CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

SAÂD KADHI, HEAD OF CERT-EU

HACK.LU 2019 / 2019-10-23

PUBLIC / TLP:WHITE

DISTURBANCE

THE SORRY STATE OF CYBERSECURITY AND WHAT WE CAN DO ABOUT IT

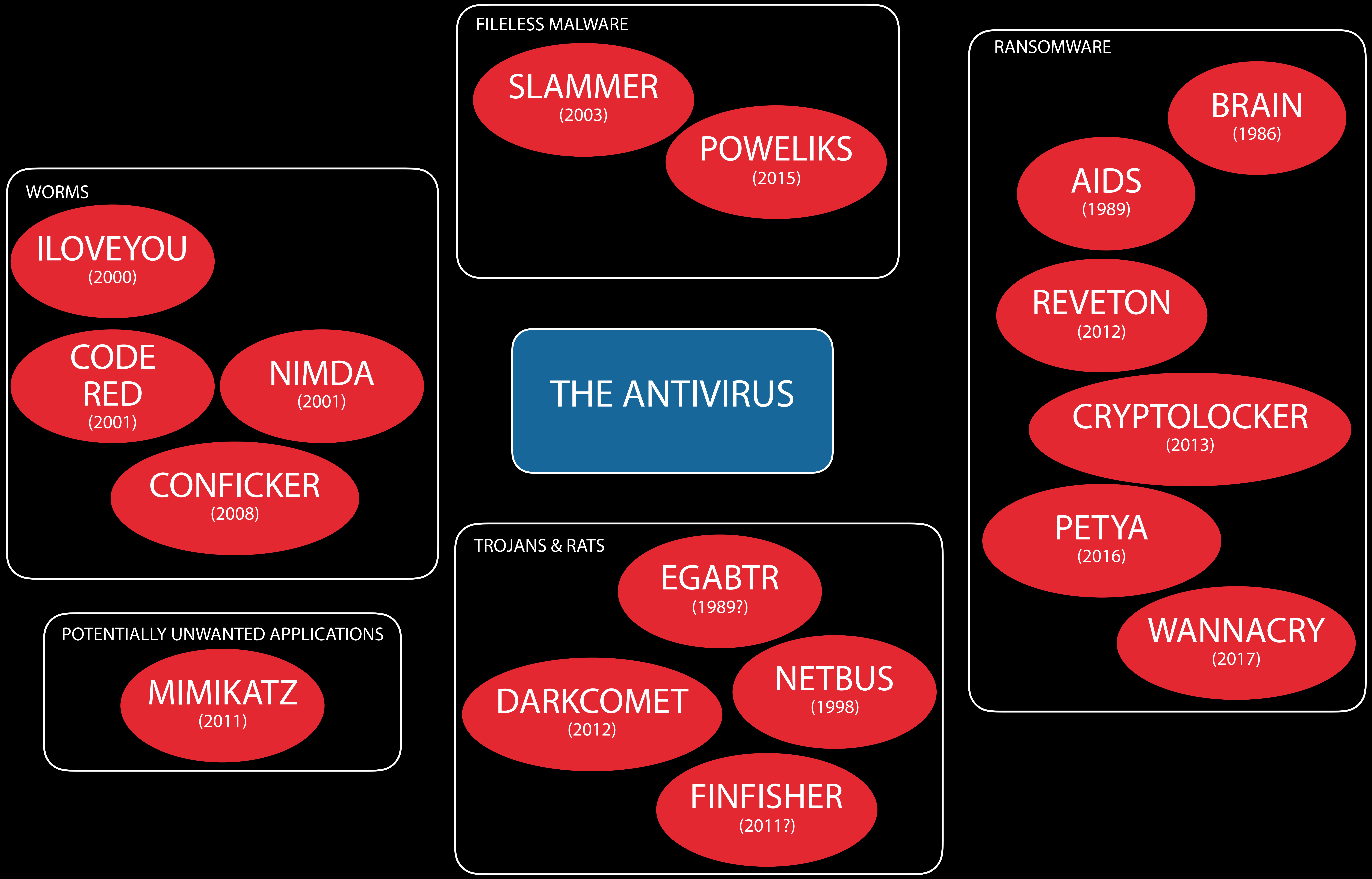
v1

IN THE BEGINNING

IN THE BEGINNING, A CYBERSECURITY PRODUCT WAS BORN

THE ANTIVIRUS

IN THE BEGINNING, IT PROTECTED US (TO SOME EXTENT)



WORMS

- ILOVEYOU (2000)
- CODE RED (2001)
- NIMDA (2001)
- CONFICKER (2008)

POTENTIALLY UNWANTED APPLICATIONS

- MIMIKATZ (2011)

FILELESS MALWARE

- SLAMMER (2003)
- POWELIKS (2015)

THE ANTIVIRUS

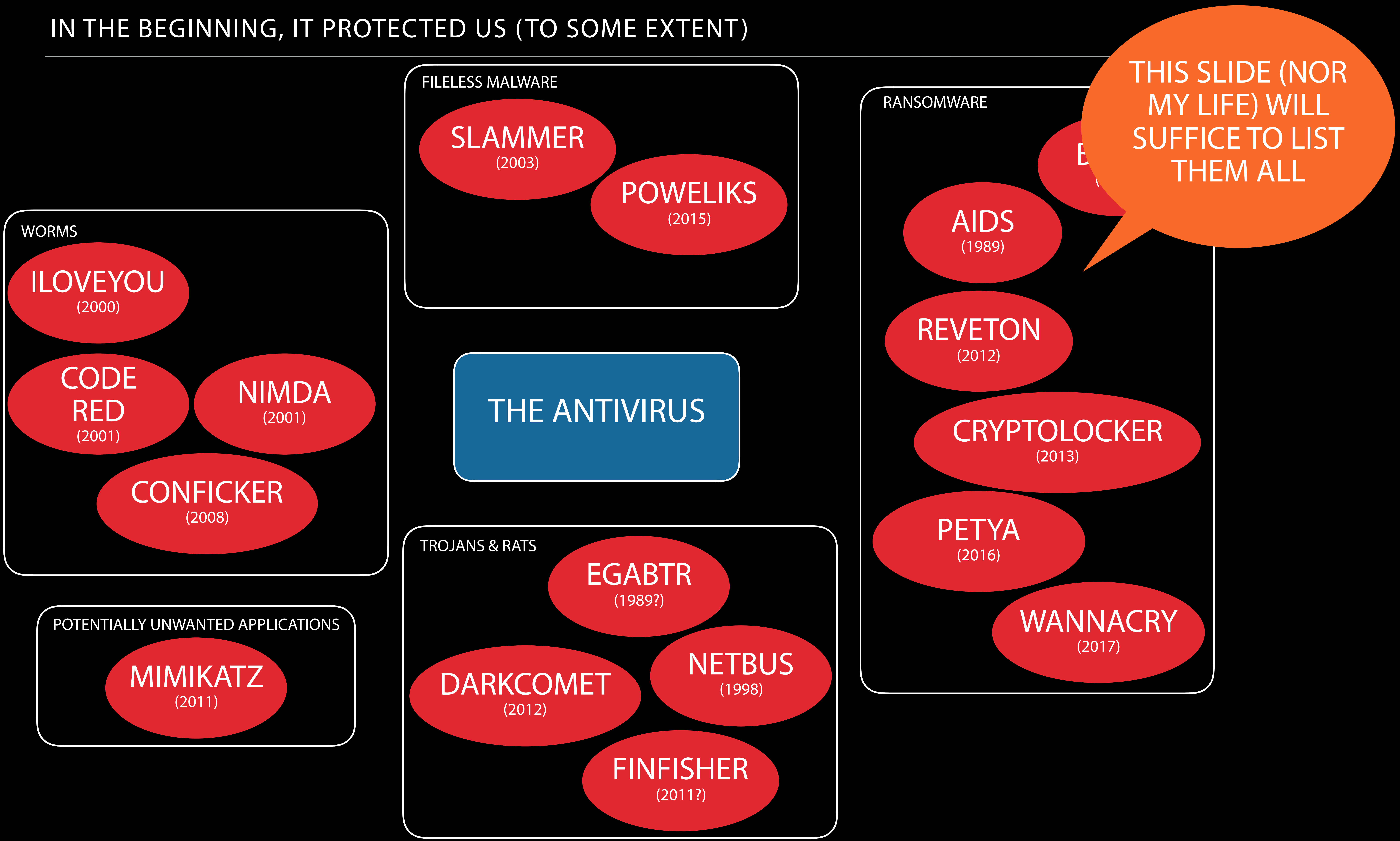
TROJANS & RATS

- EGABTR (1989?)
- DARKCOMET (2012)
- NETBUS (1998)
- FINFISHER (2011?)

RANSOMWARE

- BRAIN (1986)
- AIDS (1989)
- REVETON (2012)
- CRYPTOLOCKER (2013)
- PETYA (2016)
- WANNACRY (2017)

IN THE BEGINNING, IT PROTECTED US (TO SOME EXTENT)



FILELESS MALWARE

SLAMMER (2003)

POWELIKS (2015)

WORMS

ILOVEYOU (2000)

CODE RED (2001)

NIMDA (2001)

CONFICKER (2008)

THE ANTIVIRUS

RANSOMWARE

AIDS (1989)

REVETON (2012)

CRYPTOLOCKER (2013)

PETYA (2016)

WANNACRY (2017)

THIS SLIDE (NOR MY LIFE) WILL SUFFICE TO LIST THEM ALL

POTENTIALLY UNWANTED APPLICATIONS

MIMIKATZ (2011)

TROJANS & RATS

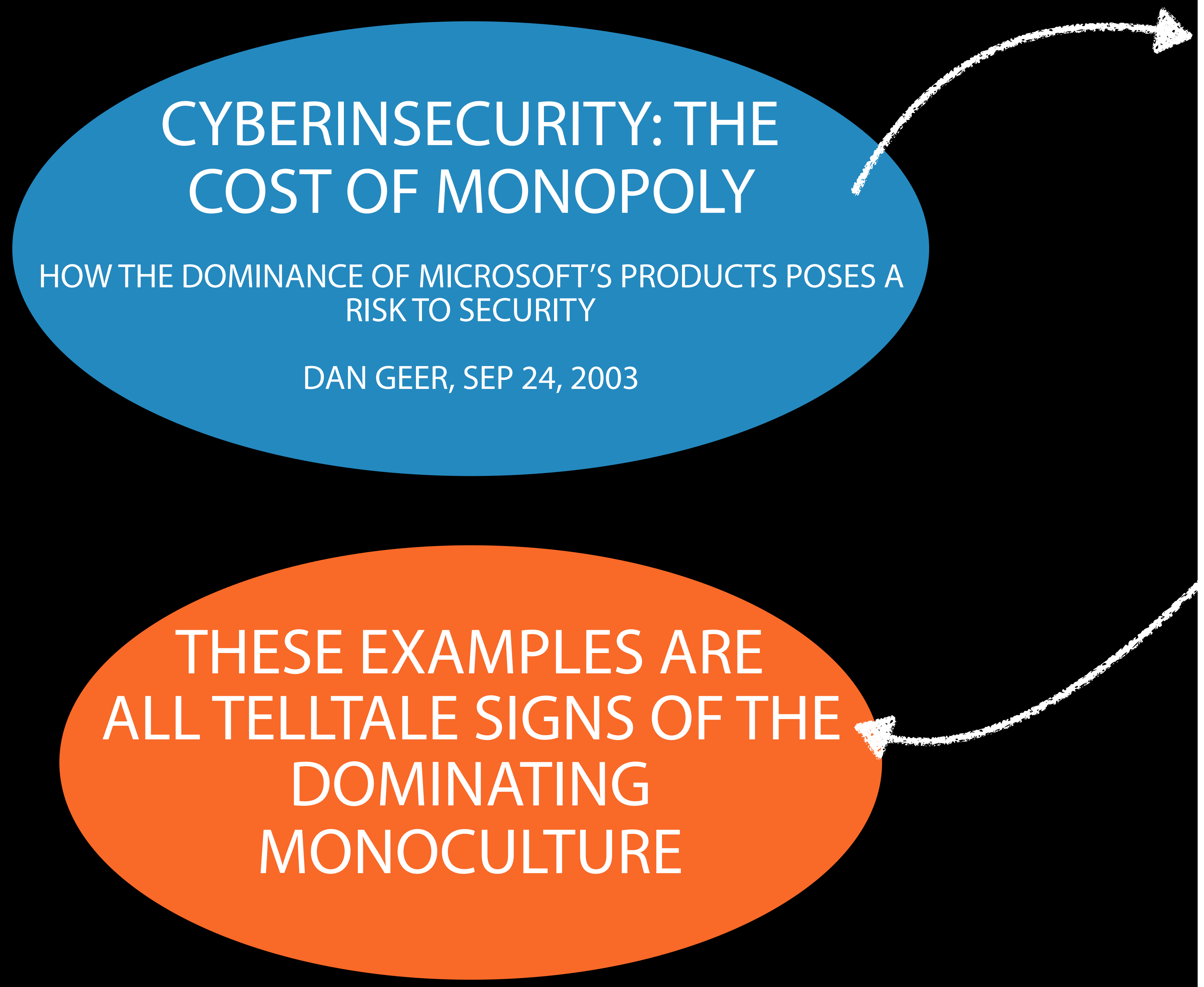
EGABTR (1989?)

DARKCOMET (2012)

NETBUS (1998)

FINFISHER (2011?)

HOW WE ENDED UP HERE?



CYBERINSECURITY: THE COST OF MONOPOLY

HOW THE DOMINANCE OF MICROSOFT'S PRODUCTS POSES A RISK TO SECURITY

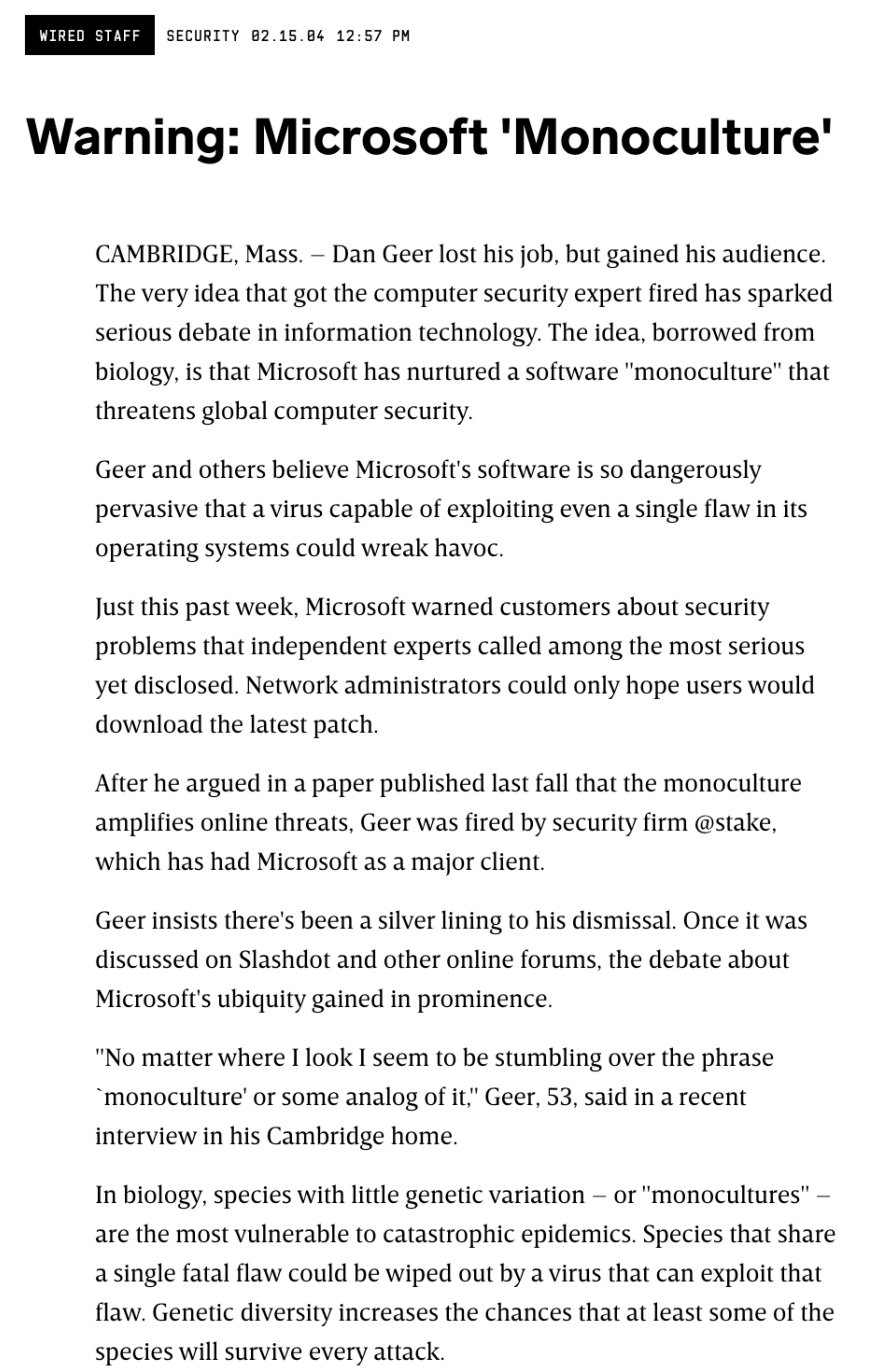
DAN GEER, SEP 24, 2003

THESE EXAMPLES ARE ALL TELLTALE SIGNS OF THE DOMINATING MONOCULTURE

BUT… A MONOCULTURE HAS ADVANTAGES

(AND THE SECURITY OF MS PRODUCTS HAS SIGNIFICANTLY AND STEADILY IMPROVED)

HOWEVER, CLASS BREAKS ARE TOO COSTLY TO IGNORE



WIRED STAFF SECURITY 02.15.04 12:57 PM

Warning: Microsoft 'Monoculture'

CAMBRIDGE, Mass. – Dan Geer lost his job, but gained his audience. The very idea that got the computer security expert fired has sparked serious debate in information technology. The idea, borrowed from biology, is that Microsoft has nurtured a software "monoculture" that threatens global computer security.

Geer and others believe Microsoft's software is so dangerously pervasive that a virus capable of exploiting even a single flaw in its operating systems could wreak havoc.

Just this past week, Microsoft warned customers about security problems that independent experts called among the most serious yet disclosed. Network administrators could only hope users would download the latest patch.

After he argued in a paper published last fall that the monoculture amplifies online threats, Geer was fired by security firm @stake, which has had Microsoft as a major client.

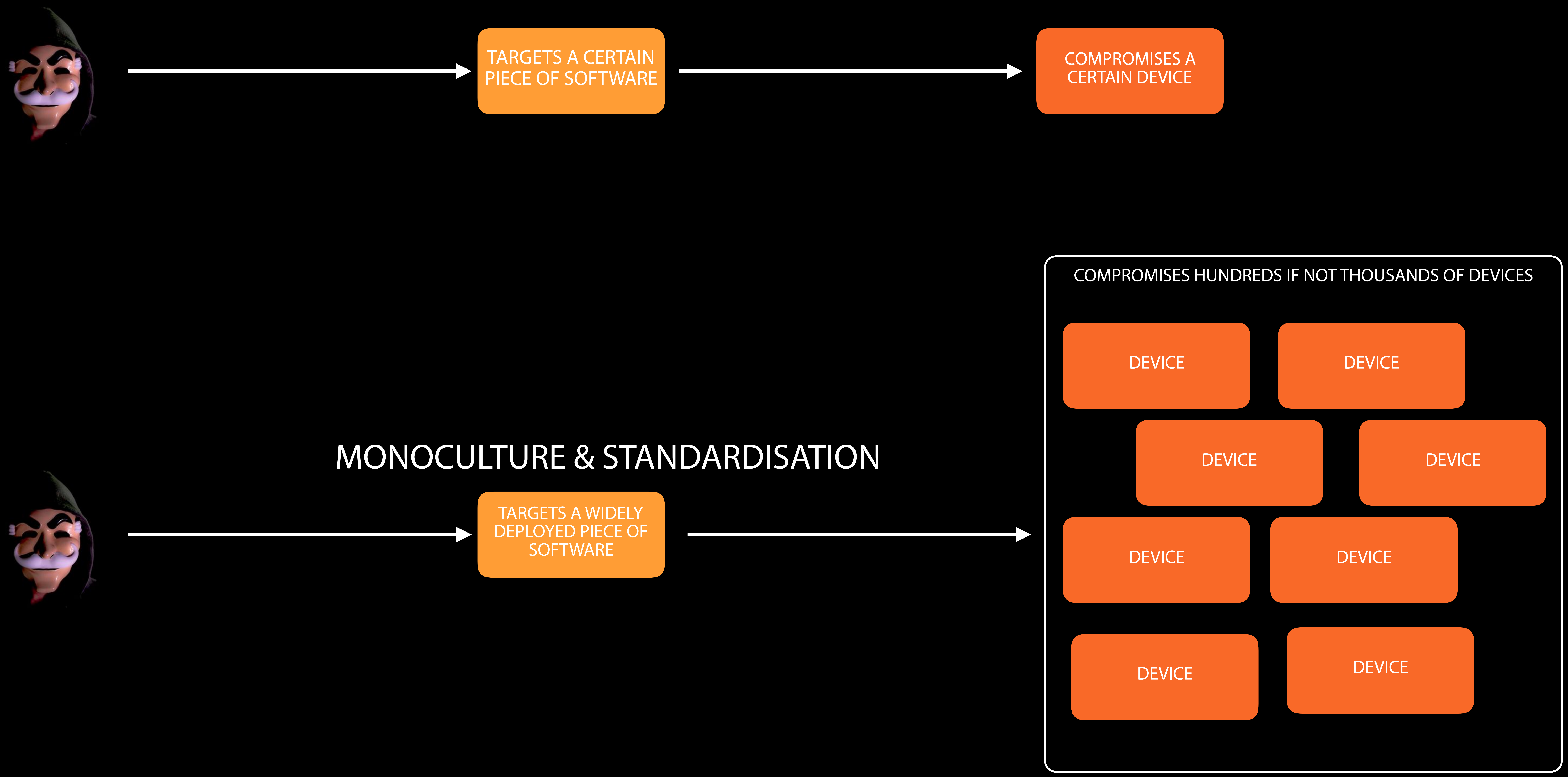
Geer insists there's been a silver lining to his dismissal. Once it was discussed on Slashdot and other online forums, the debate about Microsoft's ubiquity gained in prominence.

"No matter where I look I seem to be stumbling over the phrase `monoculture' or some analog of it," Geer, 53, said in a recent interview in his Cambridge home.

In biology, species with little genetic variation – or "monocultures" – are the most vulnerable to catastrophic epidemics. Species that share a single fatal flaw could be wiped out by a virus that can exploit that flaw. Genetic diversity increases the chances that at least some of the species will survive every attack.

Source: Wired

CLASS BREAKS 101



TARGETS A CERTAIN PIECE OF SOFTWARE

COMPROMISES A CERTAIN DEVICE

MONOCULTURE & STANDARDISATION

TARGETS A WIDELY DEPLOYED PIECE OF SOFTWARE

COMPROMISES HUNDREDS IF NOT THOUSANDS OF DEVICES

DEVICE

DEVICE

DEVICE

DEVICE

DEVICE

DEVICE

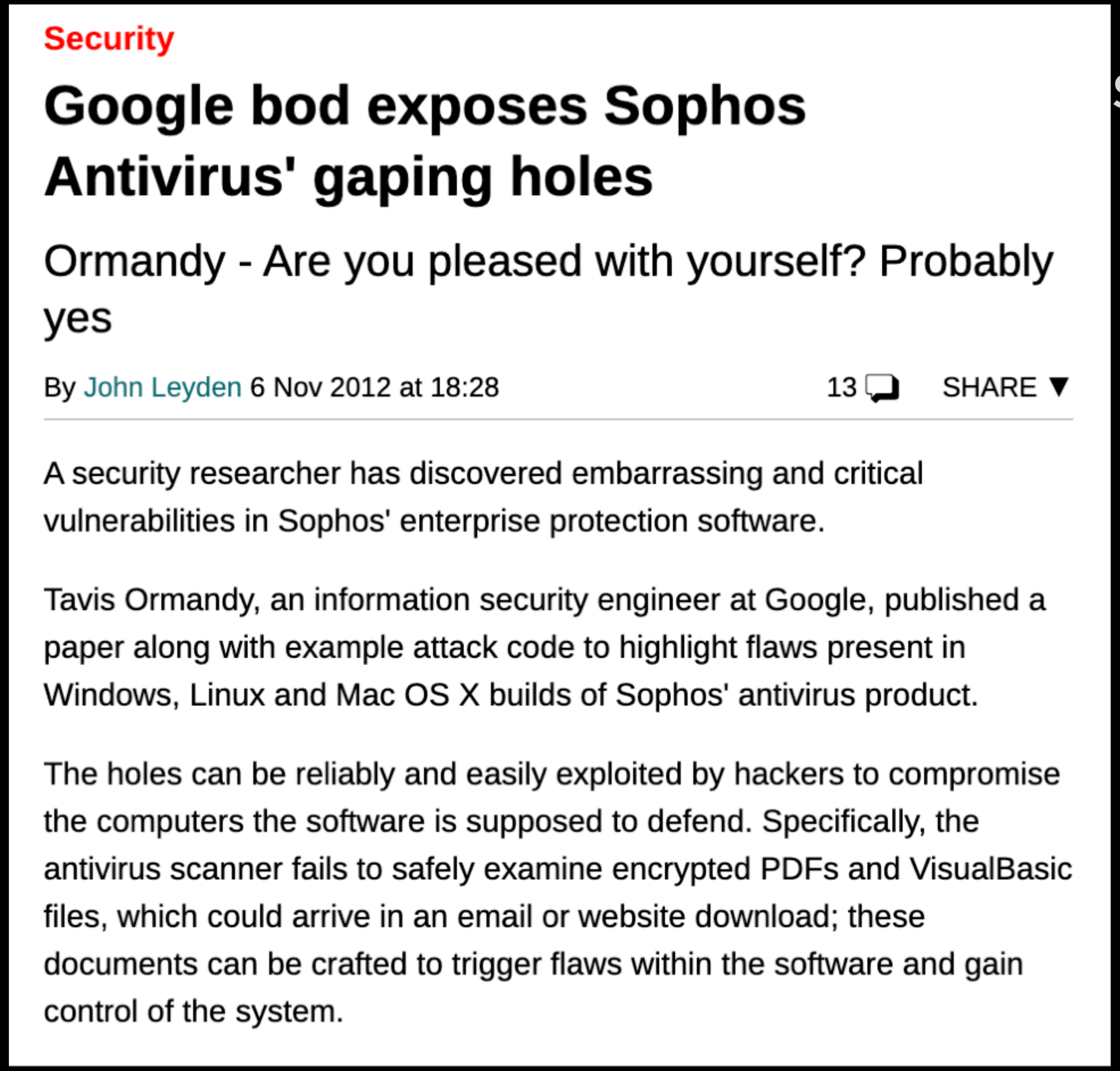
DEVICE

DEVICE

CLASS BREAKS: EXAMPLES

SYMANTEC ENDPOINT PROTECTION
(2016)

2012-2018: GOOGLE'S PROJECT ZERO FOUND SEVERAL HIGHLY CRITICAL VULNERABILITIES IN MANY OTHER AV PRODUCTS
(KASPERSKY, ESET, COMODO, TRENDMICRO, SOPHOS…)



Security

Google bod exposes Sophos Antivirus' gaping holes

Ormandy - Are you pleased with yourself? Probably yes

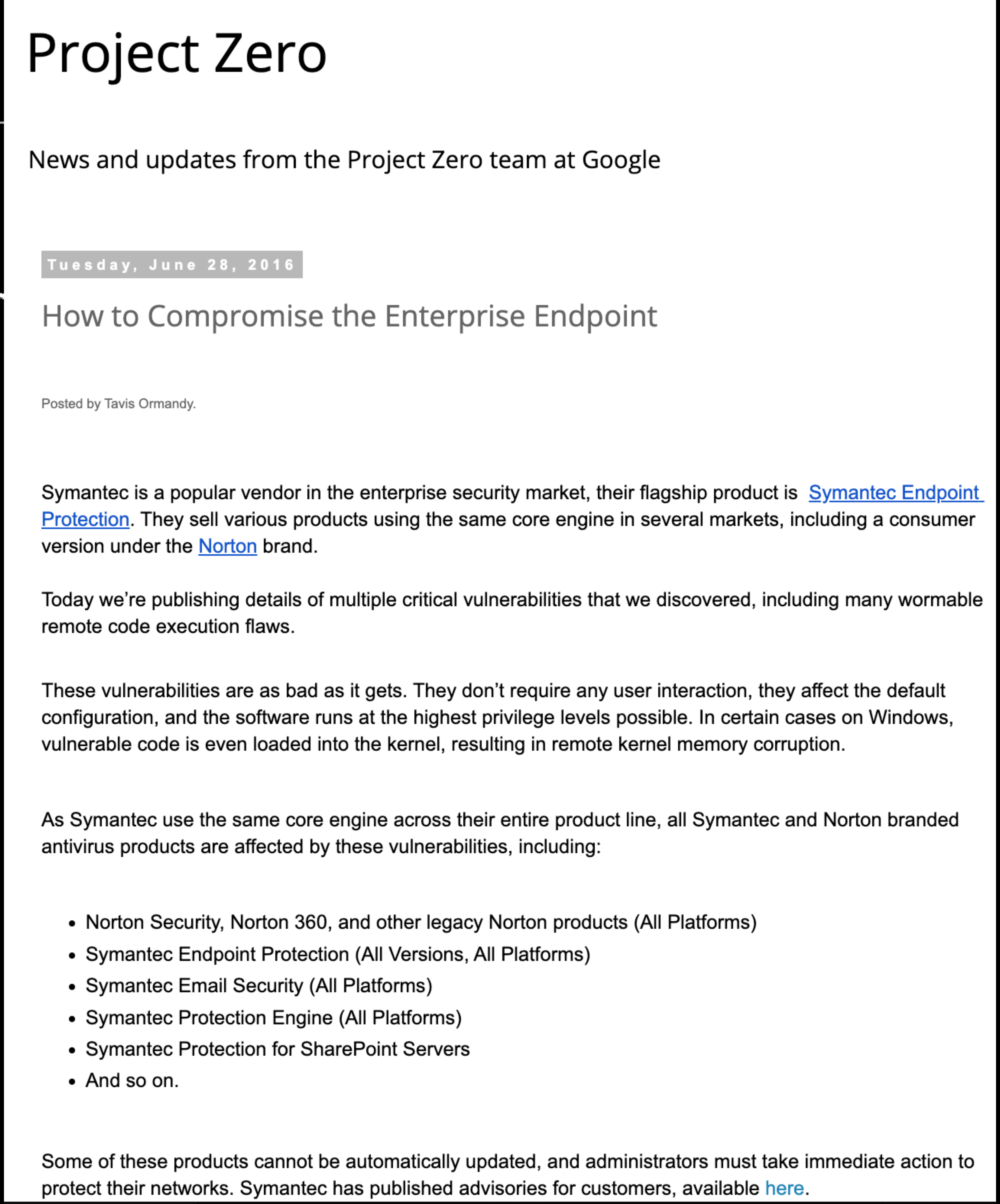
By John Leyden 6 Nov 2012 at 18:28 13 SHARE ▼

A security researcher has discovered embarrassing and critical vulnerabilities in Sophos' enterprise protection software.

Tavis Ormandy, an information security engineer at Google, published a paper along with example attack code to highlight flaws present in Windows, Linux and Mac OS X builds of Sophos' antivirus product.

The holes can be reliably and easily exploited by hackers to compromise the computers the software is supposed to defend. Specifically, the antivirus scanner fails to safely examine encrypted PDFs and VisualBasic files, which could arrive in an email or website download; these documents can be crafted to trigger flaws within the software and gain control of the system.

Source: The Register



Project Zero

News and updates from the Project Zero team at Google

Tuesday, June 28, 2016

How to Compromise the Enterprise Endpoint

Posted by Tavis Ormandy.

Symantec is a popular vendor in the enterprise security market, their flagship product is Symantec Endpoint Protection. They sell various products using the same core engine in several markets, including a consumer version under the Norton brand.

Today we're publishing details of multiple critical vulnerabilities that we discovered, including many wormable remote code execution flaws.

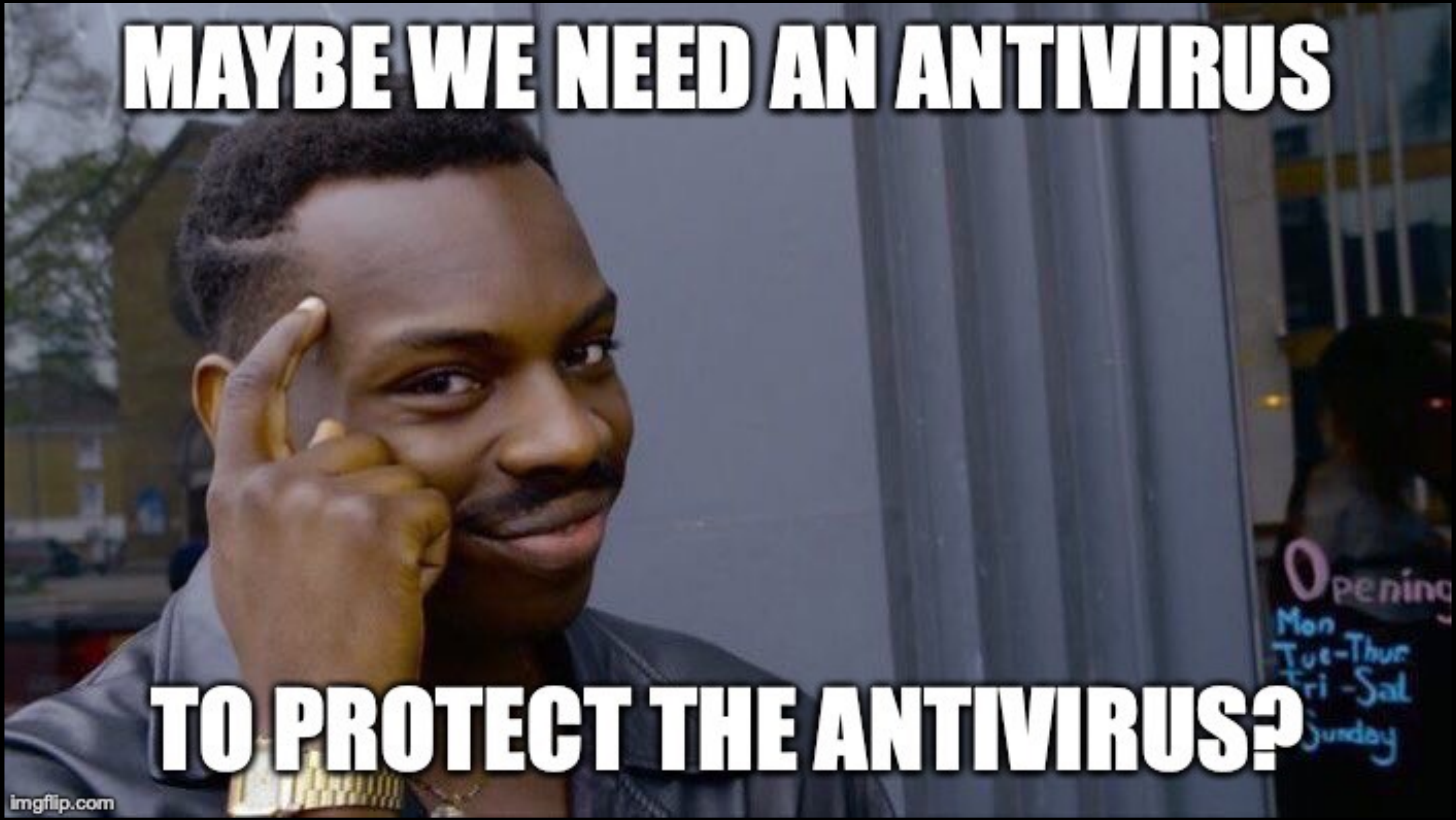
These vulnerabilities are as bad as it gets. They don't require any user interaction, they affect the default configuration, and the software runs at the highest privilege levels possible. In certain cases on Windows, vulnerable code is even loaded into the kernel, resulting in remote kernel memory corruption.

As Symantec use the same core engine across their entire product line, all Symantec and Norton branded antivirus products are affected by these vulnerabilities, including:

- Norton Security, Norton 360, and other legacy Norton products (All Platforms)
- Symantec Endpoint Protection (All Versions, All Platforms)
- Symantec Email Security (All Platforms)
- Symantec Protection Engine (All Platforms)
- Symantec Protection for SharePoint Servers
- And so on.

Some of these products cannot be automatically updated, and administrators must take immediate action to protect their networks. Symantec has published advisories for customers, available here.

Source: Google's Project Zero



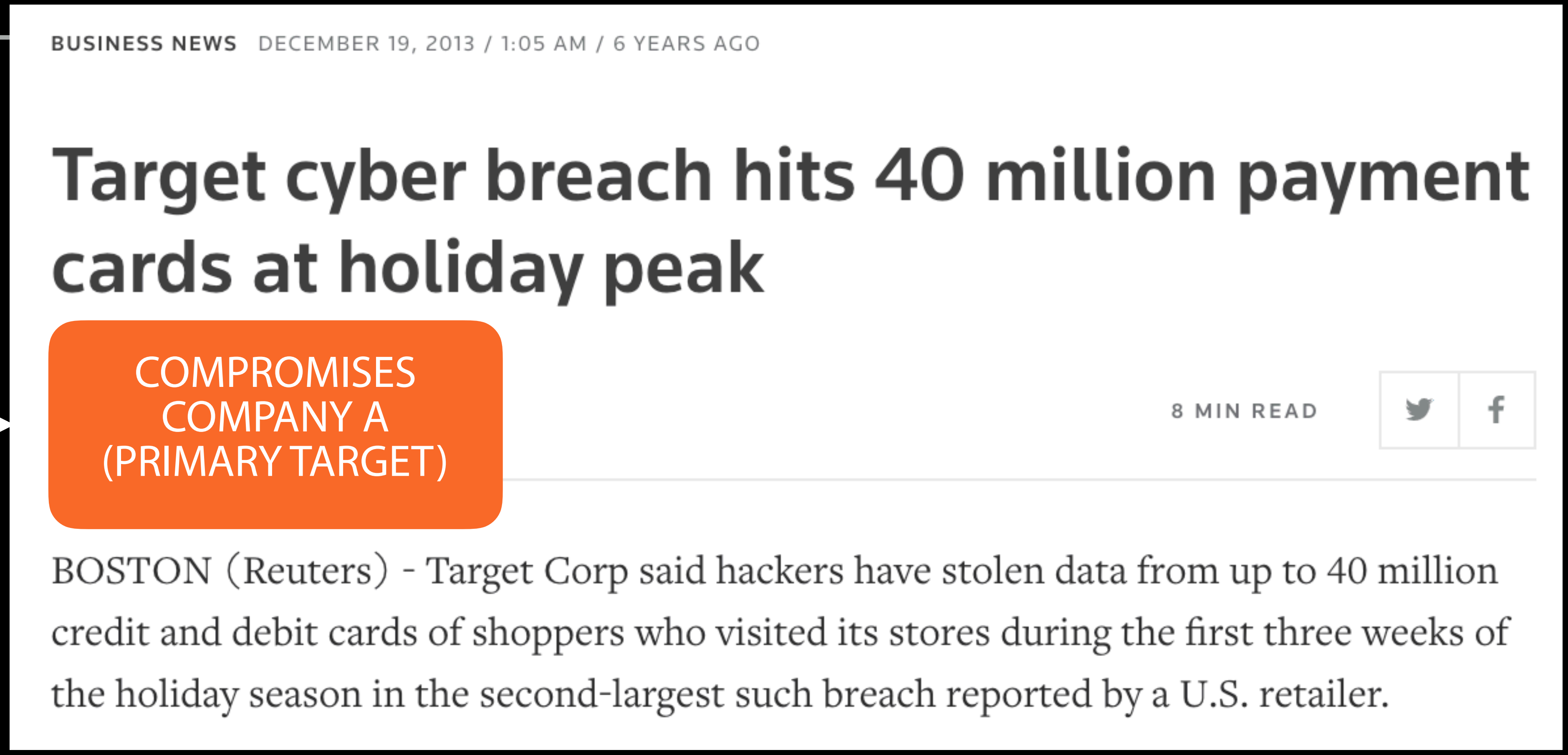
Source: imgflip.com

FROM SUPPLY-CHAIN ATTACKS TO CLASS BREAKS

TARGETS COMPANY X (SECONDARY TARGET)

FAZIO MECHANICAL SERVICES

COMPANY X IS A SUPPLIER OF COMPANY A



BUSINESS NEWS DECEMBER 19, 2013 / 1:05 AM / 6 YEARS AGO

Target cyber breach hits 40 million payment cards at holiday peak

COMPROMISES COMPANY A (PRIMARY TARGET)

8 MIN READ

BOSTON (Reuters) - Target Corp said hackers have stolen data from up to 40 million credit and debit cards of shoppers who visited its stores during the first three weeks of the holiday season in the second-largest such breach reported by a U.S. retailer.

Source: Reuters

TARGETS COMPANY X (SECONDARY TARGET)

COMPANY X IS A SUPPLIER OF MANY ORGS

COMPROMISES TENS IF NOT HUNDREDS OF COMPANIES

COMPANY A

COMPANY B

COMPANY C

COMPANY D

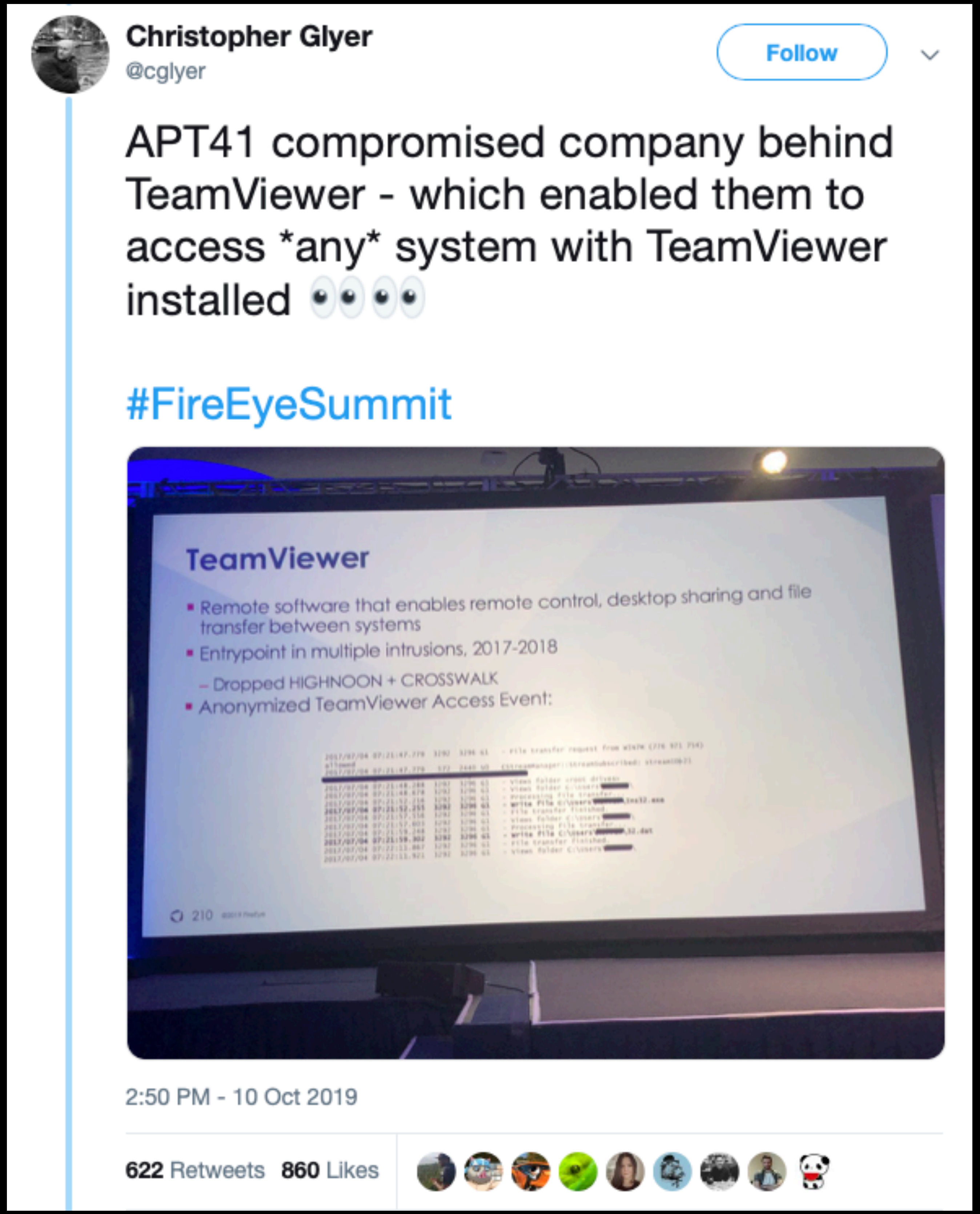
COMPANY E

COMPANY F

COMPANY G

COMPANY H

THIS IS NOT THEORETICAL



Christopher Glyer
@cglyer

Follow

APT41 compromised company behind TeamViewer - which enabled them to access *any* system with TeamViewer installed 👀👀

#FireEyeSummit

TeamViewer

- Remote software that enables remote control, desktop sharing and file transfer between systems
- Entrypoint in multiple intrusions, 2017-2018
  - Dropped HIGHNOON + CROSSWALK
- Anonymized TeamViewer Access Event:

2:50 PM - 10 Oct 2019

622 Retweets 860 Likes

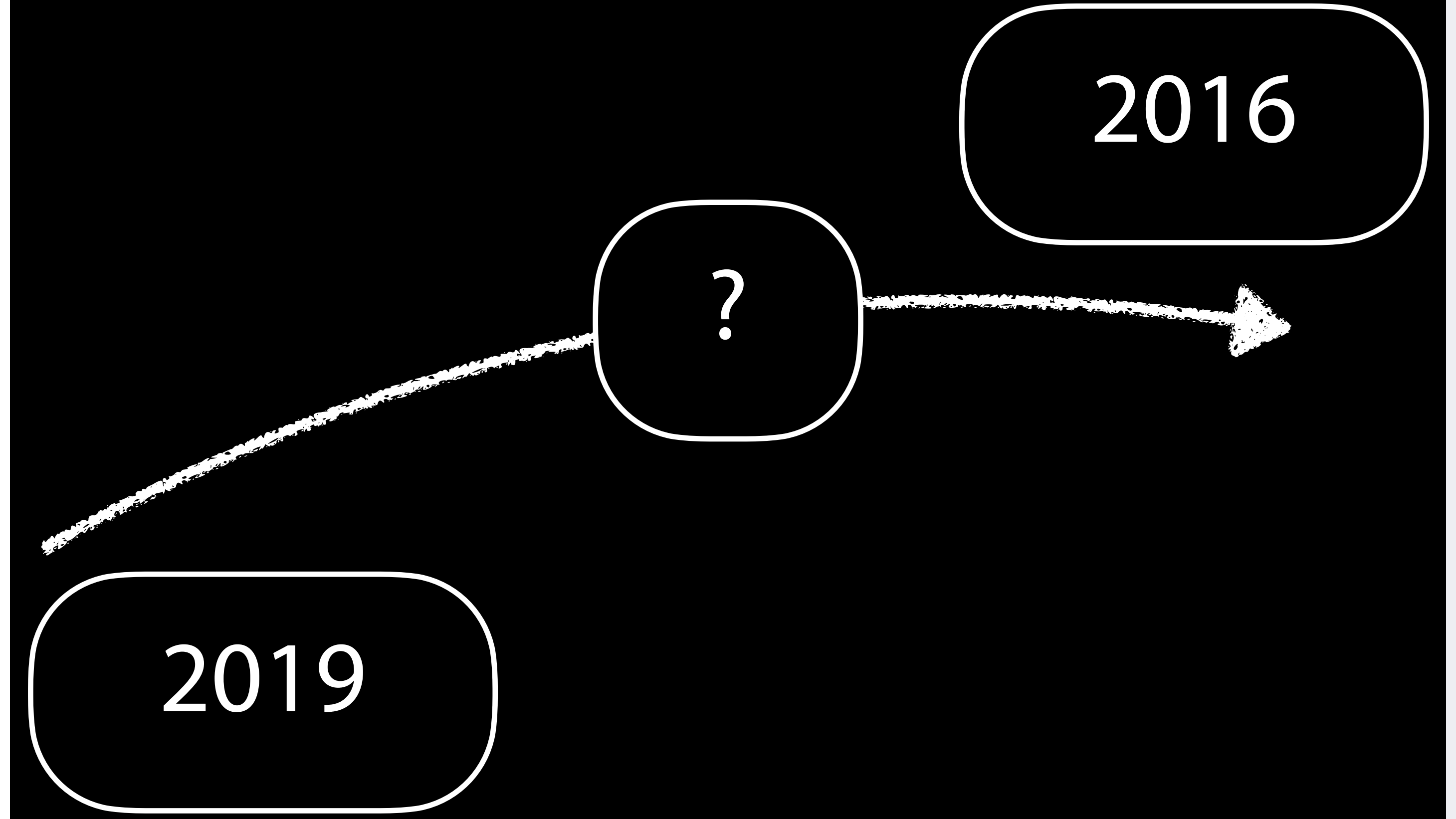
Source: Twitter

Christopher Glyer
@cglyer

Chief Security Architect @FireEye, Retired IR consultant @Mandiant, #StateOfTheHack "Co-anchor" feye.io/soth

Follow

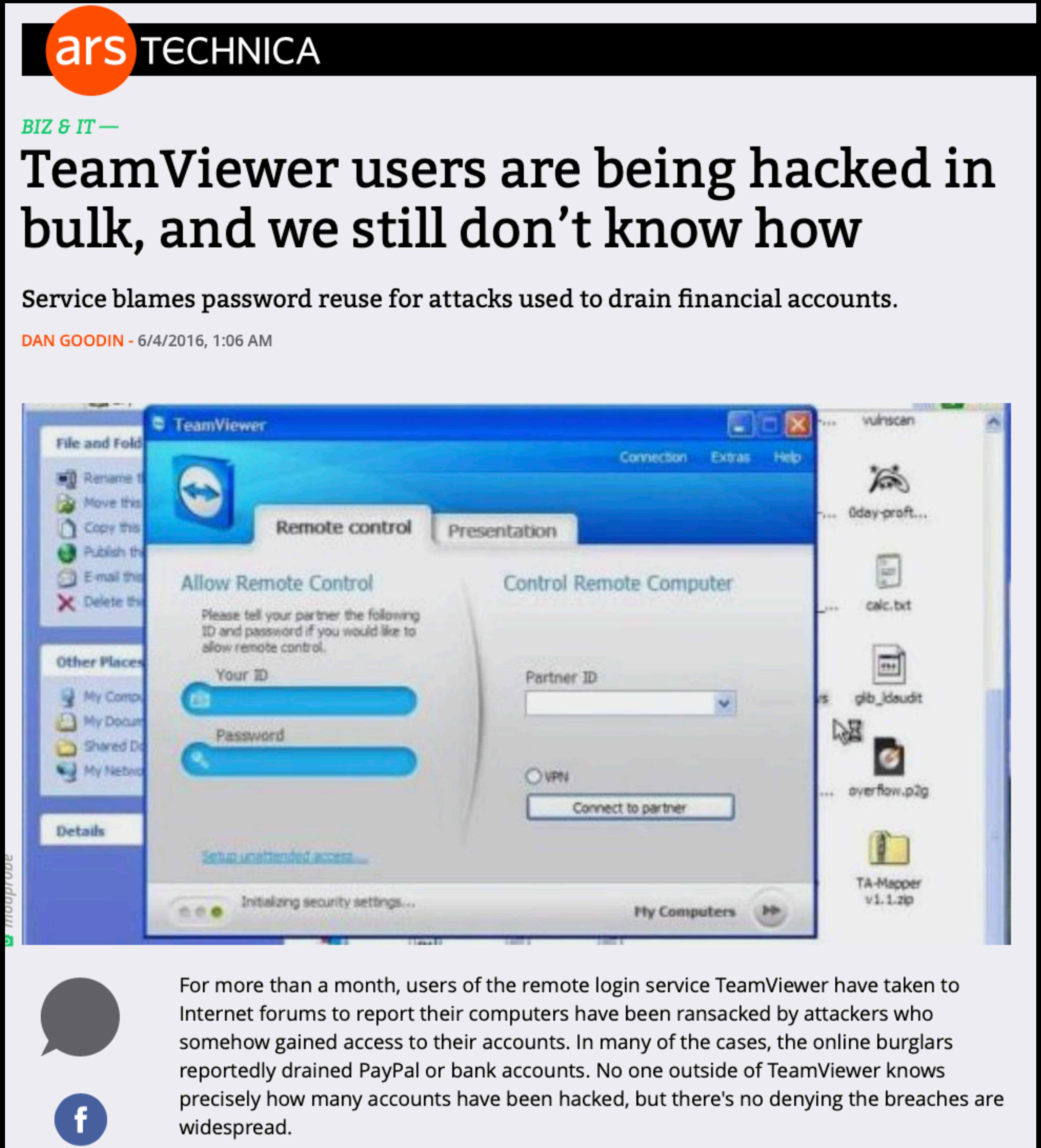
FOLLOWERS	FOLLOWING
9 226	89



2019

?

2016



ars TECHNICA

BIZ & IT —

TeamViewer users are being hacked in bulk, and we still don't know how

Service blames password reuse for attacks used to drain financial accounts.

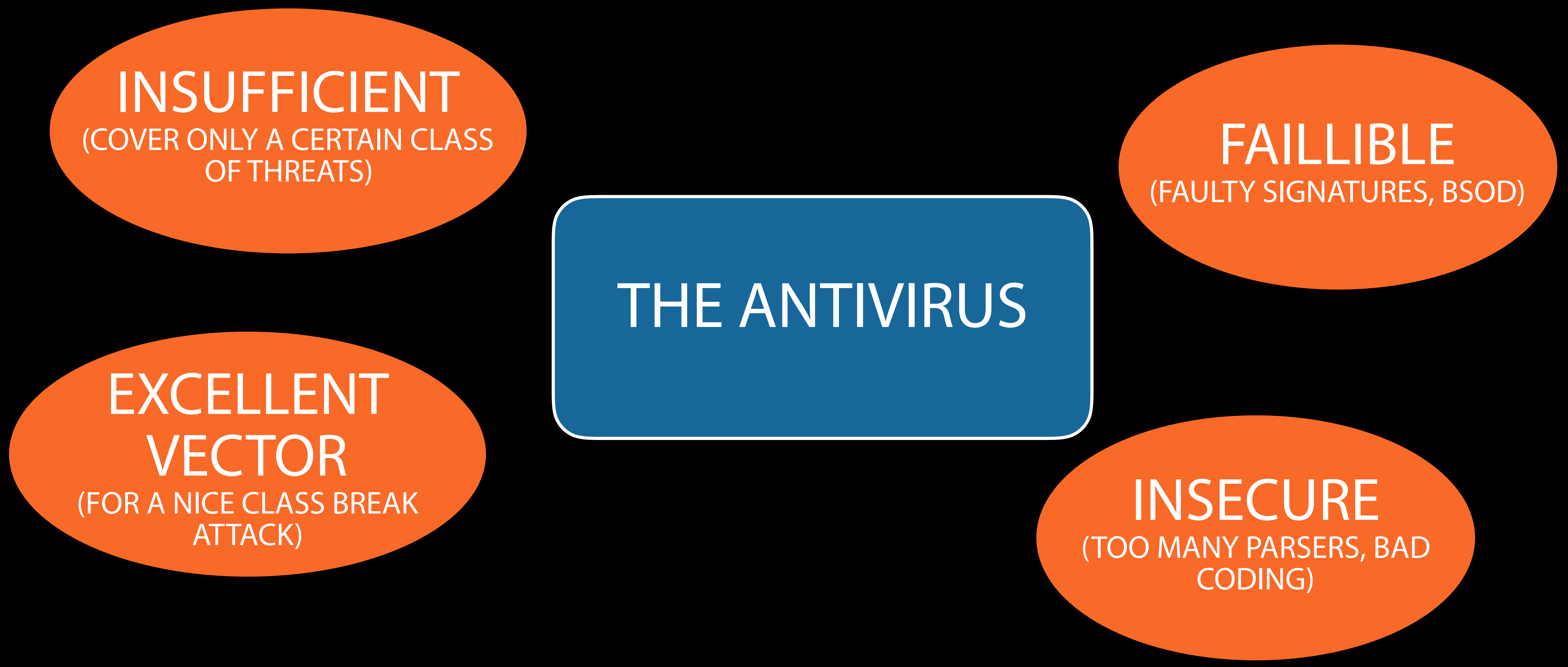
DAN GOODIN - 6/4/2016, 1:06 AM

For more than a month, users of the remote login service TeamViewer have taken to Internet forums to report their computers have been ransacked by attackers who somehow gained access to their accounts. In many of the cases, the online burglars reportedly drained PayPal or bank accounts. No one outside of TeamViewer knows precisely how many accounts have been hacked, but there's no denying the breaches are widespread.

Source: Arstechnica

MARCHING TOWARD FAILURE

IN THE BEGINNING…



THE ANTIVIRUS

INSUFFICIENT
(COVER ONLY A CERTAIN CLASS OF THREATS)

EXCELLENT VECTOR
(FOR A NICE CLASS BREAK ATTACK)

FAILLIBLE
(FAULTY SIGNATURES, BSOD)

INSECURE
(TOO MANY PARSERS, BAD CODING)

WITH GROWING DIGITALISATION COMES PRODUCT PROLIFERATION

UTM

UBA

UEBA

2FA

SANDBOX

ANTI-MALWARE

NETWORK FIREWALL
(WITH DPI)

VPN

NIDS

THREAT FEEDS

VULNERABILITY SCANNERS

WAF

THE ANTIVIRUS

NIPS

TIP

SOAR

ANTI-SPAM

SIEM

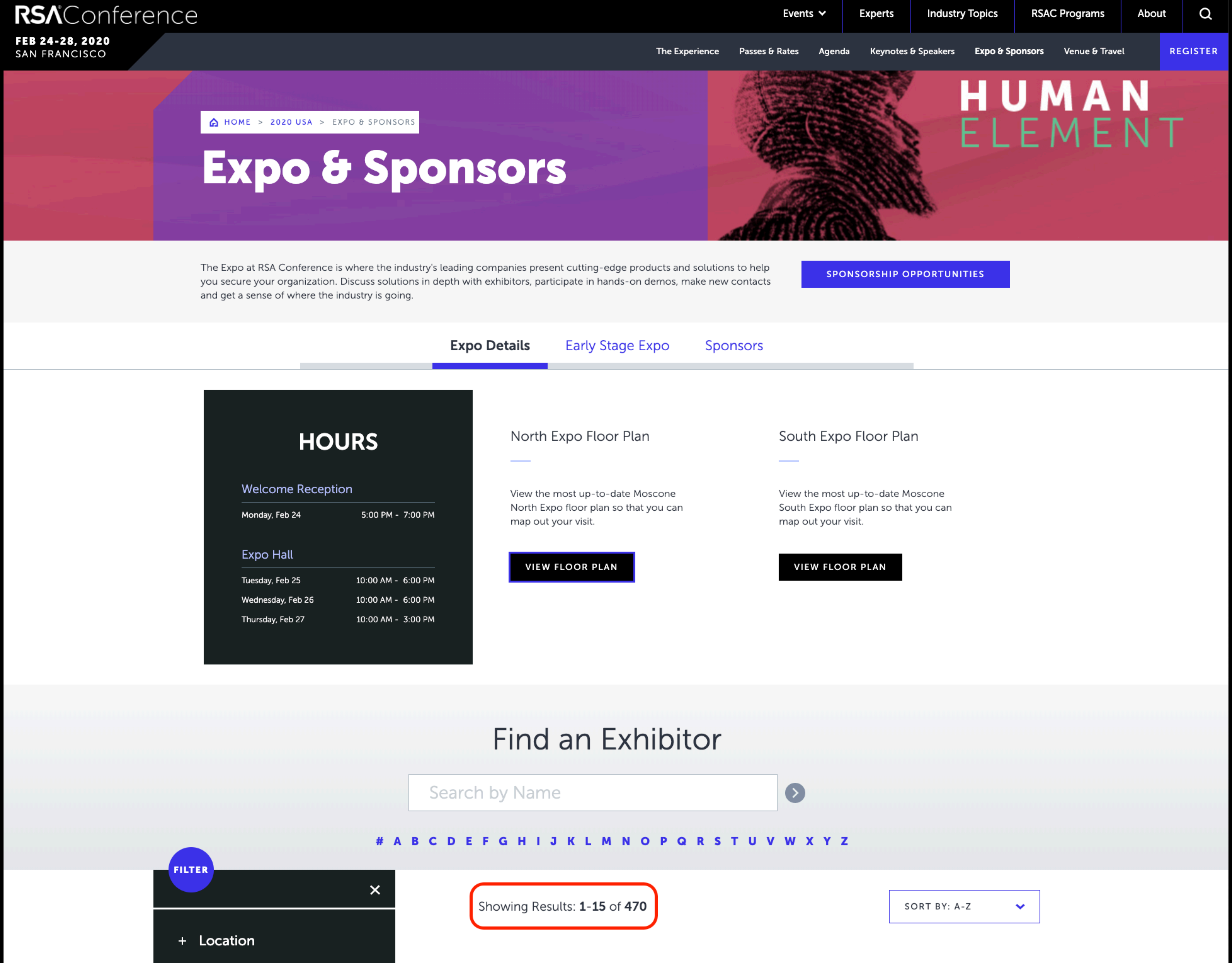
EPP

PROXY

PERSONAL FIREWALL
(WITH DPI)

DLP

EDR



Expo & Sponsors

The Expo at RSA Conference is where the industry's leading companies present cutting-edge products and solutions to help you secure your organization. Discuss solutions in depth with exhibitors, participate in hands-on demos, make new contacts and get a sense of where the industry is going.

HOURS

Welcome Reception

Monday, Feb 24	5:00 PM - 7:00 PM

Expo Hall

Tuesday, Feb 25	10:00 AM - 6:00 PM
Wednesday, Feb 26	10:00 AM - 6:00 PM
Thursday, Feb 27	10:00 AM - 3:00 PM

North Expo Floor Plan

View the most up-to-date Moscone North Expo floor plan so that you can map out your visit.

South Expo Floor Plan

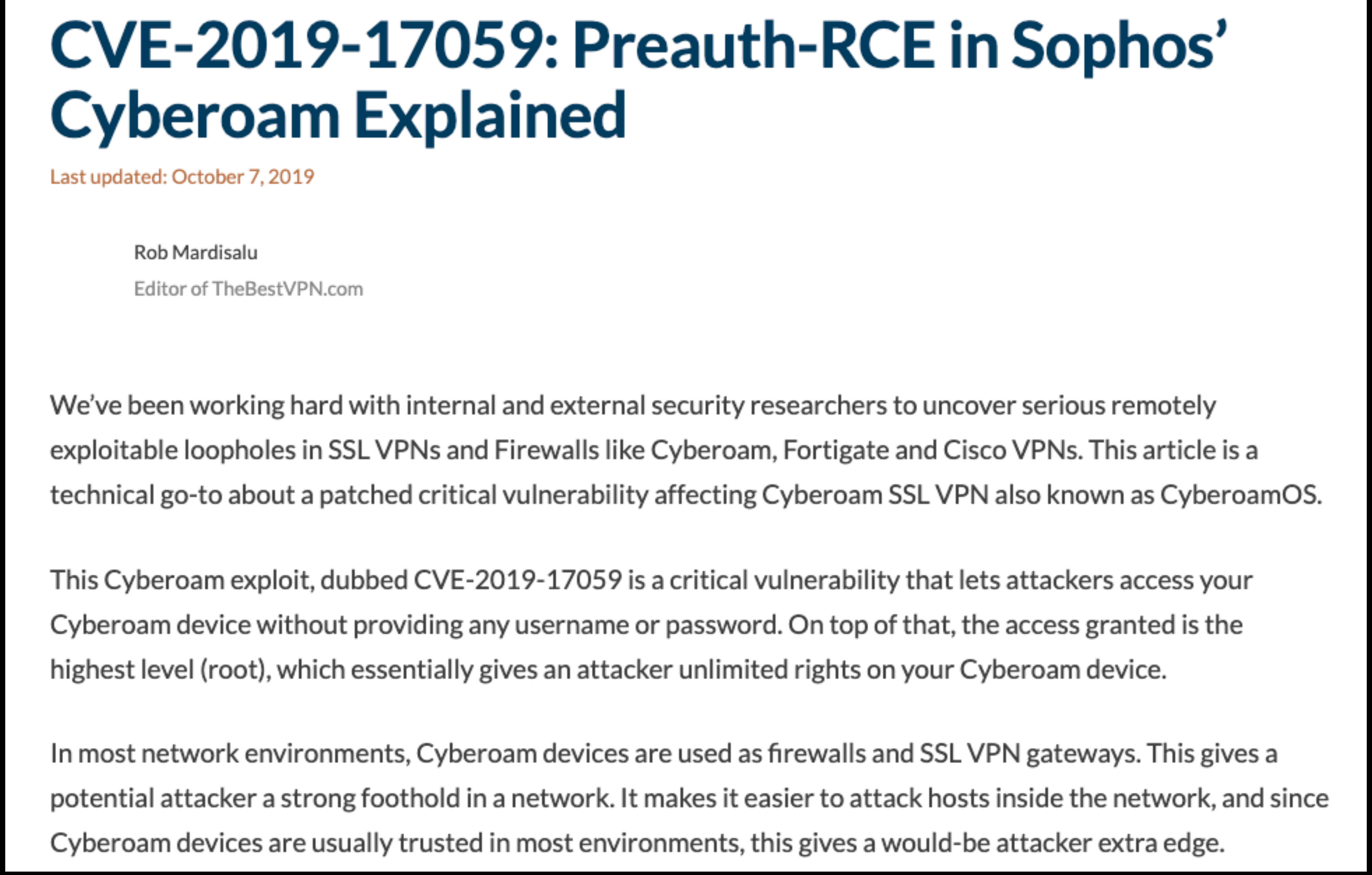
View the most up-to-date Moscone South Expo floor plan so that you can map out your visit.

Find an Exhibitor

Showing Results: **1-15** of **470**

Source: RSA Conference

LIKE THE ANTIVIRUS, THESE 'SOLUTIONS' ARE ALL PART OF THE ATTACK SURFACE



CVE-2019-17059: Preauth-RCE in Sophos' Cyberoam Explained

Last updated: October 7, 2019

Rob Mardisalu
Editor of TheBestVPN.com

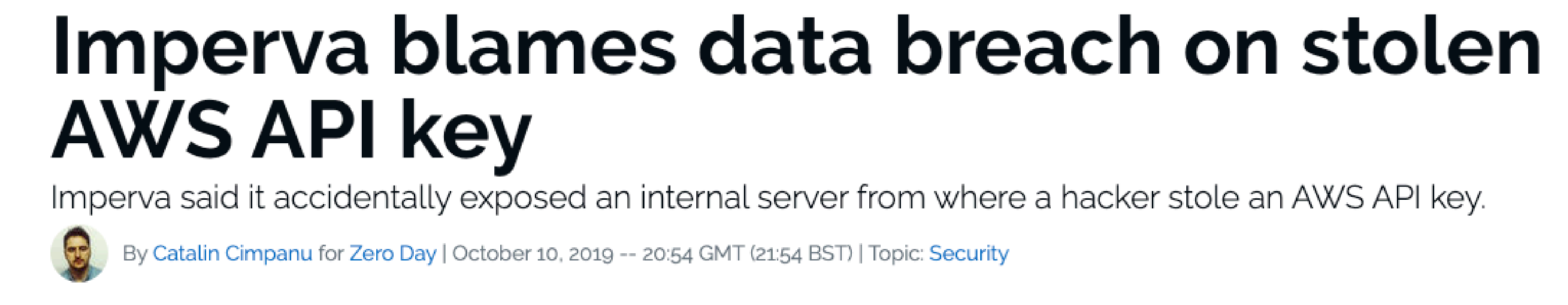
We've been working hard with internal and external security researchers to uncover serious remotely exploitable loopholes in SSL VPNs and Firewalls like Cyberoam, Fortigate and Cisco VPNs. This article is a technical go-to about a patched critical vulnerability affecting Cyberoam SSL VPN also known as CyberoamOS.

This Cyberoam exploit, dubbed CVE-2019-17059 is a critical vulnerability that lets attackers access your Cyberoam device without providing any username or password. On top of that, the access granted is the highest level (root), which essentially gives an attacker unlimited rights on your Cyberoam device.

In most network environments, Cyberoam devices are used as firewalls and SSL VPN gateways. This gives a potential attacker a strong foothold in a network. It makes it easier to attack hosts inside the network, and since Cyberoam devices are usually trusted in most environments, this gives a would-be attacker extra edge.

7 Oct 2019, Source: thebestvpn

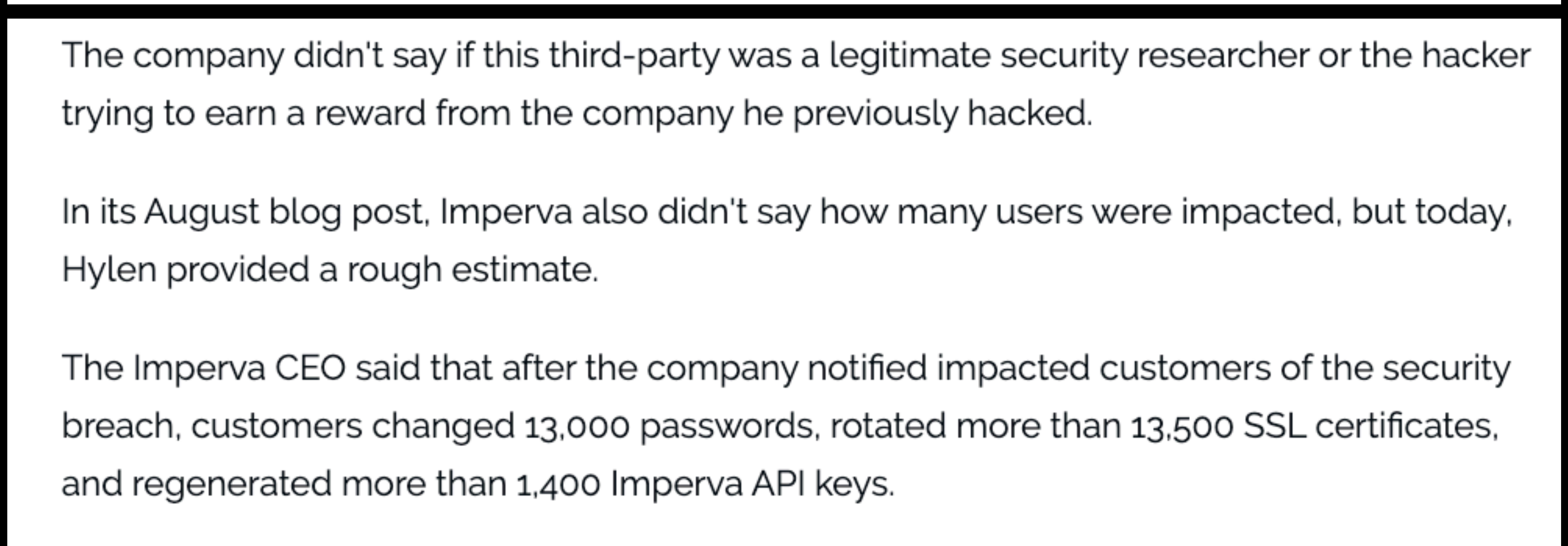
10 Oct 2019, Source: ZDNet



Imperva blames data breach on stolen AWS API key

Imperva said it accidentally exposed an internal server from where a hacker stole an AWS API key.

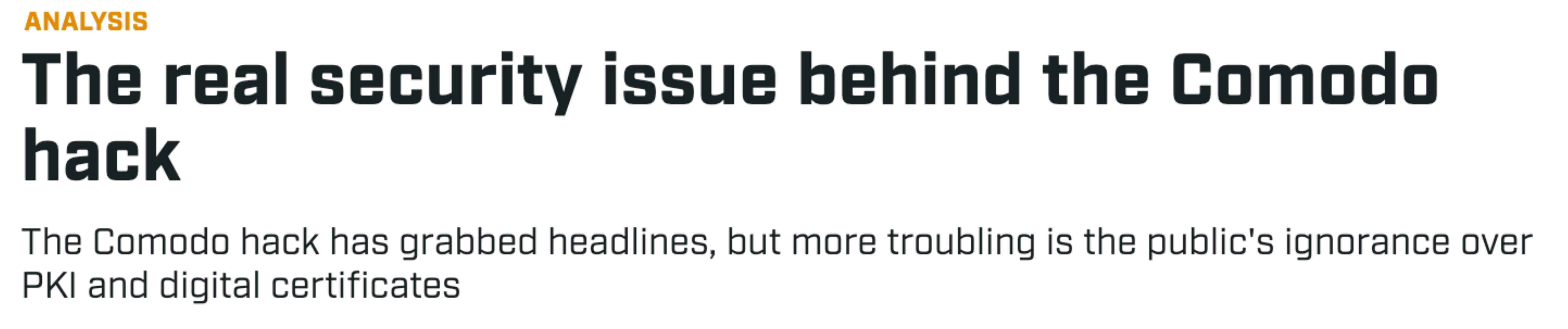
By Catalin Cimpanu for Zero Day | October 10, 2019 -- 20:54 GMT (21:54 BST) | Topic: Security



The company didn't say if this third-party was a legitimate security researcher or the hacker trying to earn a reward from the company he previously hacked.

In its August blog post, Imperva also didn't say how many users were impacted, but today, Hylen provided a rough estimate.

The Imperva CEO said that after the company notified impacted customers of the security breach, customers changed 13,000 passwords, rotated more than 13,500 SSL certificates, and regenerated more than 1,400 Imperva API keys.

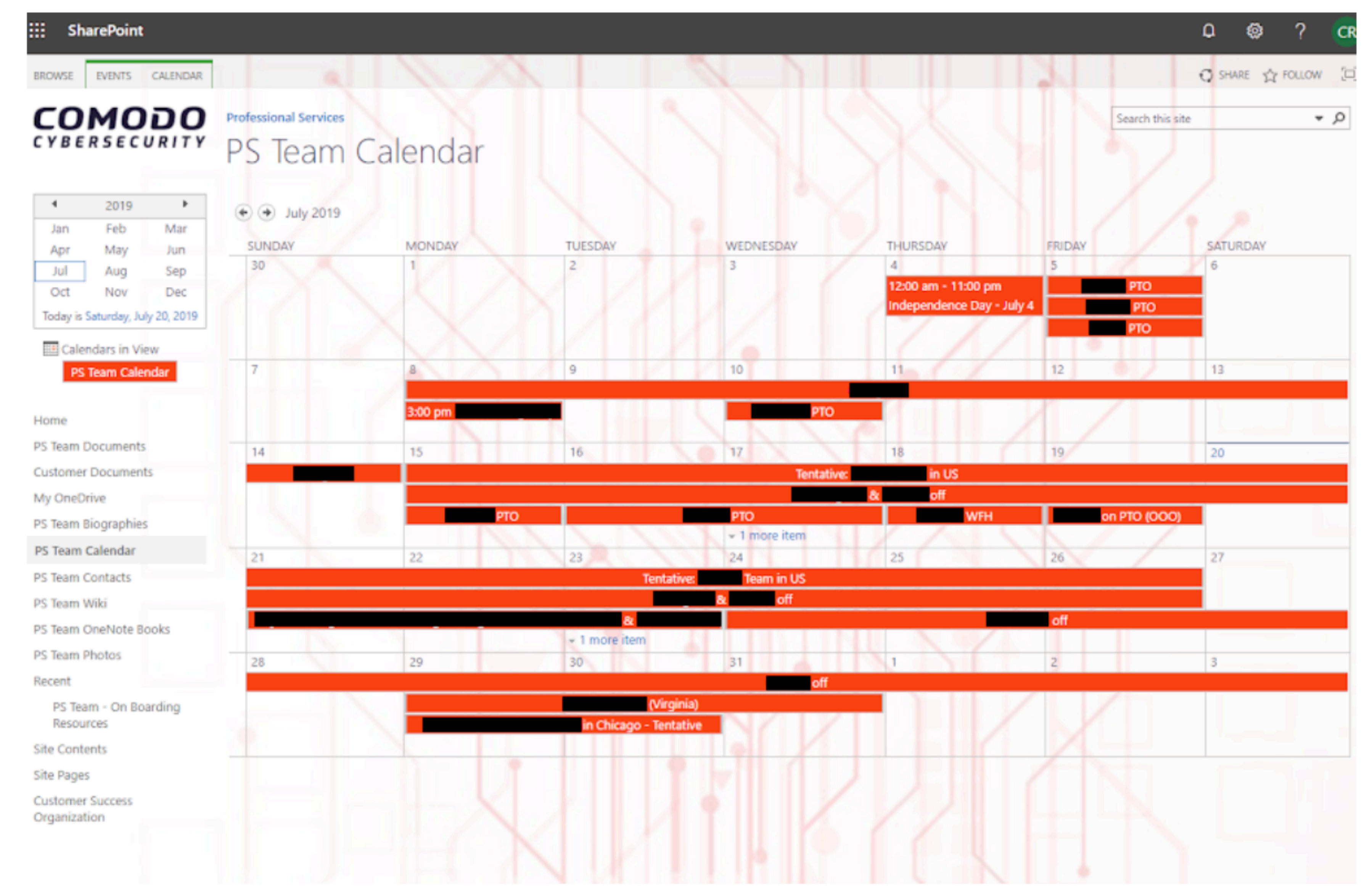


ANALYSIS

The real security issue behind the Comodo hack

The Comodo hack has grabbed headlines, but more troubling is the public's ignorance over PKI and digital certificates

2011, Source: CSOOnline



PS Team Calendar

Today is Saturday, July 20, 2019

July 2019

12:00 am - 11:00 pm Independence Day - July 4

[redacted] PTO

[redacted] PTO

[redacted] PTO

[redacted]

3:00 pm [redacted]

[redacted] PTO

[redacted]

Tentative: [redacted] in US

[redacted] & [redacted] off

[redacted] PTO

[redacted] PTO

[redacted] WFH

[redacted] on PTO (OOO)

1 more item

Tentative: [redacted] Team in US

[redacted] & [redacted] off

[redacted] & [redacted]

[redacted] off

1 more item

[redacted] off

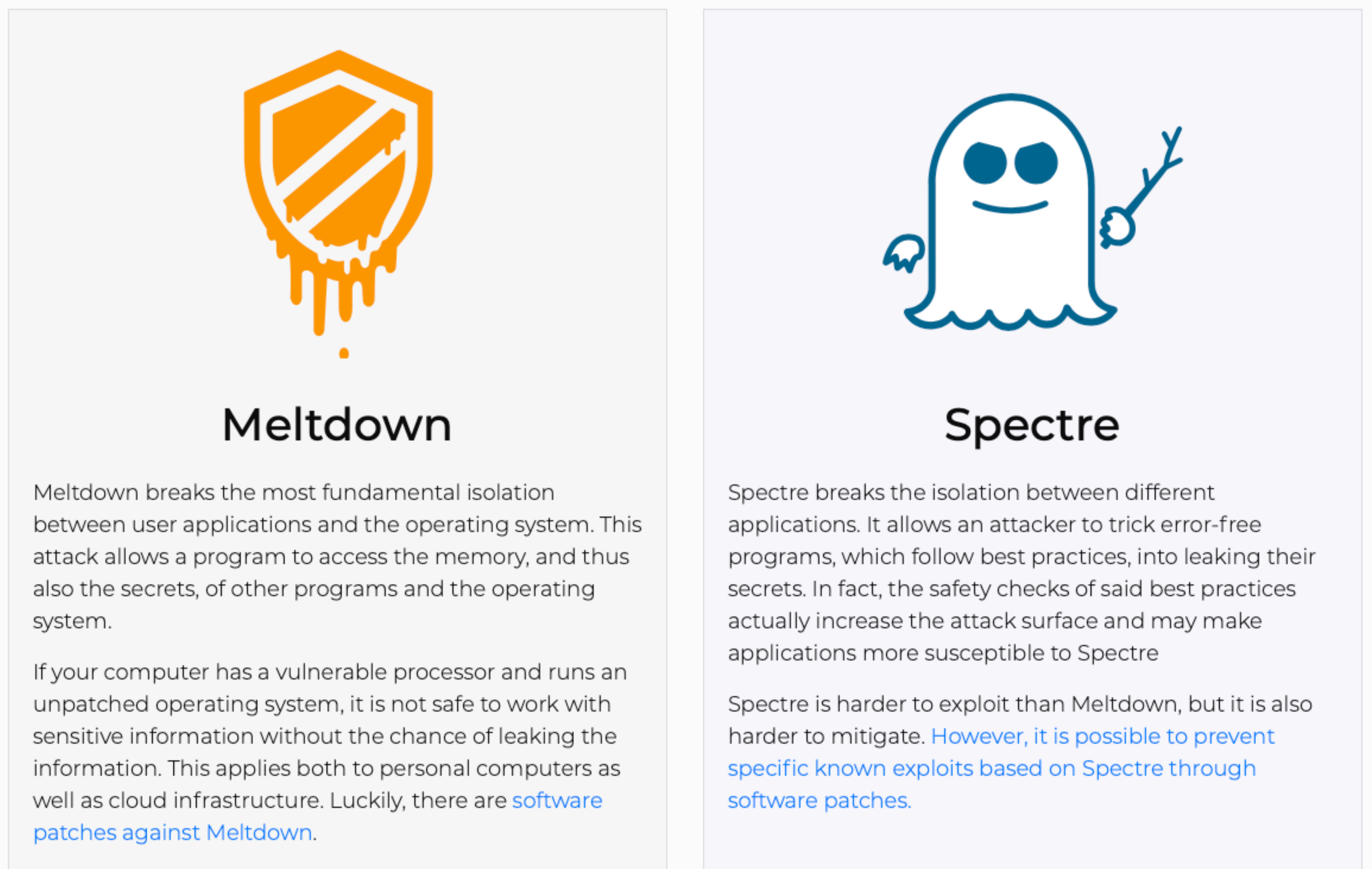
[redacted] (Virginia)

[redacted] in Chicago - Tentative

A screenshot of a staff calendar on Comodo's internal site (Image: supplied)

2019
Source: TechCrunch

… RUNNING ON TOP OF VULNERABLE PROCESSORS



Meltdown

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

If your computer has a vulnerable processor and runs an unpatched operating system, it is not safe to work with sensitive information without the chance of leaking the information. This applies both to personal computers as well as cloud infrastructure. Luckily, there are software patches against Meltdown.

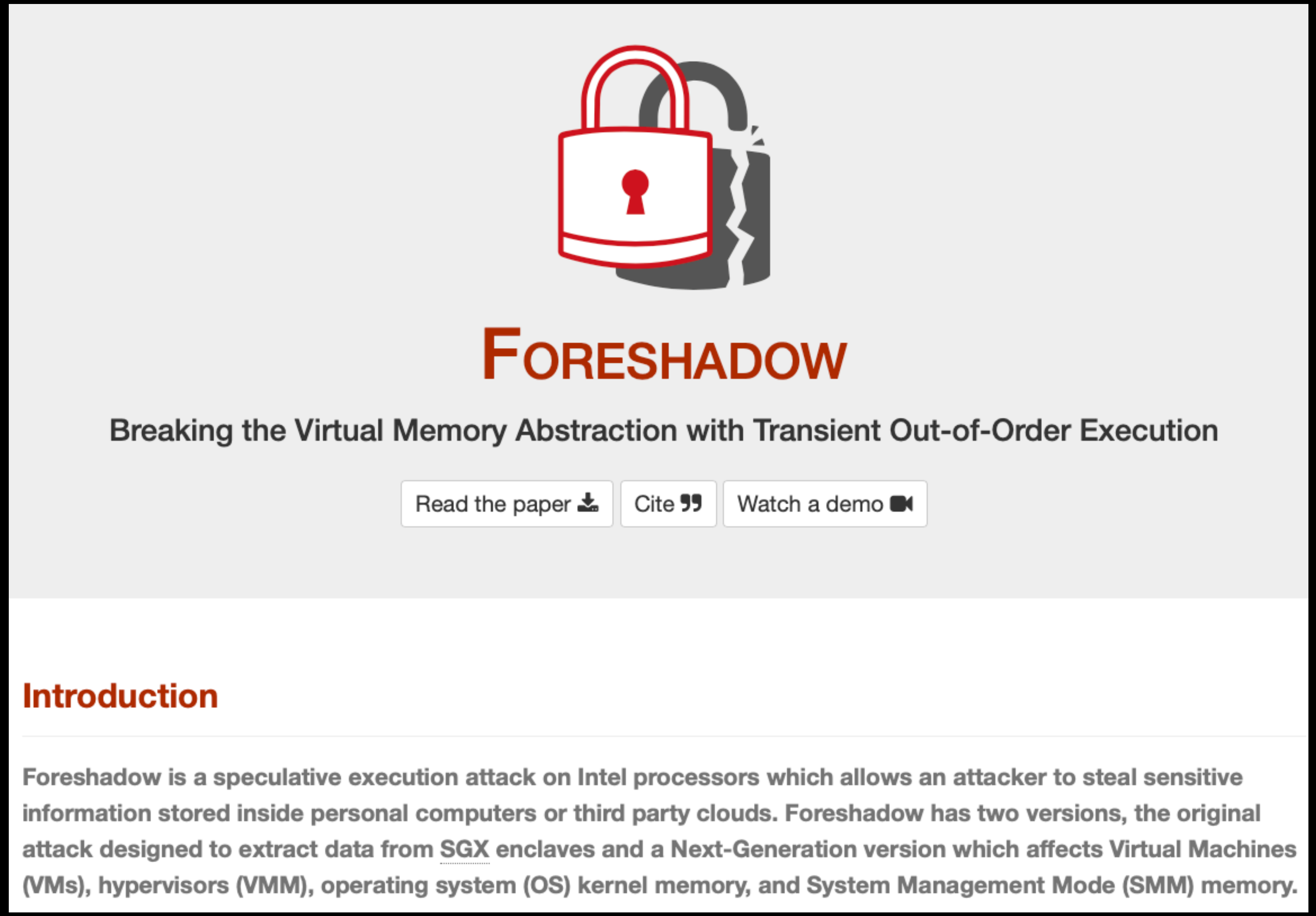
Spectre

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre

Spectre is harder to exploit than Meltdown, but it is also harder to mitigate. However, it is possible to prevent specific known exploits based on Spectre through software patches.

Source: https://meltdownattack.com

Source: https://foreshadowattack.eu



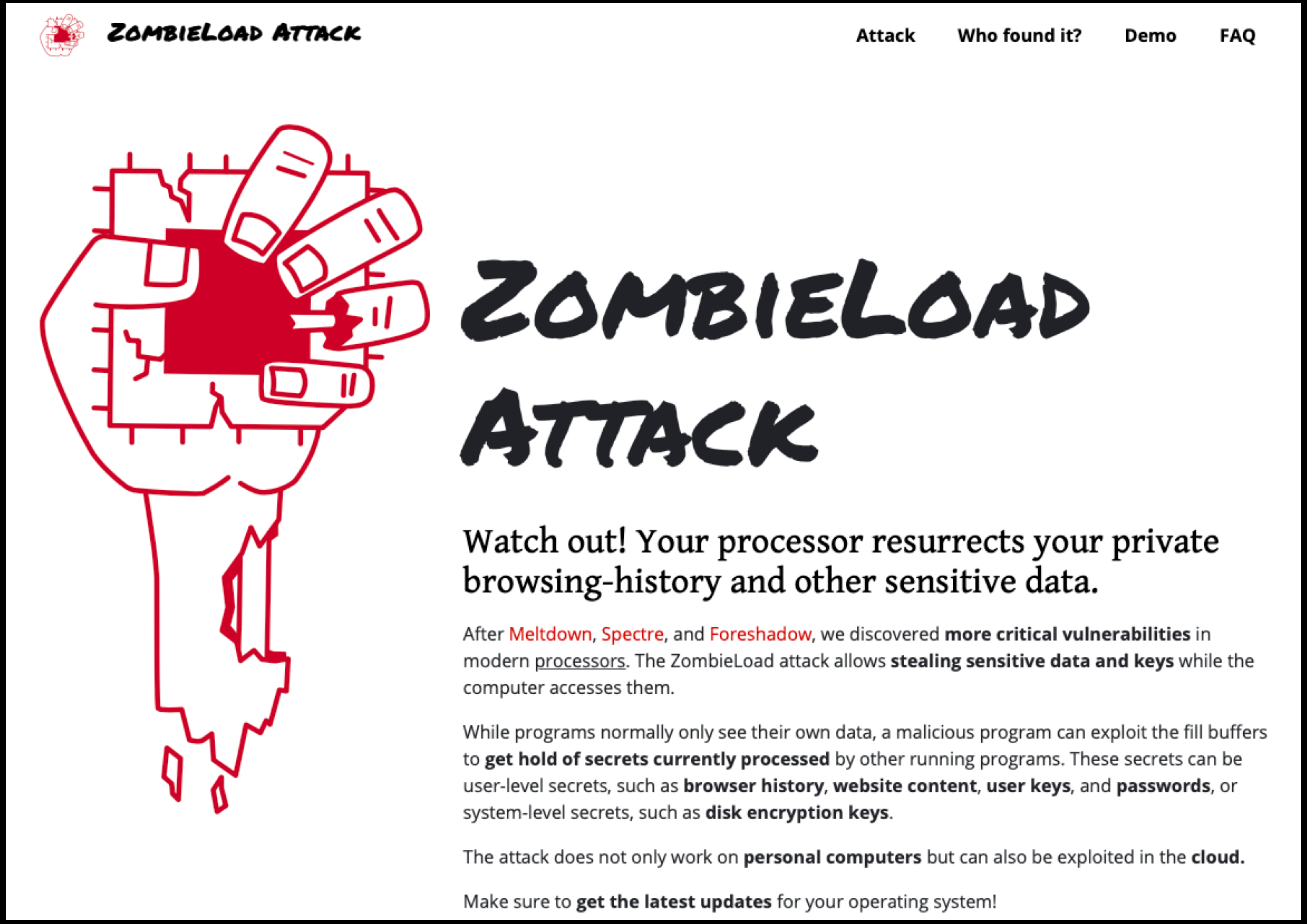
Foreshadow

Breaking the Virtual Memory Abstraction with Transient Out-of-Order Execution

Read the paper | Cite | Watch a demo

Introduction

Foreshadow is a speculative execution attack on Intel processors which allows an attacker to steal sensitive information stored inside personal computers or third party clouds. Foreshadow has two versions, the original attack designed to extract data from SGX enclaves and a Next-Generation version which affects Virtual Machines (VMs), hypervisors (VMM), operating system (OS) kernel memory, and System Management Mode (SMM) memory.



ZombieLoad Attack

Watch out! Your processor resurrects your private browsing-history and other sensitive data.

After Meltdown, Spectre, and Foreshadow, we discovered **more critical vulnerabilities** in modern processors. The ZombieLoad attack allows **stealing sensitive data and keys** while the computer accesses them.

While programs normally only see their own data, a malicious program can exploit the fill buffers to **get hold of secrets currently processed** by other running programs. These secrets can be user-level secrets, such as **browser history**, **website content**, **user keys**, and **passwords**, or system-level secrets, such as **disk encryption keys**.

The attack does not only work on **personal computers** but can also be exploited in the **cloud.**

Make sure to **get the latest updates** for your operating system!

Source: https://zombieloadattack.com

AND THEY NEED HUMANS & €€€ TO INSTALL, USE AND MAINTAIN

CONFIGURE LOGGING PROPERLY (NO, IT'S NOT A FIRE & FORGET TASK)

BUY THREAT FEEDS

MONITOR THE HEALTH OF THE SYSTEM (ARE YOU SURE YOU ARE NOT MISSING LOGS?)

BUILD AND MAINTAIN USE CASES

TRAIN PEOPLE (TO USE SOME OBSCURE QUERY LANGUAGE)

BUY A TIP

BUY SOFTWARE

SIEM

BUY AN ADD-ON FOR YOUR COMPLIANCE NEEDS

MAKE CLUSTERS & BACK-UPS

HIRE DATA SCIENTISTS

BUY HARDWARE

RECRUIT SYSADMINS

BUY AN INCIDENT RESPONSE PLATFORM

BUY SUPPORT

BUY PRO SERVICES (BECAUSE YOU NEED NEW PARSERS AND YOUR EXISTING PARSERS WILL BREAK)

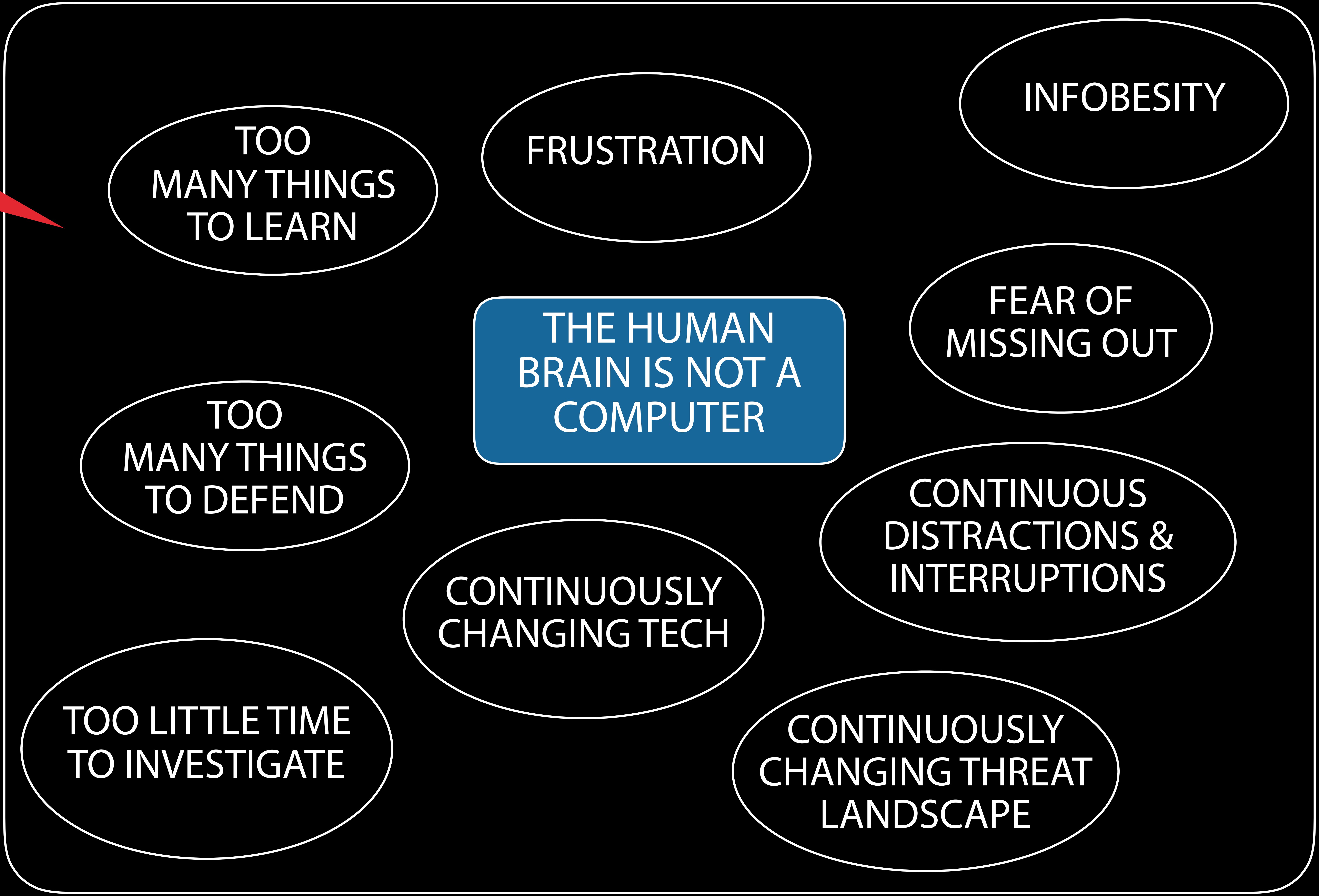
CONFIGURE ALERTS (AND HOPE YOUR ANALYSTS WON'T DIE OUT OF FALSE POSITIVE FATIGUE)

BUY PRO SERVICES (BECAUSE THERE ARE ALWAYS 'EDGE CASES')

HOUSTON, WE HAVE A SERIOUS LAYER 8 PROBLEM

TRENDING!

THE PERFECT RECIPE FOR DOOM (& BURNOUTS)



THE HUMAN BRAIN IS NOT A COMPUTER

TOO MANY THINGS TO LEARN

FRUSTRATION

INFOBESITY

FEAR OF MISSING OUT

TOO MANY THINGS TO DEFEND

CONTINUOUS DISTRACTIONS & INTERRUPTIONS

CONTINUOUSLY CHANGING TECH

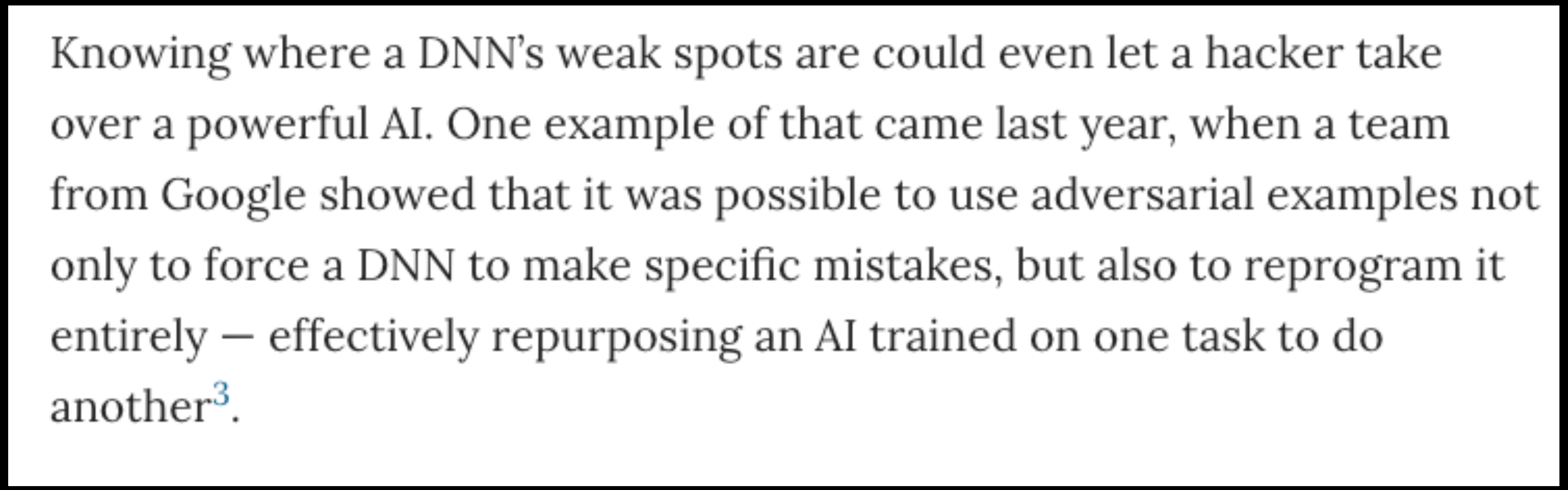
TOO LITTLE TIME TO INVESTIGATE

CONTINUOUSLY CHANGING THREAT LANDSCAPE

HANG ON APOLLO! HELP IS ON ITS WAY!

NOPE, ARTIFICIAL INTELLIGENCE IS NOWHERE READY TO HELP US

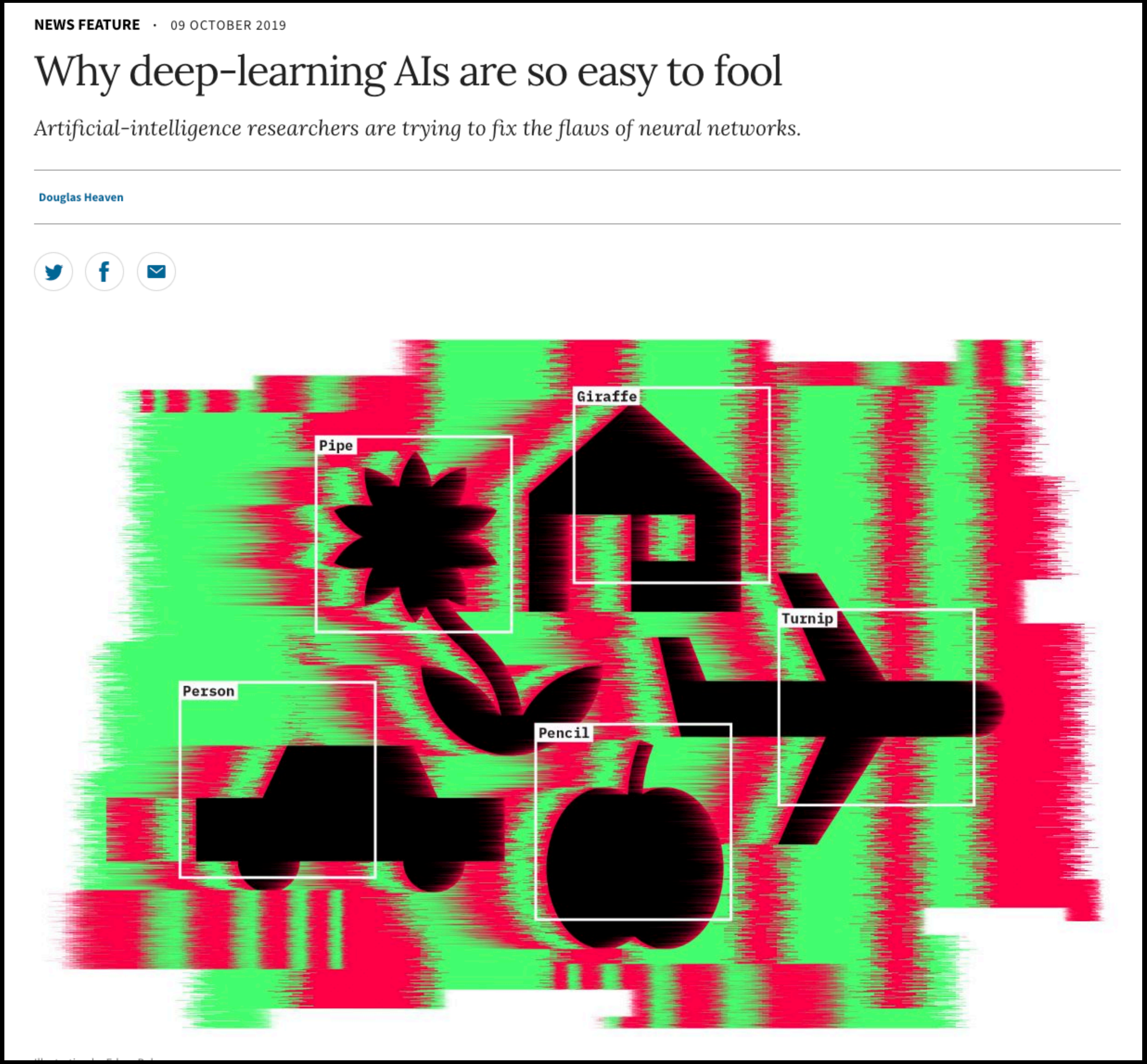
BREAKING DEEP NEURAL NETWORKS (DNNs) IS VERY EASY



Knowing where a DNN's weak spots are could even let a hacker take over a powerful AI. One example of that came last year, when a team from Google showed that it was possible to use adversarial examples not only to force a DNN to make specific mistakes, but also to reprogram it entirely — effectively repurposing an AI trained on one task to do another[3].

Further reading: Adversarial Reprogramming of Neural Networks, Cornell University

ALGORITHMS ARE CREATED BY 'FLAWED' HUMANS & TRAINED ON DATA OF VARYING QUALITY WHILE RUNNING ON VULNERABLE PROCESSORS



NEWS FEATURE · 09 OCTOBER 2019

Why deep-learning AIs are so easy to fool

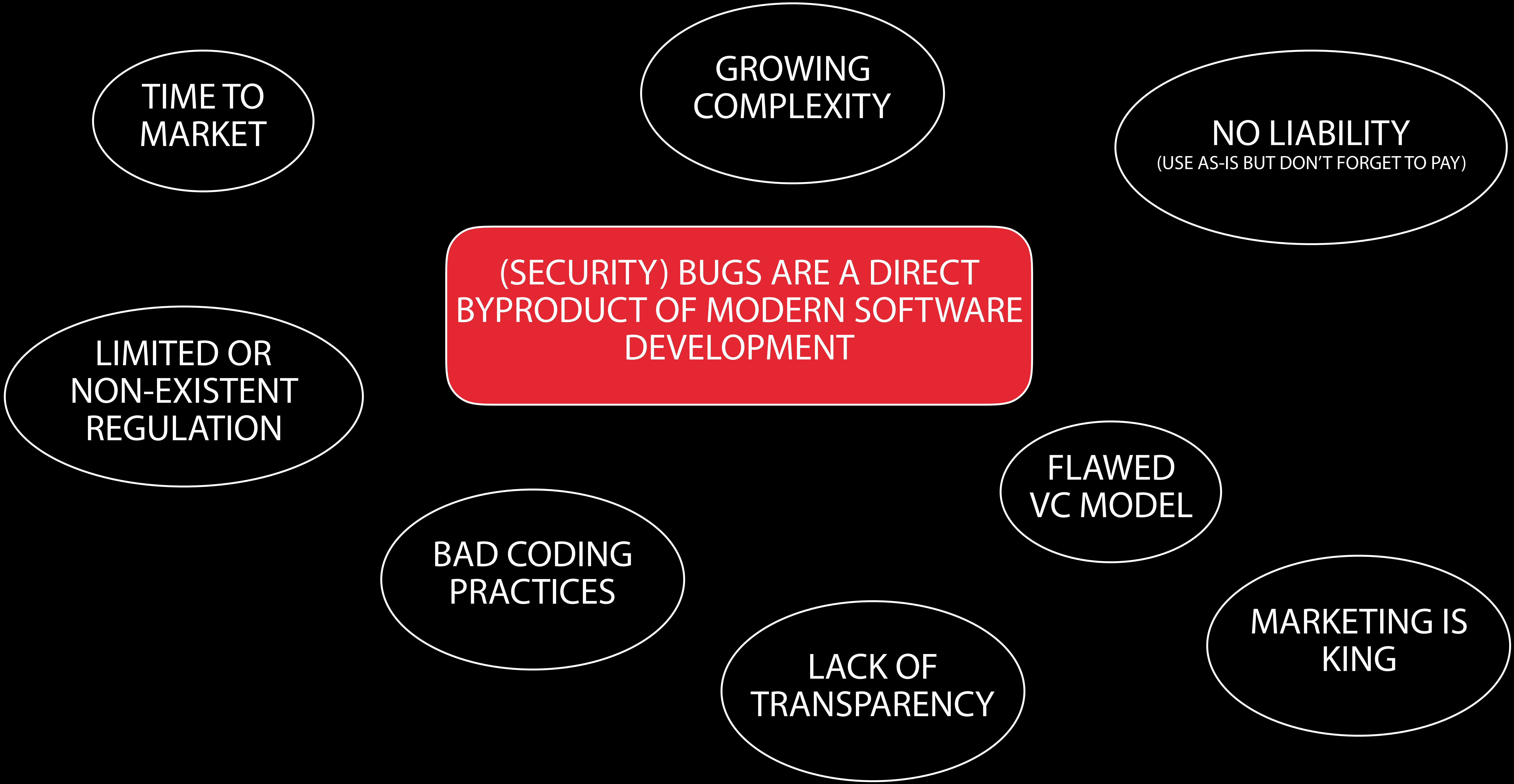
Artificial-intelligence researchers are trying to fix the flaws of neural networks.

Douglas Heaven

Source: Nature

BREAKING THE FAILURE CYCLE

THERE IS NO SILVER BULLET



(SECURITY) BUGS ARE A DIRECT BYPRODUCT OF MODERN SOFTWARE DEVELOPMENT

TIME TO MARKET

GROWING COMPLEXITY

NO LIABILITY
(USE AS-IS BUT DON'T FORGET TO PAY)

LIMITED OR NON-EXISTENT REGULATION

FLAWED VC MODEL

BAD CODING PRACTICES

LACK OF TRANSPARENCY

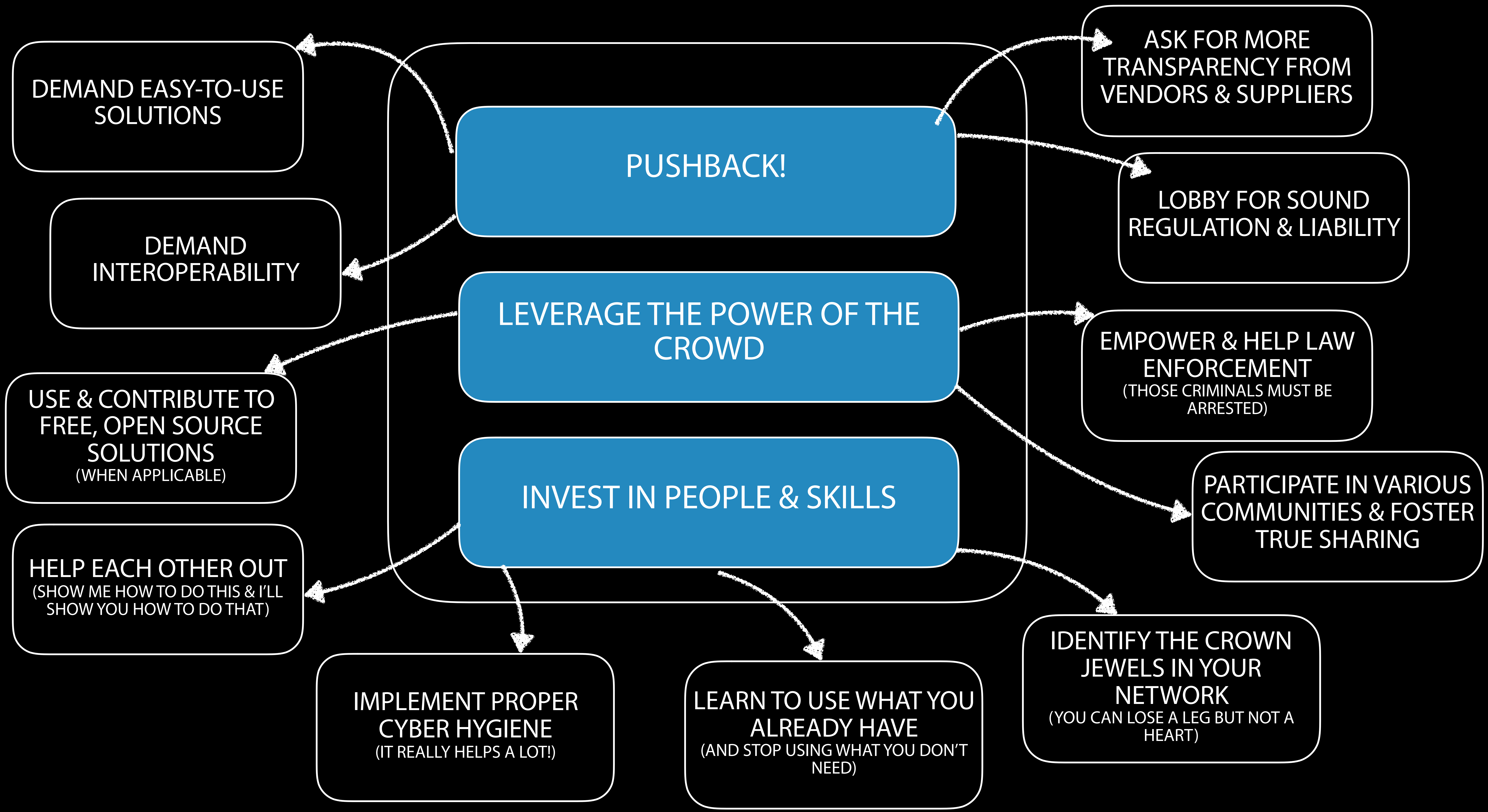
MARKETING IS KING

AND THINGS ARE GETTING WORSE

> *The over-complexification of provisioning and deployment pipelines is a dangerous trend. I don't trust the layers upon layers of scripts and tools to not break randomly, and I worry the maintenance cost is getting out of hands. Yes, I'm looking at you, k8s.*

Source: Julien Vehent, Firefox Operations Security at @Mozilla. Author of Security DevOps http://securing-devops.com; coder & speaker.

WE KNOW THE SOLUTIONS AND THEY REQUIRE COURAGE & HARD WORK



PUSHBACK!

DEMAND EASY-TO-USE SOLUTIONS

DEMAND INTEROPERABILITY

ASK FOR MORE TRANSPARENCY FROM VENDORS & SUPPLIERS

LOBBY FOR SOUND REGULATION & LIABILITY

LEVERAGE THE POWER OF THE CROWD

USE & CONTRIBUTE TO FREE, OPEN SOURCE SOLUTIONS (WHEN APPLICABLE)

EMPOWER & HELP LAW ENFORCEMENT (THOSE CRIMINALS MUST BE ARRESTED)

PARTICIPATE IN VARIOUS COMMUNITIES & FOSTER TRUE SHARING

INVEST IN PEOPLE & SKILLS

HELP EACH OTHER OUT (SHOW ME HOW TO DO THIS & I'LL SHOW YOU HOW TO DO THAT)

IMPLEMENT PROPER CYBER HYGIENE (IT REALLY HELPS A LOT!)

LEARN TO USE WHAT YOU ALREADY HAVE (AND STOP USING WHAT YOU DON'T NEED)

IDENTIFY THE CROWN JEWELS IN YOUR NETWORK (YOU CAN LOSE A LEG BUT NOT A HEART)

THINK CONSTITUENT

CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

CREATE VALUE