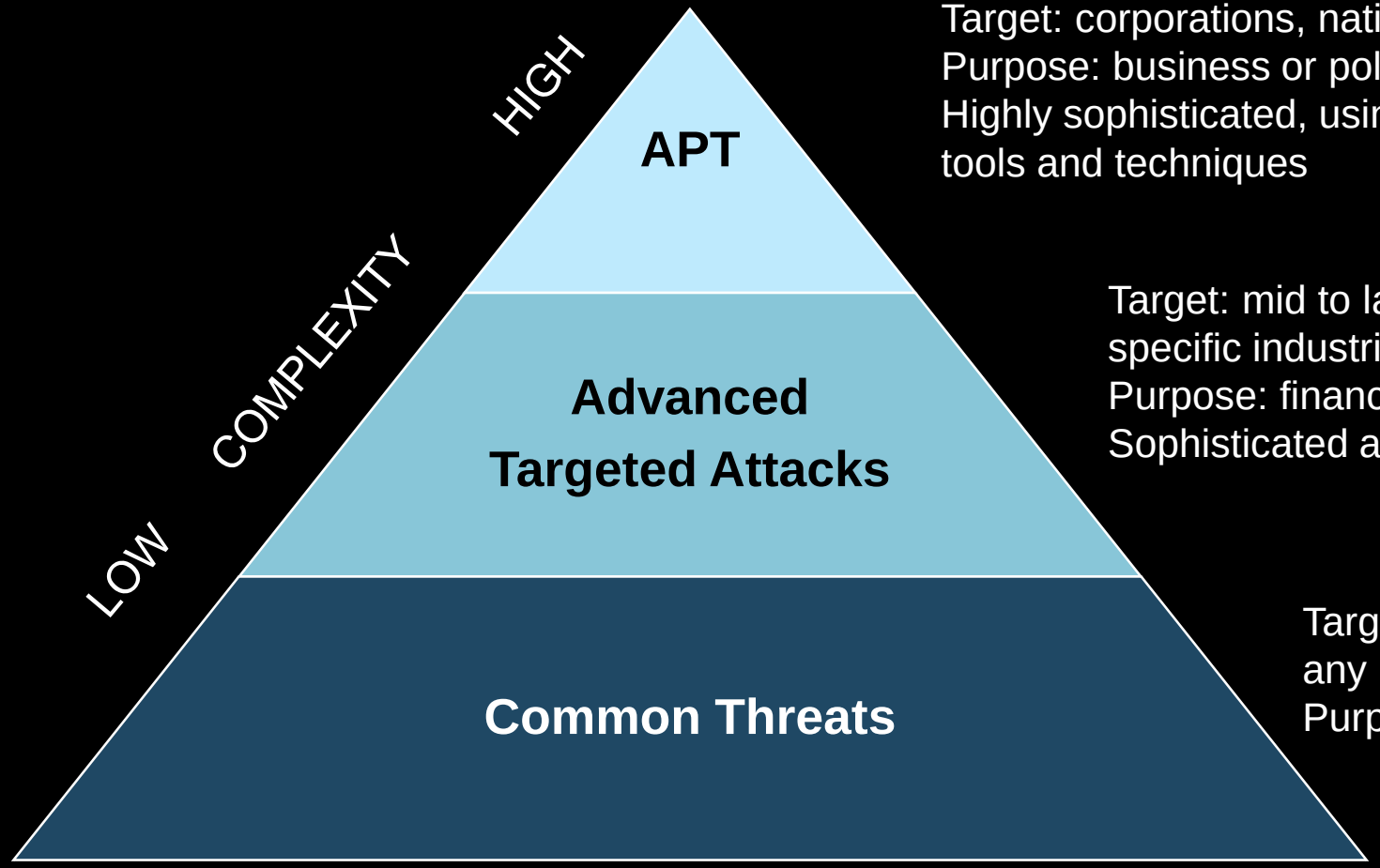


Data: PwC Global State of Information Security Survey 2015, 2016

Theft of “hard” intellectual property increased 56% in 2015

Data: PwC Global State of Information Security Survey 2015, 2016

ADVANCED PERSISTENT THREATS are highly sophisticated



Target: corporations, nations, governments
Purpose: business or political espionage
Highly sophisticated, using custom-made tools and techniques

Target: mid to large organizations, specific industries
Purpose: financial
Sophisticated attacks

Target: small organizations, any user
Purpose: financial

89% of attacks have financial or espionage motivates
(Verizon, DBIR, 2016)

5 months to discover a breach

50% of breached companies need an external forensics team

51 billion EURO damage

in German economy

350 - 575 billion Dollar world wide economical damage

In 2019 2.1 trillion $ damage

Ransomware

The concept dates back in the 80s, long before bitcoin existed

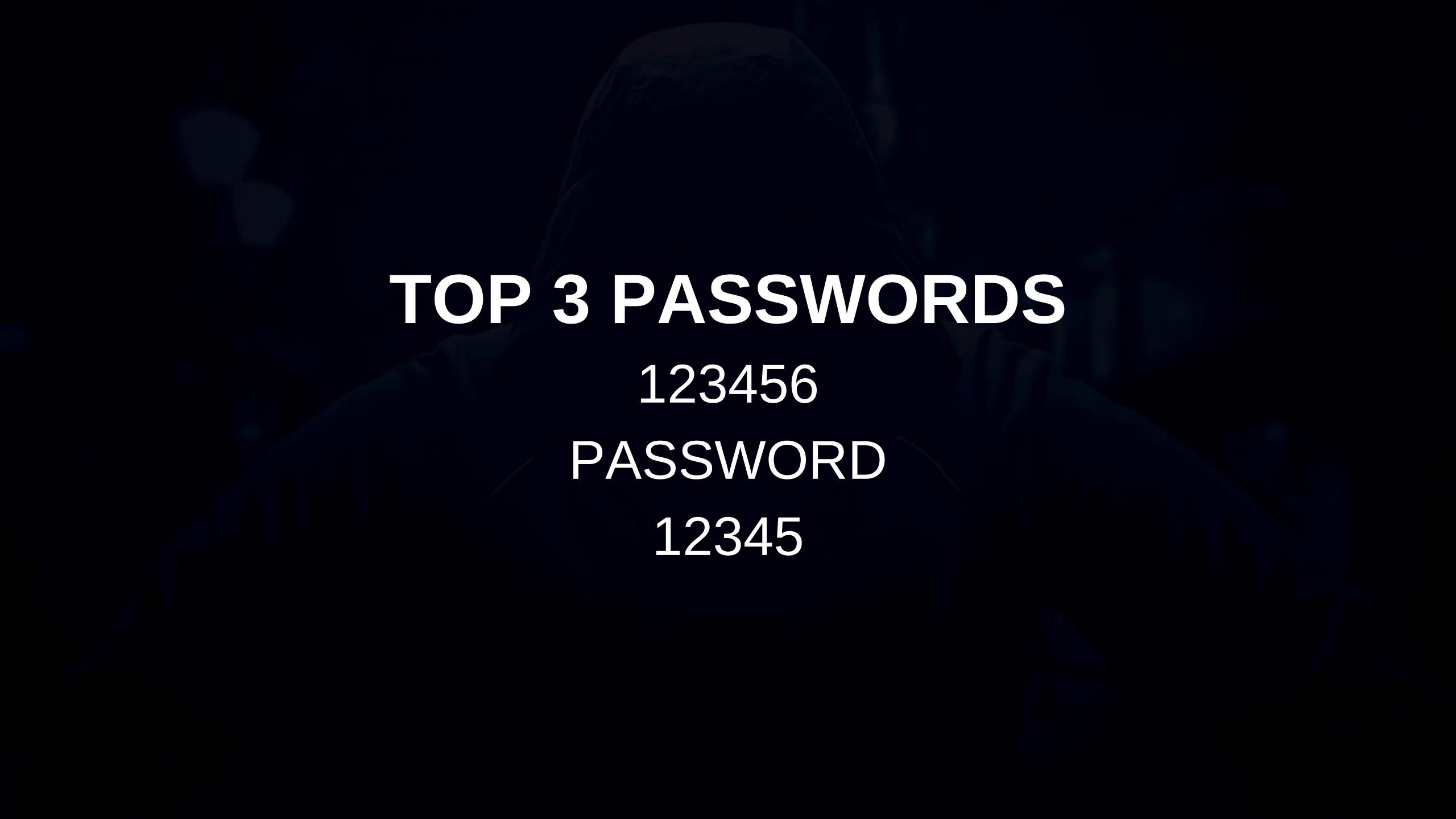
In 2014, ransomware and malvertising crossed paths and in 2015 we've seen an explosive growth

50 times more people had their devices held hostage by crypto-ransomware in 2014 compared to 2013 and even more in 2015

Investigations take time because of complexity and jurisdiction

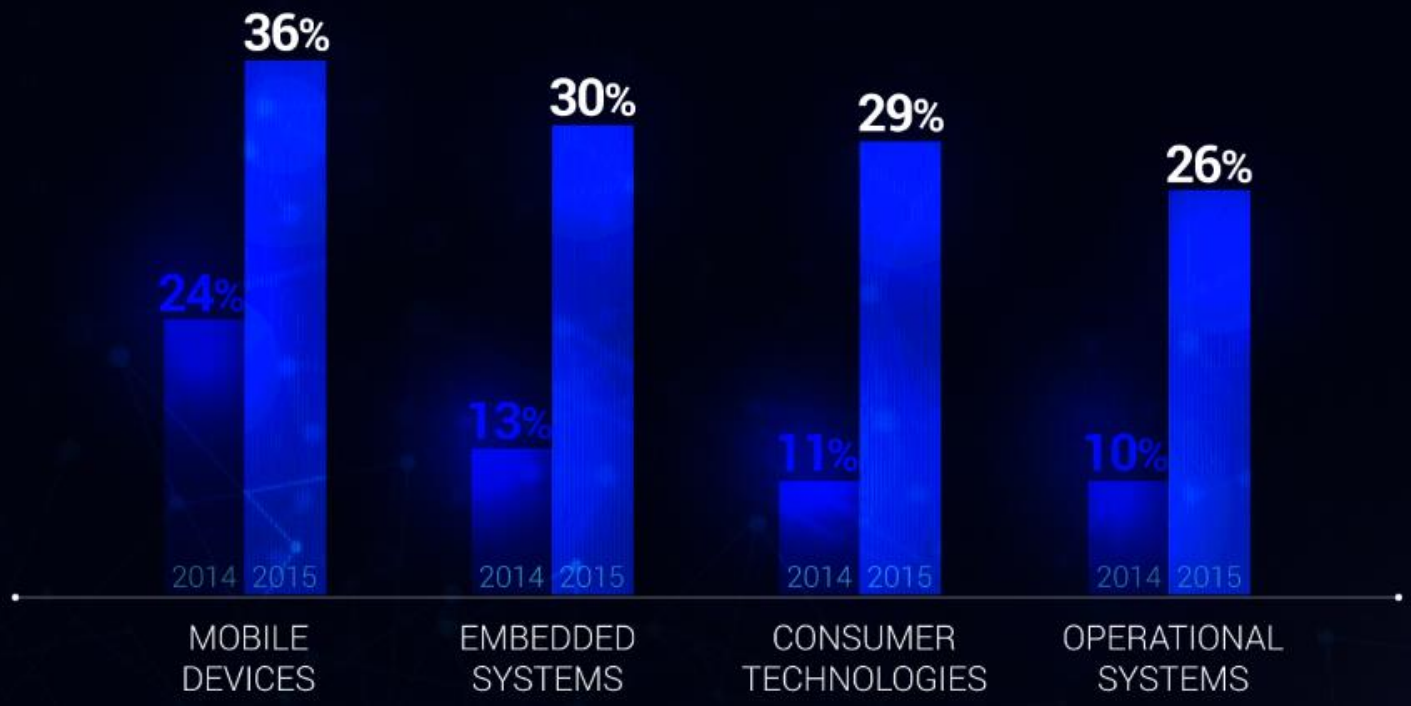
In 2015 and early 2016 we've seen ransomware migrating to Linux and Mac OS X.

Evolution of Ransomware

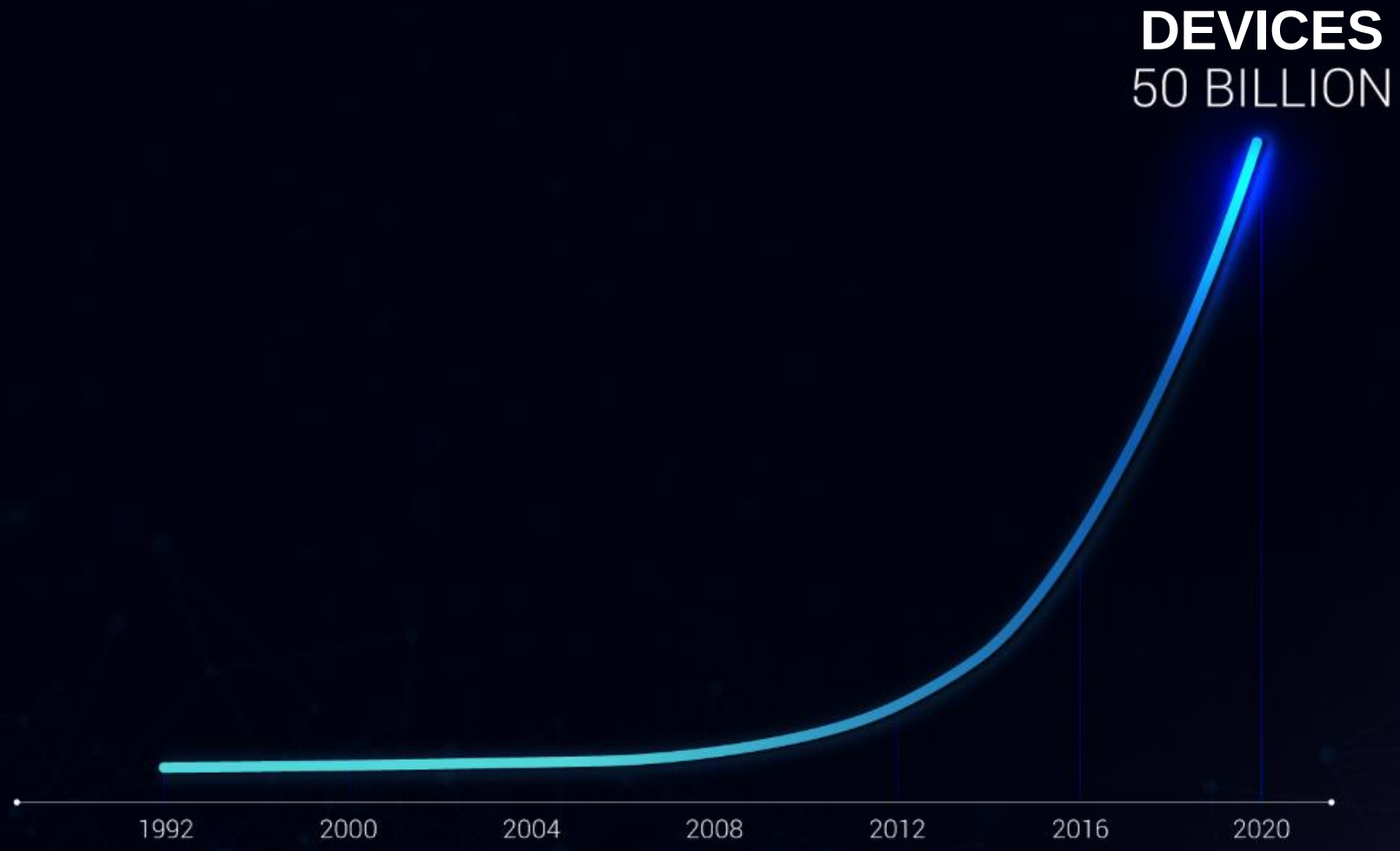

TOP 3 PASSWORDS
123456
PASSWORD
12345


INTERNET OF THINGS
CONNECTING EVERYTHING

ATTACKS ON IOT DEVICES



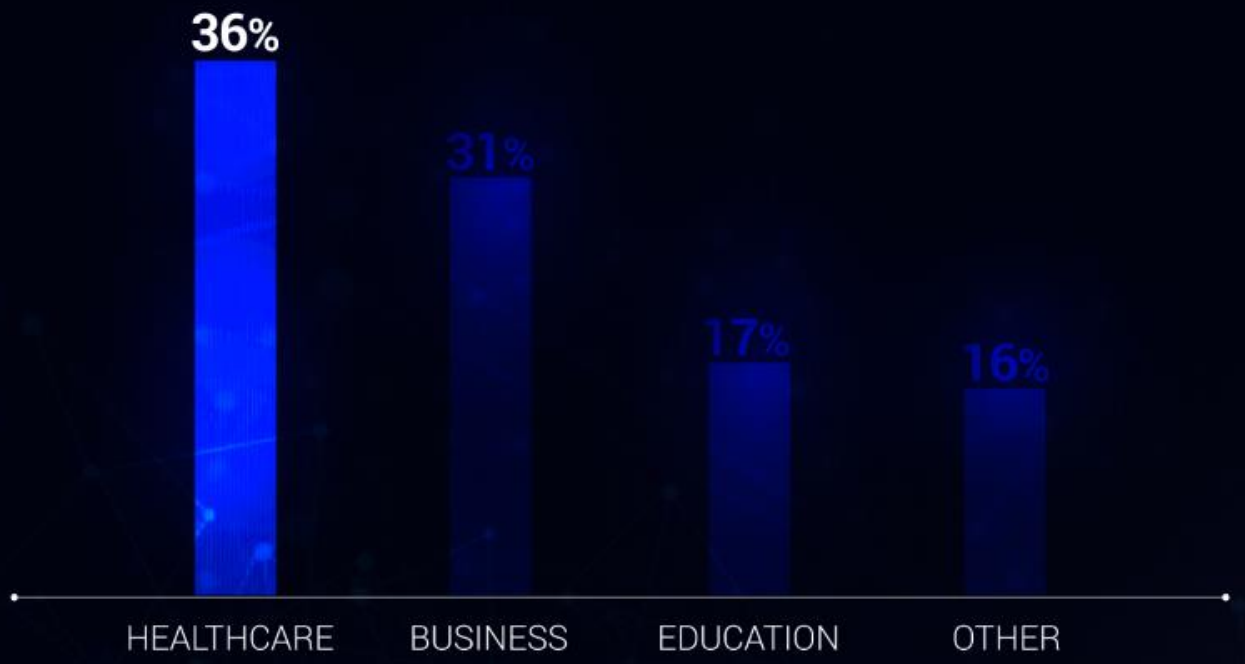
Data: PwC Global State of Information Security Survey 2015, 2016


DEVICES
50 BILLION
1992
2000
2004
2008
2012
2016
2020

Exploits & vulnerabilities

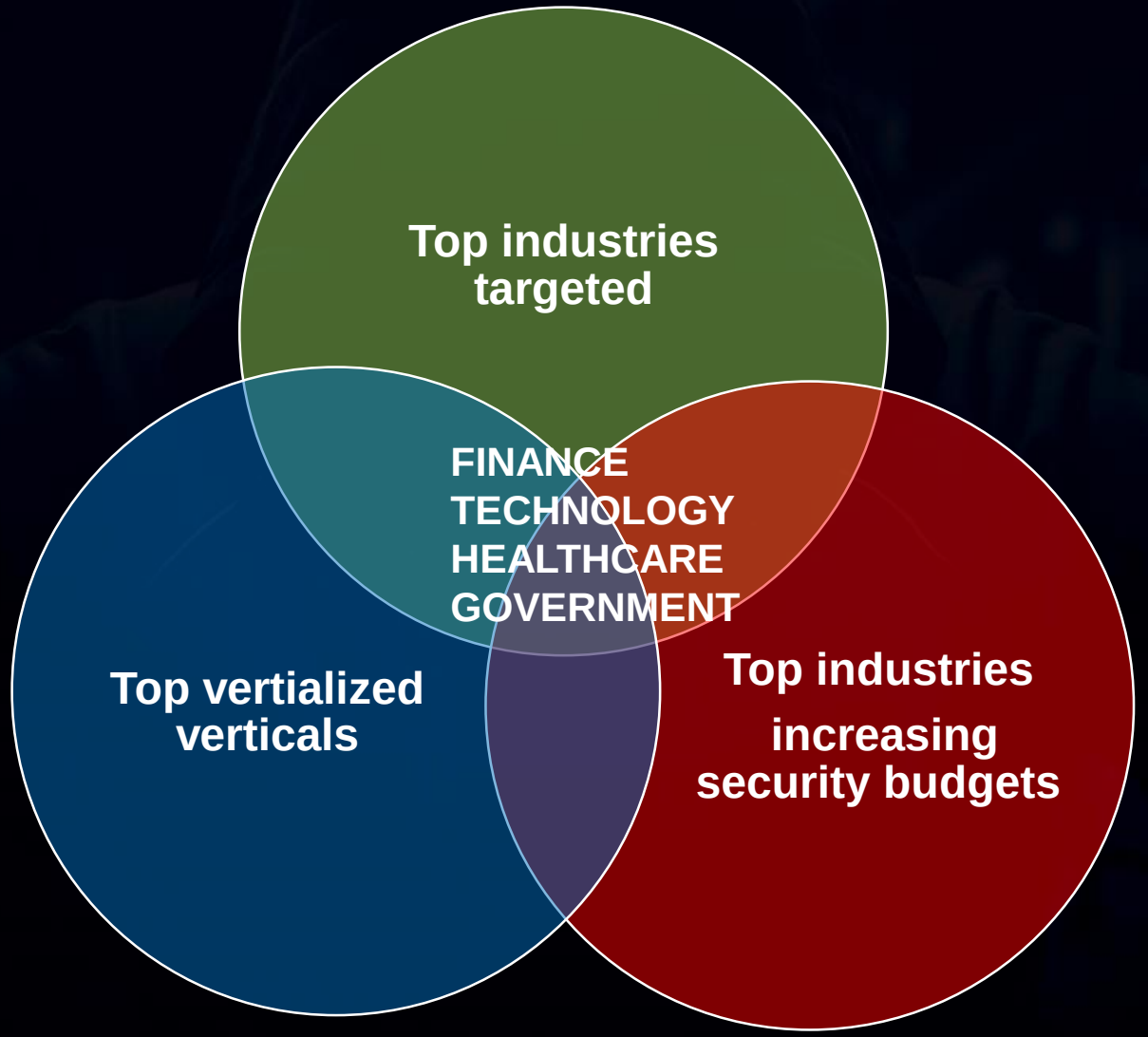
- RootPipe, HeartBleed, ShellShock, Poodle
- Within hours after HeartBleed became public knowledge, attackers started to exploit it
- HeartBleed got its own logo!
- Shellcode affects Windows, Linux and OSX
- Big news because they compromised servers instead of endpoints
- Almost 10% increase in the number of browser vulnerabilities, with IE on the first place and Google Chrome on the second.
- 84% mobile vulnerabilities were related to iOS in 2015, compared to 11% for Android and 4% for BlackBerry

HEALTHCARE IN FOCUS



Data: Identity Theft Resource Center, Data Breach Category Summary 2016

TARGET VERTICALS



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160908-03	U.S. Customs and Border Protection	DC	9/6/2016	Electronic	Government/Military	Yes - Published #	5,000

Customs and Border Protection released the personally identifiable information, including Social Security numbers, of thousands of individuals to dozens of federal agencies during an investigation of cheating on polygraph tests. CBP violated some aspects of the Privacy Act in distributing the information across government, the Homeland Security Department's inspector general found in its report. The agency collected and distributed information such as Social Security numbers, email and mailing addresses, and phone numbers of individuals who had purchased materials from two individuals who helped job applicants pass polygraphs.

Attribution 1

Publication: Government Executive Author:
Article Title: DHS Exposes Thousands of Individuals' Private Information -- Including Feds, Golfers and Priests
Article URL: http://www.govexec.com/oversight/2016/09/dhs-exposes-thousands-individuals-private-information-including-feds-gol

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160907-06	Vulcan Industries	AL	8/31/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently became aware of a malware intrusion affecting our Siegel Display Products e-commerce platform by targeting customers' payment card information. Promptly after discovering the intrusion, we contained it and conducted an in-depth investigation, engaging outside cybersecurity experts to determine the facts. We estimate that the malware operated between July 3 and July 22, 2016. Based on our investigation, we believe this unauthorized person may have accessed documents or records containing your name, billing address, email address and credit card number (including CCV number).

Attribution 1

Publication: VT AG's office Author:
Article Title: Vulcan Industries
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Vulcan%20Industriues%20SBN%20to%20Consumers.p

TARGETED ATTACKS

CARBANAK

- $1 BN from over 100 financial institutions
- Roughly between $2.5 mil – $10 mil per bank
- 2 years / 30 countries. Feb 2015 still active

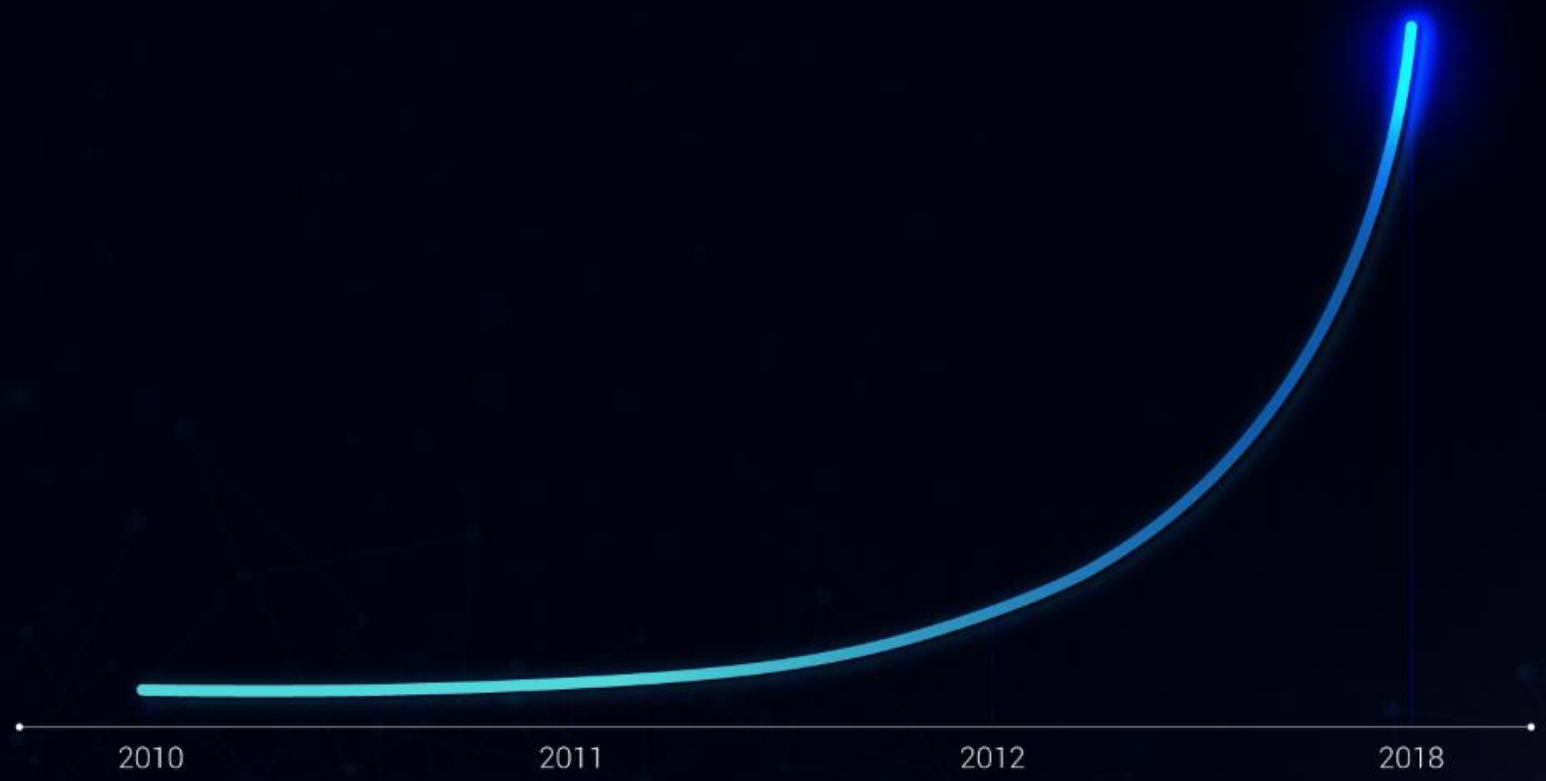
TARGETED ATTACKS

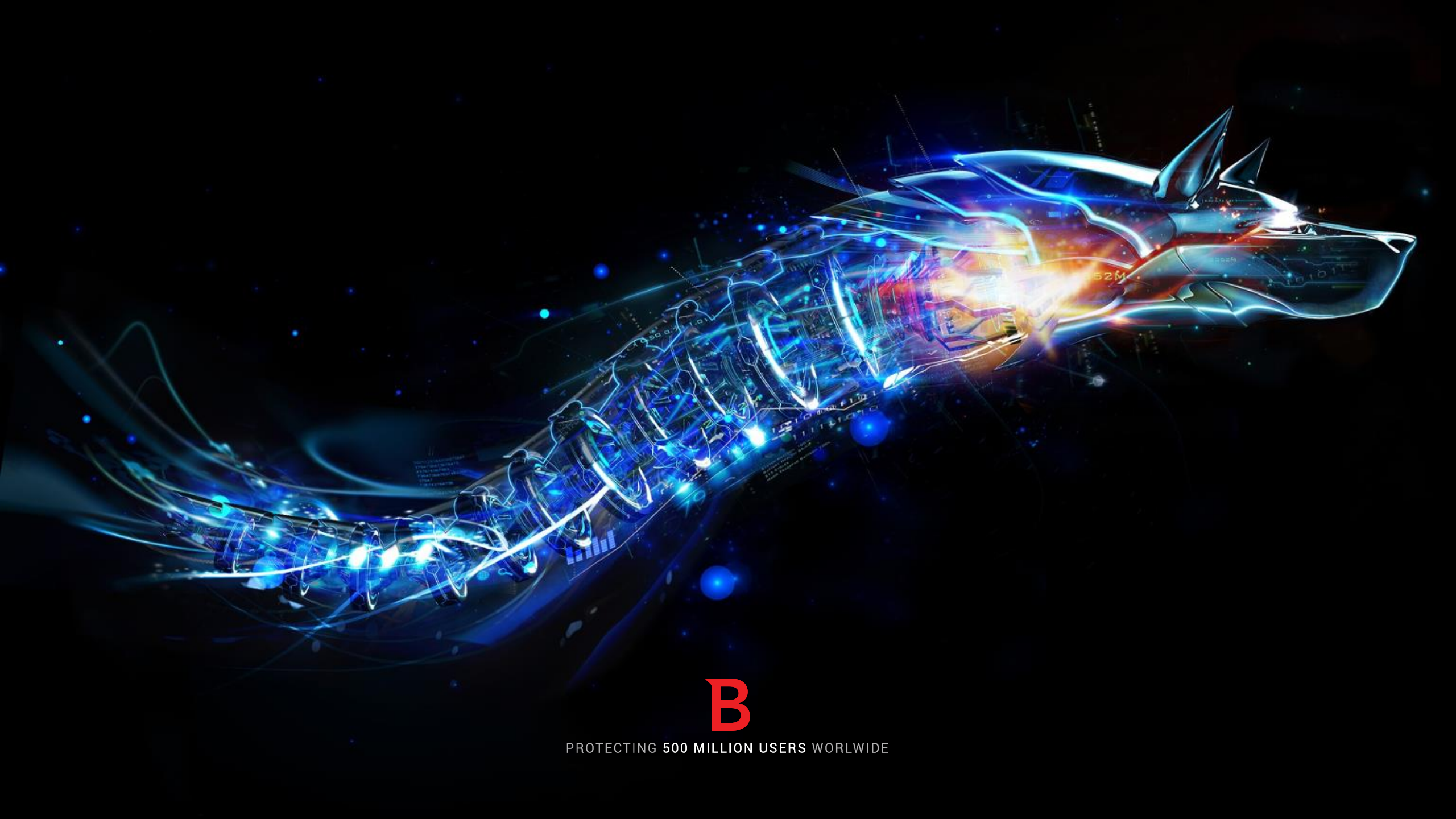
Wild Neutron

- cyber-espionage
- Apple, Microsoft, Facebook and Twitter among victims
- 11 countries and territories
- The latest round of attacks in 2015 uses a stolen certificate belonging to Acer and an unknown Flash Player exploit

MOBILE MALWARE

+250K




B
PROTECTING 500 MILLION USERS WORLWIDE