RISE OF MACHINES

Protecting The New Identities

Jens Sabitzer, CISSP

The Future: Machines

What Are Machines?

v =
argmaxb∈{Yes,No}
Pr(b) Q i Pr(ai | b)

Device

Code

Algorithm

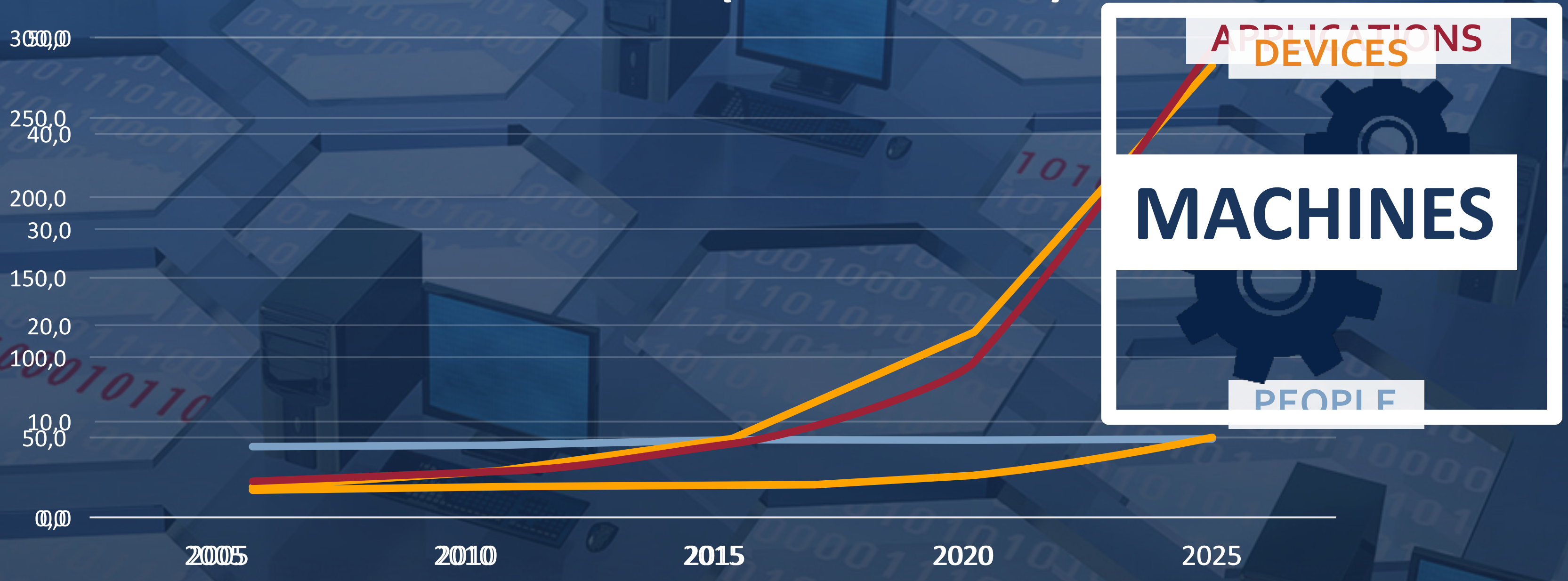
Service

Machines Growing Exponentially

Growth Factors

- Cloud
- Virtual Machines
- Containerization
- DevOps
- Mobile Devices
- Internet of Things
- Industrial IoT
- Data Access
- Privacy Laws

PROJECTED GROWTH (IN BILLIONS)

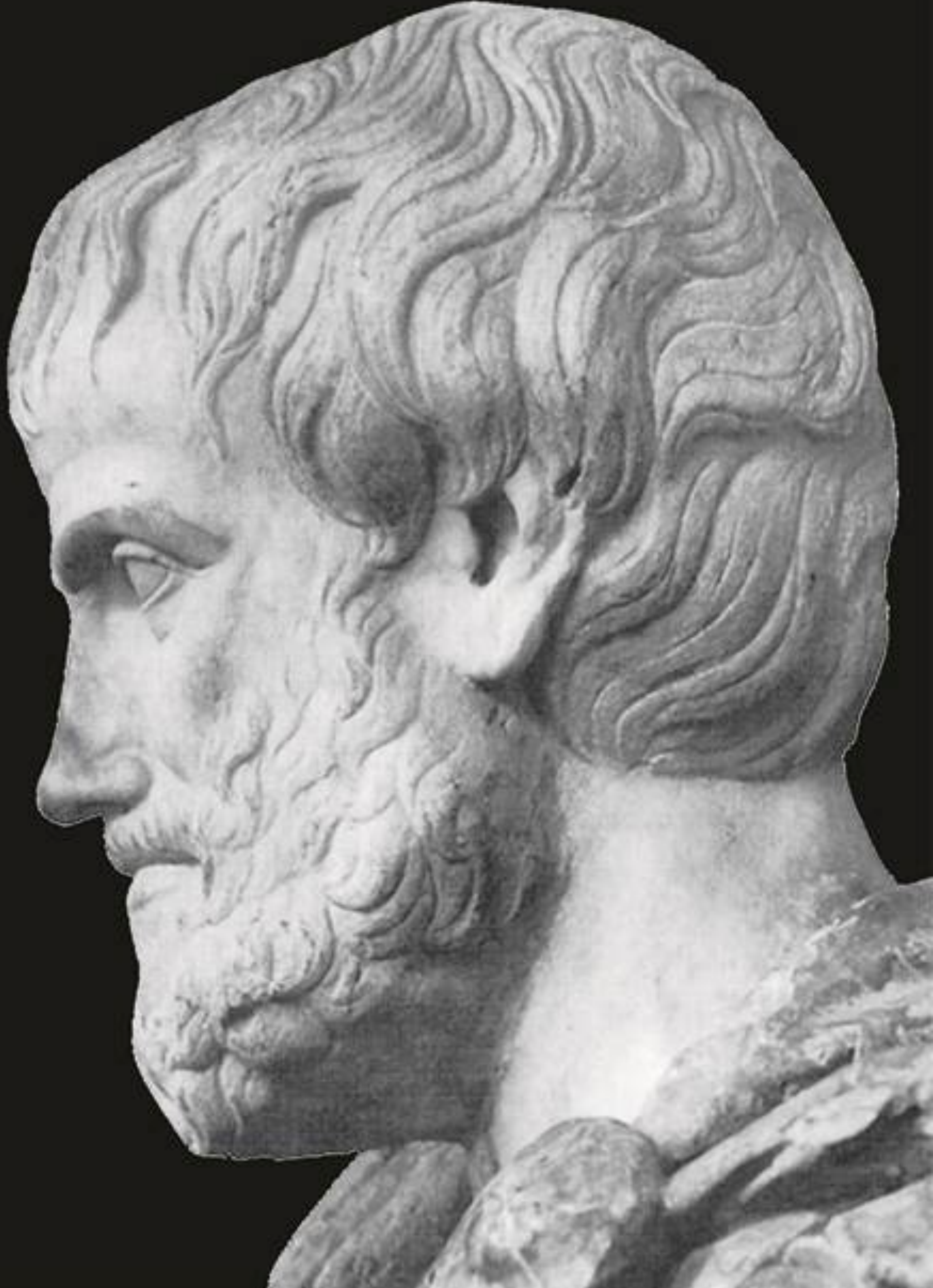


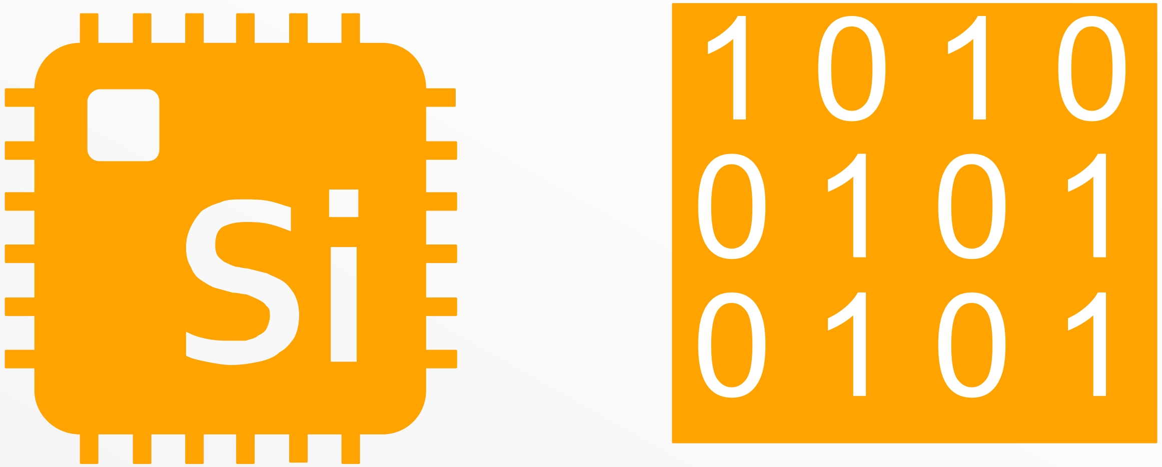
An entity without an identity cannot exist because it would be nothing

Aristotle

Law of Identity

Metaphysics, Book IV, Part 4



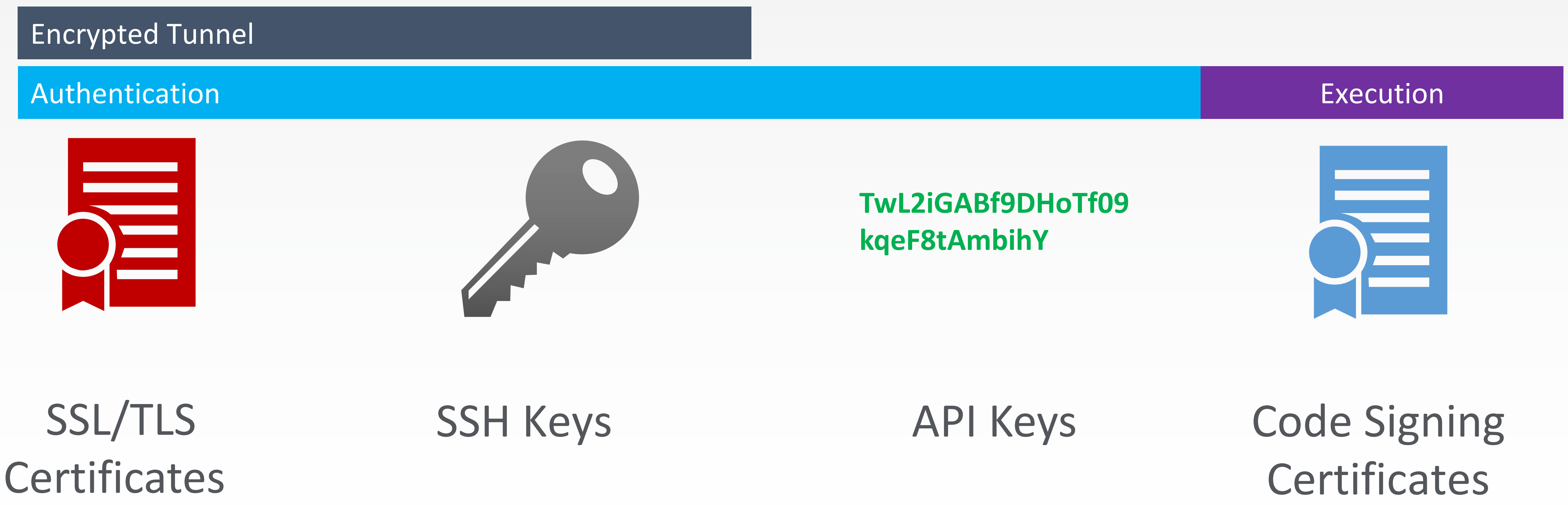


HUMANS

User name, Password, Biometric

MACHINES

What are Machine Identities?



Encrypted Tunnel

Authentication

Execution

TwL2iGABf9DHoTf09
kqeF8tAmbihY

SSL/TLS Certificates

SSH Keys

API Keys

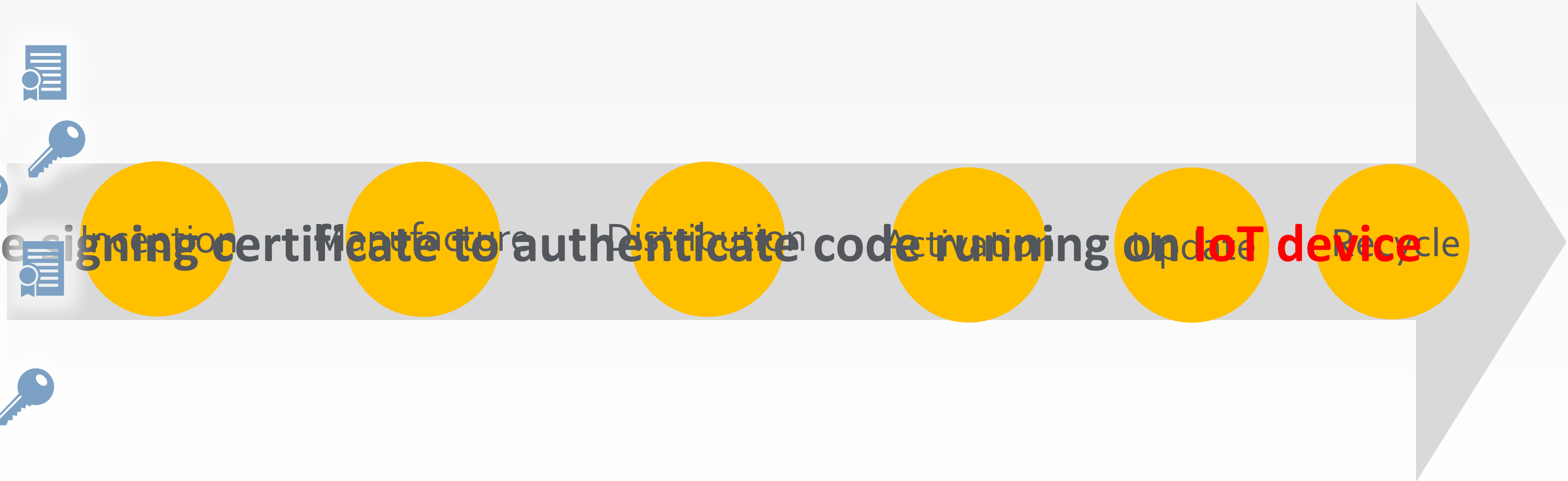
Code Signing Certificates

T50
127.116.27.251
172.229.99.114
125.201.98.217
T84
E5847
174.229.37.129
T14
250.116.74.182
T18
174.229.37.129

Role & Lifecycle of Machine Identities

SSH key for cloud-to-cloud DevOps orchestration

Code signing certificate to authenticate code running on IoT device



TLS certificate to authenticate cloud app to IoT devices

How Are We Doing?

Research by TechValidate

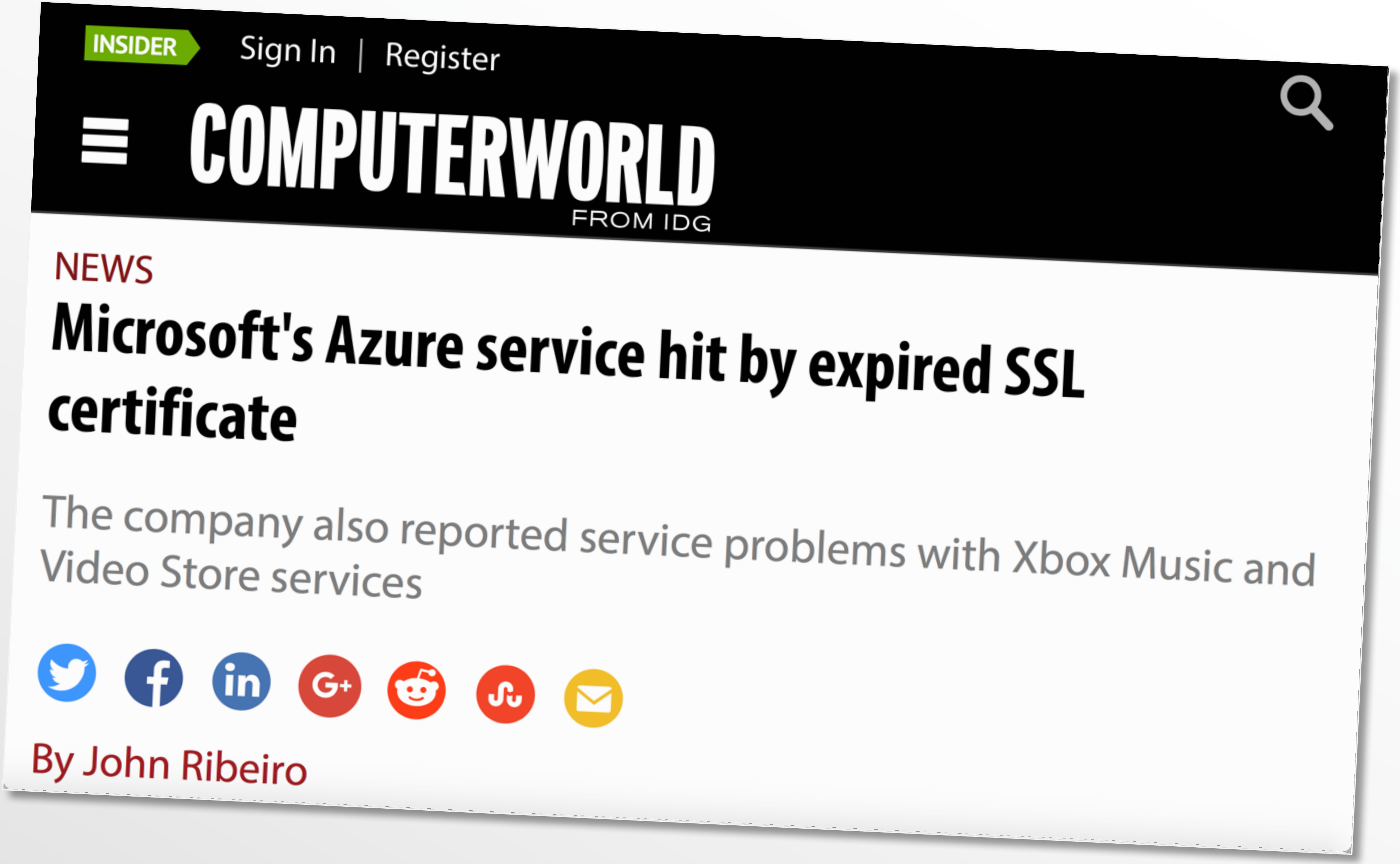
16,500 Unknown Keys & Certificates Found

On average, IT security professionals found 16,543 additional keys and certificates using Venafi that were previously unknown.

Source: TechValidate survey of 47 Venafi users

Published: **Oct. 14, 2015**

TVID: **363-53E-598**

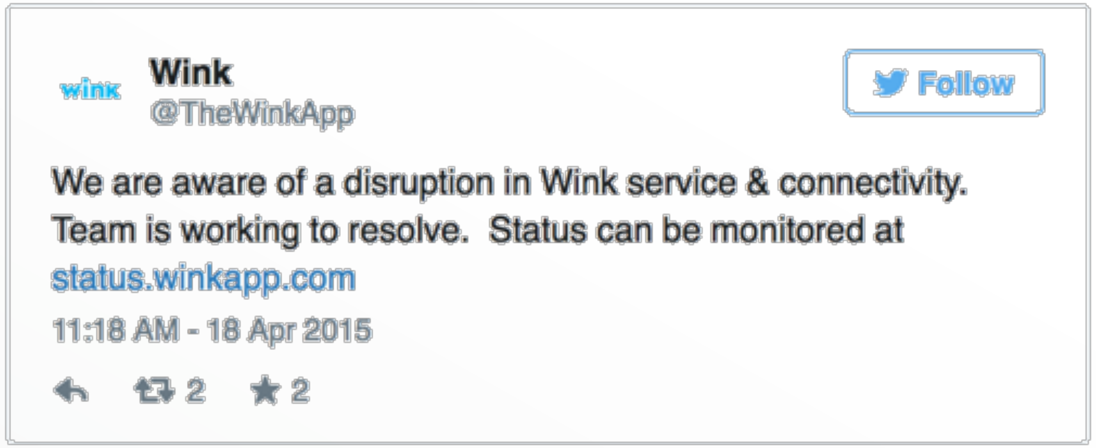


NEWS

Microsoft's Azure service hit by expired SSL certificate

The company also reported service problems with Xbox Music and Video Store services

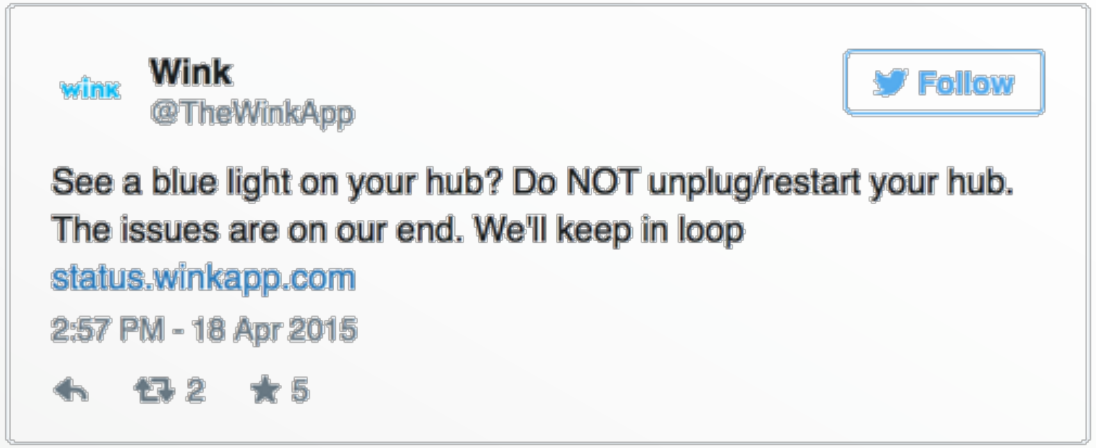
By John Ribeiro



Wink
@TheWinkApp

We are aware of a disruption in Wink service & connectivity. Team is working to resolve. Status can be monitored at status.winkapp.com

11:18 AM - 18 Apr 2015

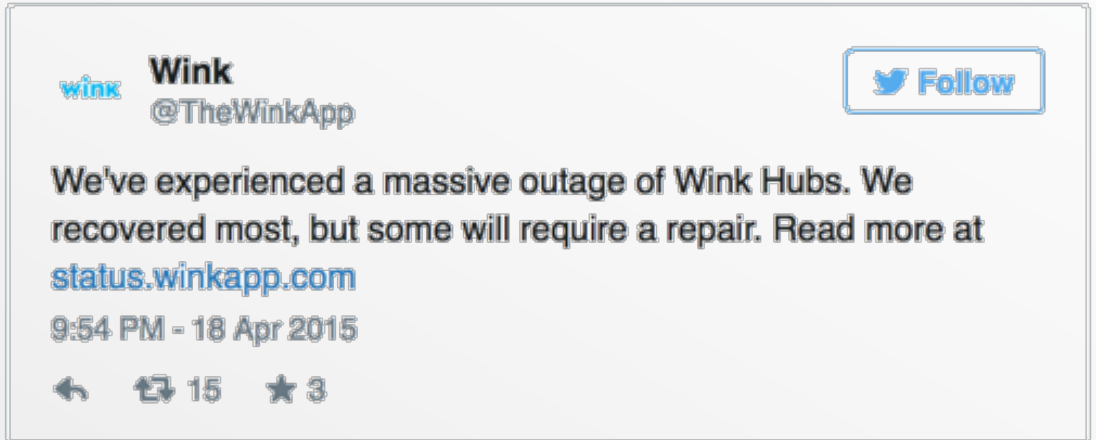


Wink
@TheWinkApp

See a blue light on your hub? Do NOT unplug/restart your hub. The issues are on our end. We'll keep in loop status.winkapp.com

2:57 PM - 18 Apr 2015

Uh-oh

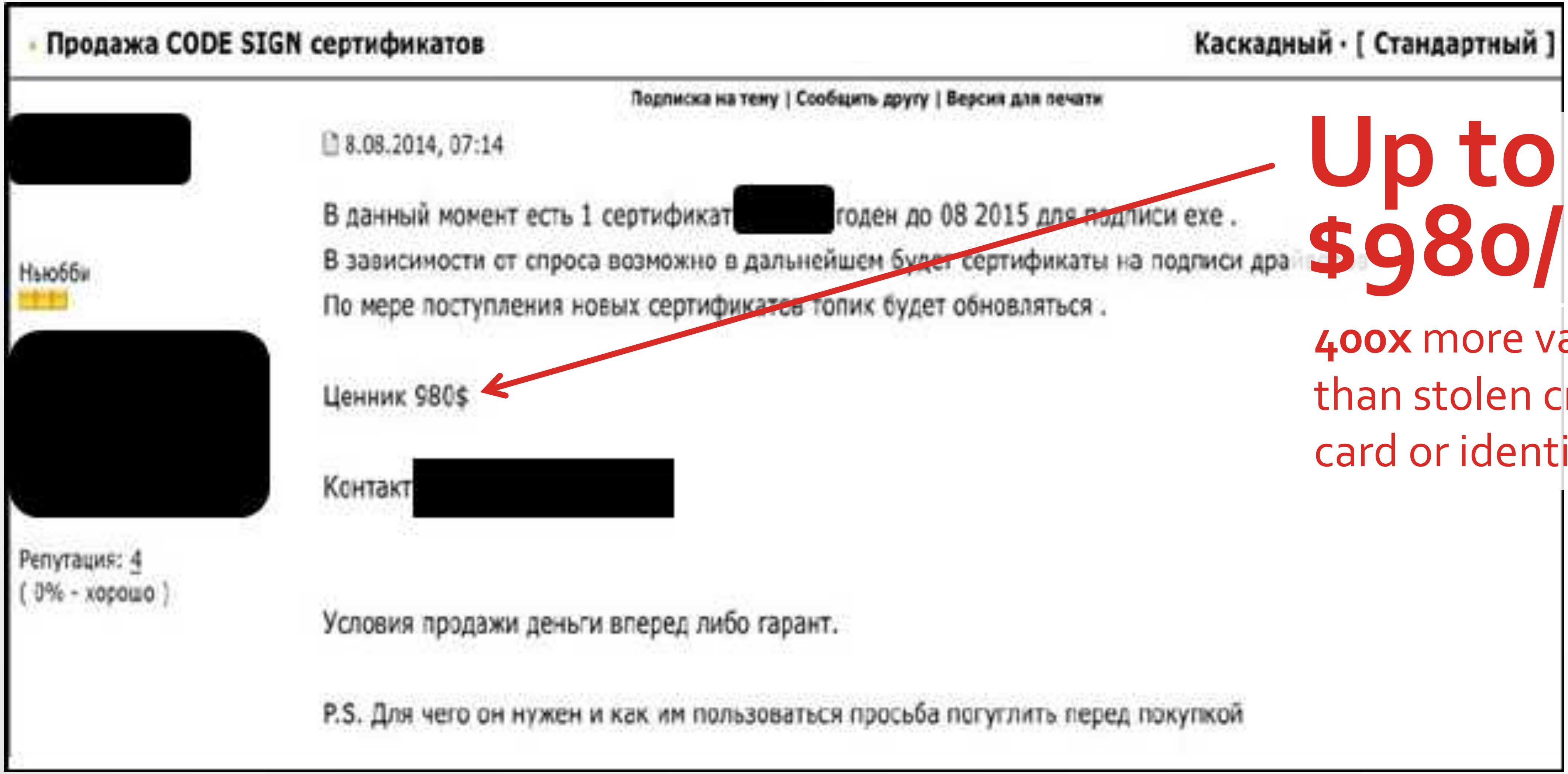


Wink
@TheWinkApp

We've experienced a massive outage of Wink Hubs. We recovered most, but some will require a repair. Read more at status.winkapp.com

9:54 PM - 18 Apr 2015

“Stealing Certificates will be the Next Big Market for Hackers”



Продажа CODE SIGN сертификатов

Каскадный · [Стандартный]

Подписка на тему | Сообщить другу | Версия для печати

[redacted]

Ньюбби

[redacted]

Репутация: 4
(0% - хорошо)

8.08.2014, 07:14

В данный момент есть 1 сертификат [redacted] годен до 08 2015 для подписи exe .
В зависимости от спроса возможно в дальнейшем будут сертификаты на подписи дра
По мере поступления новых сертификатов топик будет обновляться .

Ценник 980$

Контакт [redacted]

Условия продажи деньги вперед либо гарант.

P.S. Для чего он нужен и как им пользоваться просьба погуглить перед покупкой

Up to $980/ea

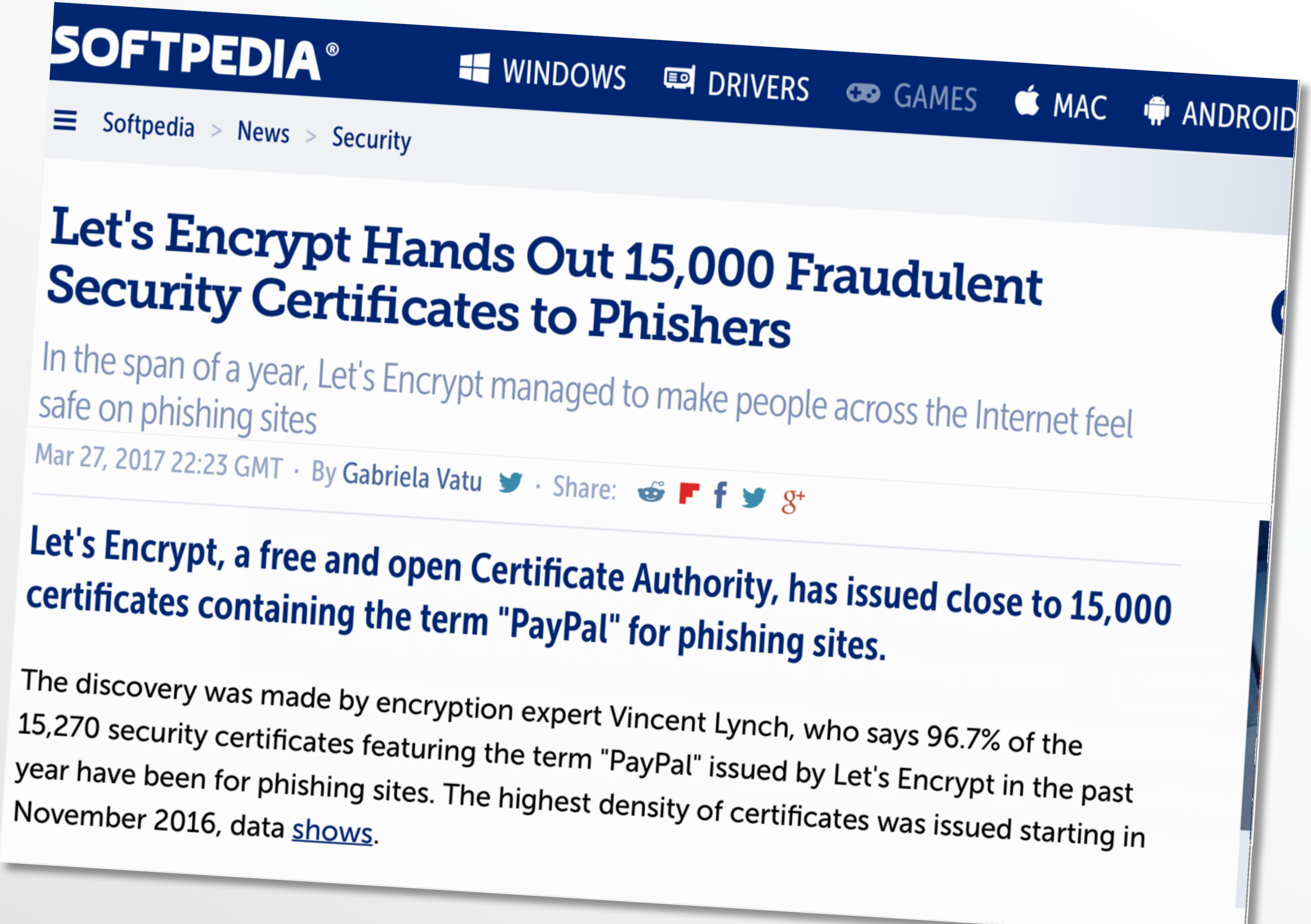
400x more valuable than stolen credit card or identity #

“70% OF MALWARE ATTACKS WILL USE SSL BY 2020”

Gartner

100 million certificates

June 2017



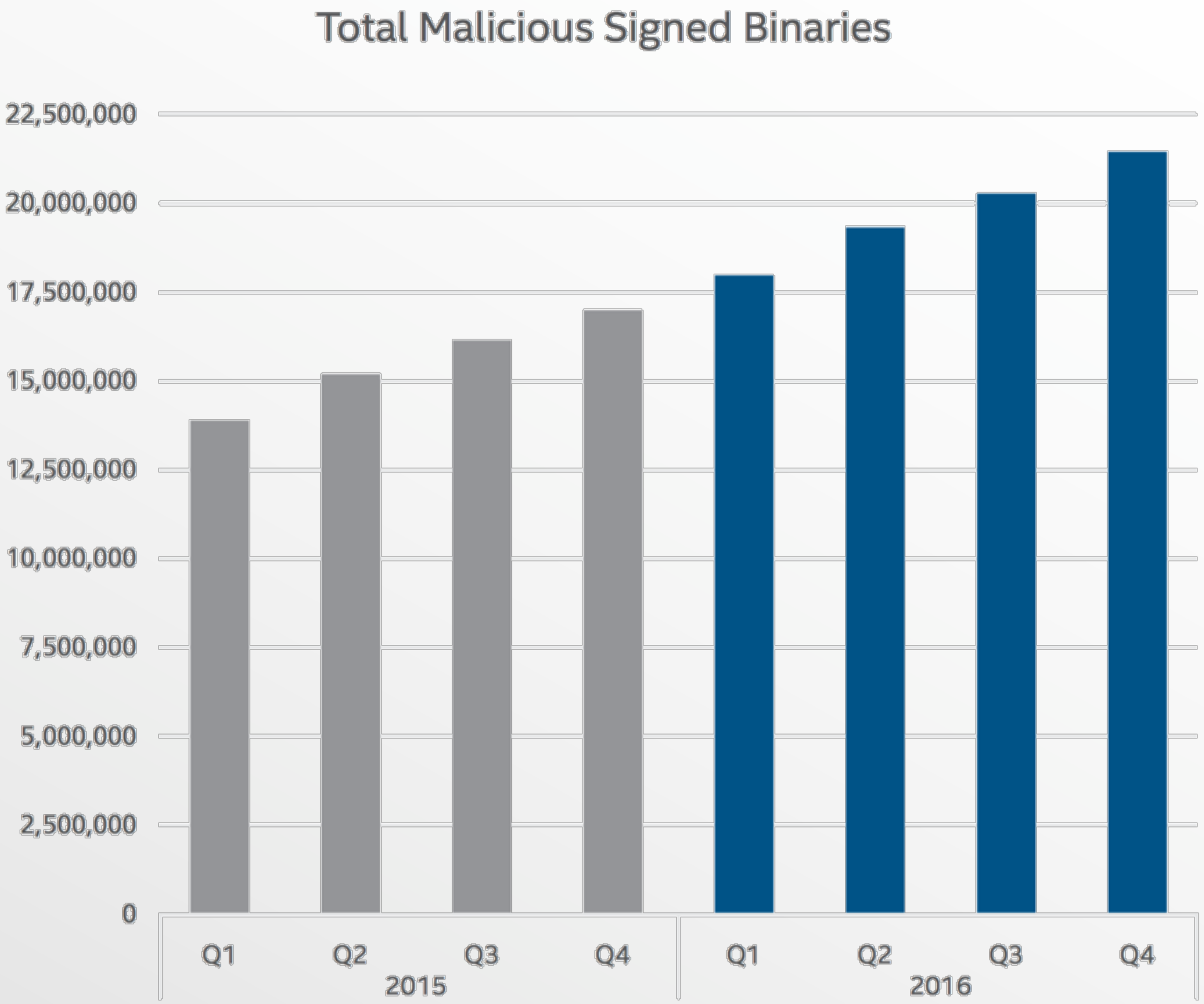
Let's Encrypt Hands Out 15,000 Fraudulent Security Certificates to Phishers

In the span of a year, Let's Encrypt managed to make people across the Internet feel safe on phishing sites

Mar 27, 2017 22:23 GMT · By Gabriela Vatu

Let's Encrypt, a free and open Certificate Authority, has issued close to 15,000 certificates containing the term "PayPal" for phishing sites.

The discovery was made by encryption expert Vincent Lynch, who says 96.7% of the 15,270 security certificates featuring the term "PayPal" issued by Let's Encrypt in the past year have been for phishing sites. The highest density of certificates was issued starting in November 2016, data shows.



McAfee™ by Intel

Would your organization tolerate

24,000 user IDs & passwords

with no awareness, policies, or control?

Would your organization tolerate

24,000 user keys & certificates

with no awareness, policies, or control?

Misuse of Machine Identities

TAKE ON TRUSTED IDENTITY

Phishing effectiveness
Malicious code execution

ESTABLISH TRUSTED IDENTITY

Create backdoors
Build privilege

RUN WITHOUT IDENTITY

Hide, stealth, cloak

BLIND TO ATTACK

One Unknown Certificate

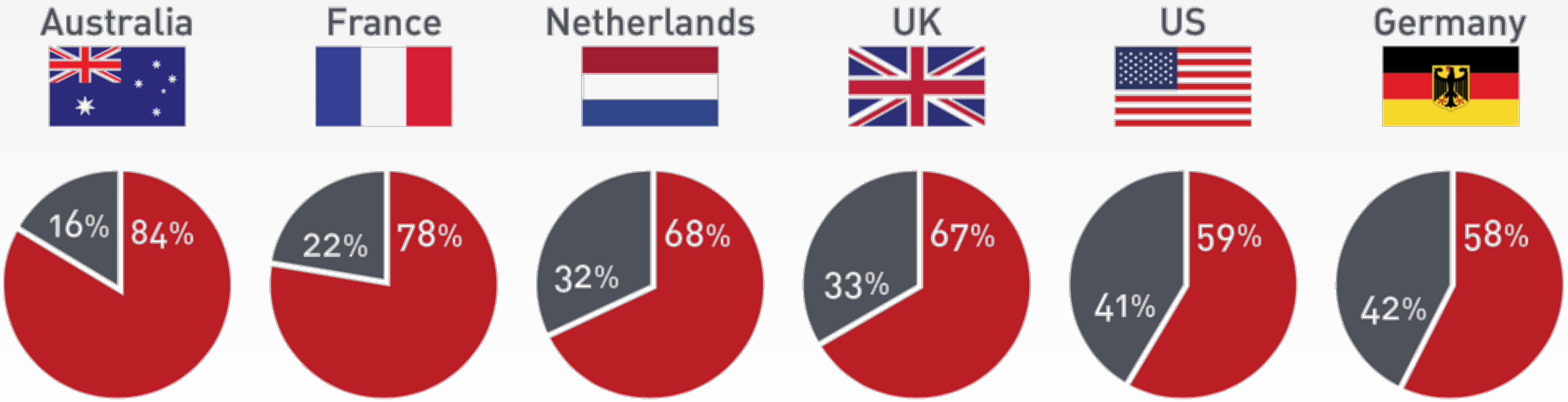
=

Encrypted tunnel

=

Can’t see what’s coming

Heartbleed: T+1 Year



RED= % NOT HEARTBLEED REMEDIATED

Weaponizing Machine Identities

2010-2012

Attacks Begin

- 2010: Blueprint - Stuxnet and Duqu
- 2011: CAs Attacked
- 2012: Online Trust Questioned by Experts

2013

Attacks Become Mainstream

- SSH & server key theft
- Code-signing certificate theft
- MITM by CA compromise

2014

Advanced Campaigns Launch

- Targeted key & certificate theft
- Sold on Underground
- Multi-year campaigns
- SSL & SSH vulnerabilities

2015

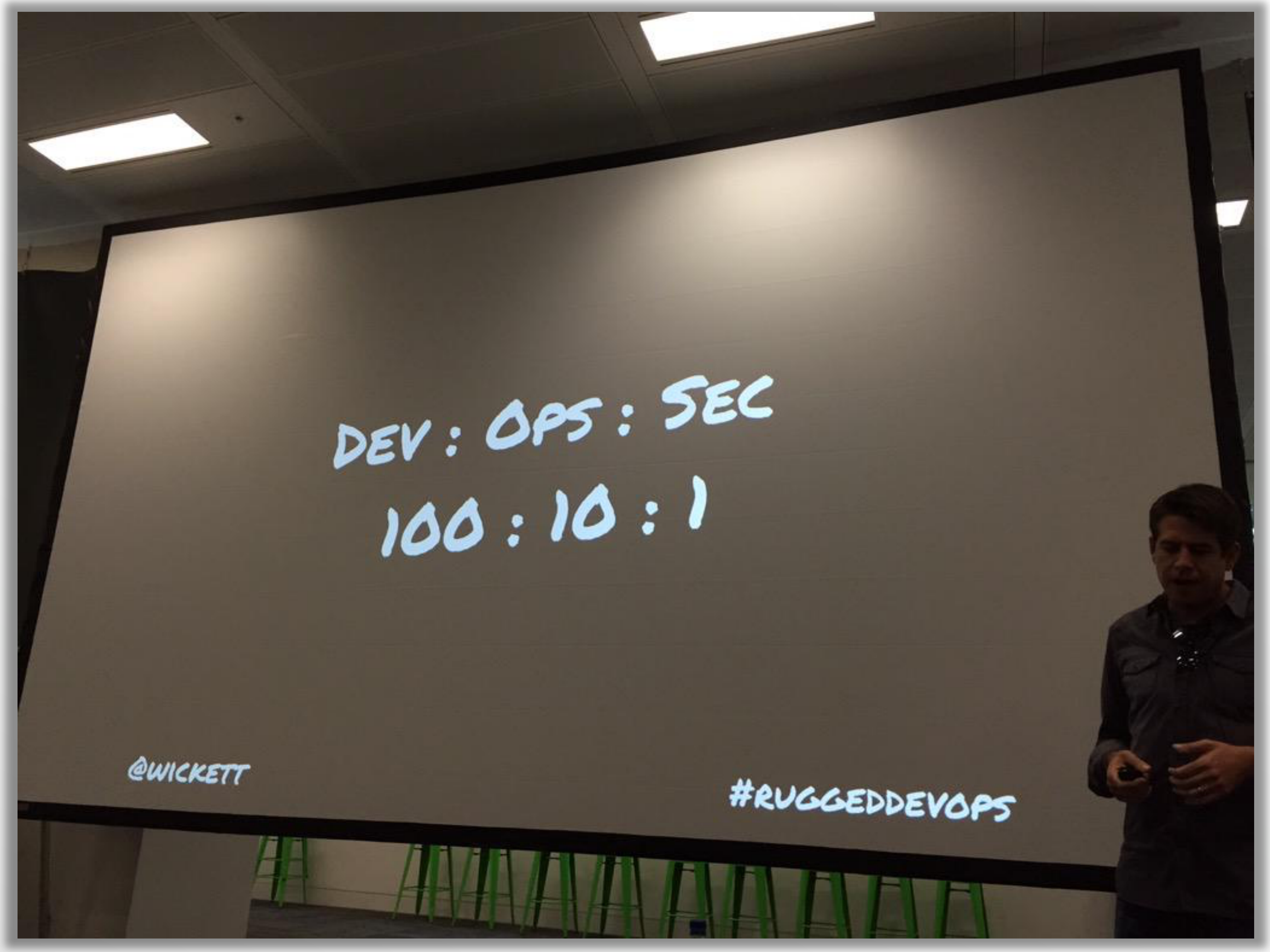
Online Trust Crumbles

- Price increases on underground
- Digitally-signed malware doubles quarterly
- SSL/TLS used to hide activity
- MitM attacks
- SSH pivoting

2016-2017

Threatscape Expands

- SSL/TLS used to bypass security
- Encrypt Everywhere grows attack surface
- SHA-1 deprecation
- SHA-1 collision succesful



DEV : OPS : SEC

100 : 10 : 1

@WICKETT

#RUGGEDDEVOPS

Traditional IT

Multi-layer

Fixed infrastructure

Fixed number of keys & cer

DevOps

Grows infinitely

Elastic and organic

10X - ∞

Global Bank

Slow IT

13,000

keys & certificates

DevOps

>100,000

keys & certificates
and growing

If not fast and easy, developers will side step security and create new vulnerabilities

Taking Action

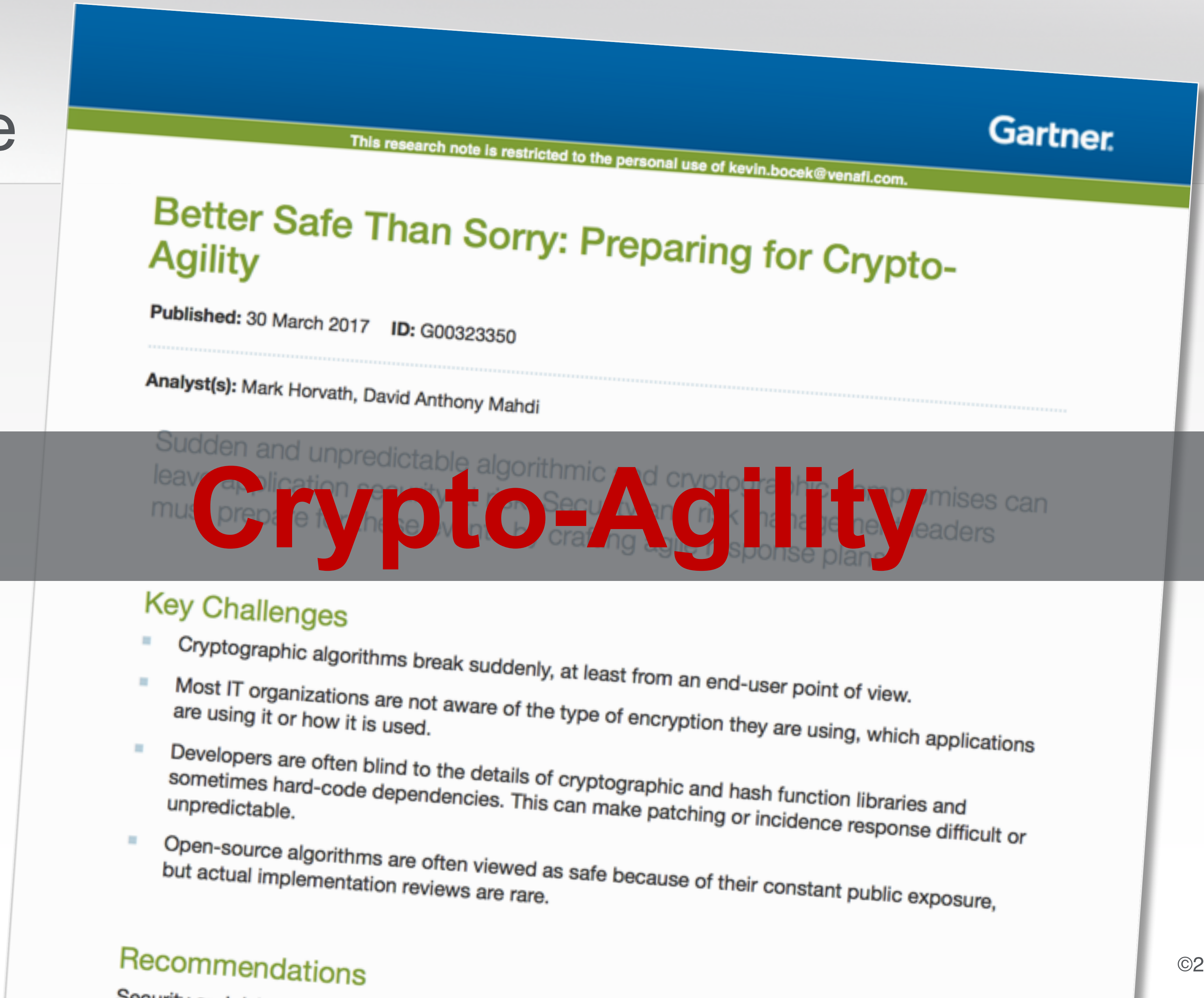
Learn More

Symantec™

CA Agility

all certificates must be replaced by 23 Oct 2018

Learn More



Gartner

This research note is restricted to the personal use of kevin.bocek@venafi.com.

Better Safe Than Sorry: Preparing for Crypto-Agility

Published: 30 March 2017 **ID:** G00323350

Analyst(s): Mark Horvath, David Anthony Mahdi

Sudden and unpredictable algorithmic and cryptographic compromises can leave application security at risk. Security and risk management leaders must prepare for these events by crafting agile response plans.

Key Challenges

- Cryptographic algorithms break suddenly, at least from an end-user point of view.
- Most IT organizations are not aware of the type of encryption they are using, which applications are using it or how it is used.
- Developers are often blind to the details of cryptographic and hash function libraries and sometimes hard-code dependencies. This can make patching or incidence response difficult or unpredictable.
- Open-source algorithms are often viewed as safe because of their constant public exposure, but actual implementation reviews are rare.

Recommendations

Crypto-Agility

Learn More

NIST

ITL BULLETIN FOR JULY 2012

Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance

Paul Turner, Venafi

William Polk, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

Elaine Barker, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

1. Executive Summary

As the use of Public Key Infrastructure (PKI) and digital certificates (e.g., the use of Transport Layer Security [TLS] and Secure Sockets Layer [SSL]) for the security of systems has increased, the certification authorities (CAs) that issue certificates have increasingly become targets for sophisticated cyber-attacks. In 2011, several public certification authorities were attacked, and at least two attacks resulted in the successful issuance of fraudulent certificates by the attackers. An attacker who breaches a CA to generate and obtain fraudulent certificates does so to launch further attacks against other organizations or individuals. An attacker can also use fraudulent certificates to authenticate as another individual or system or to forge digital signatures.

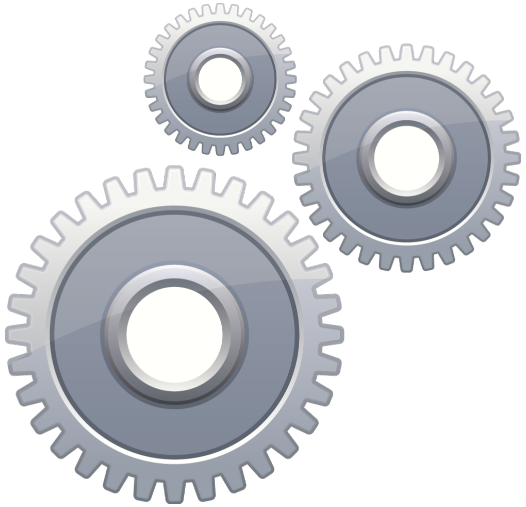
These recent attacks on CAs make it imperative that organizations ensure th
CAs and must also be prepared to respond
certifi

CA Recovery Plan

©2017 Venafi

Gain Intelligence

Set, Enforce a Policy

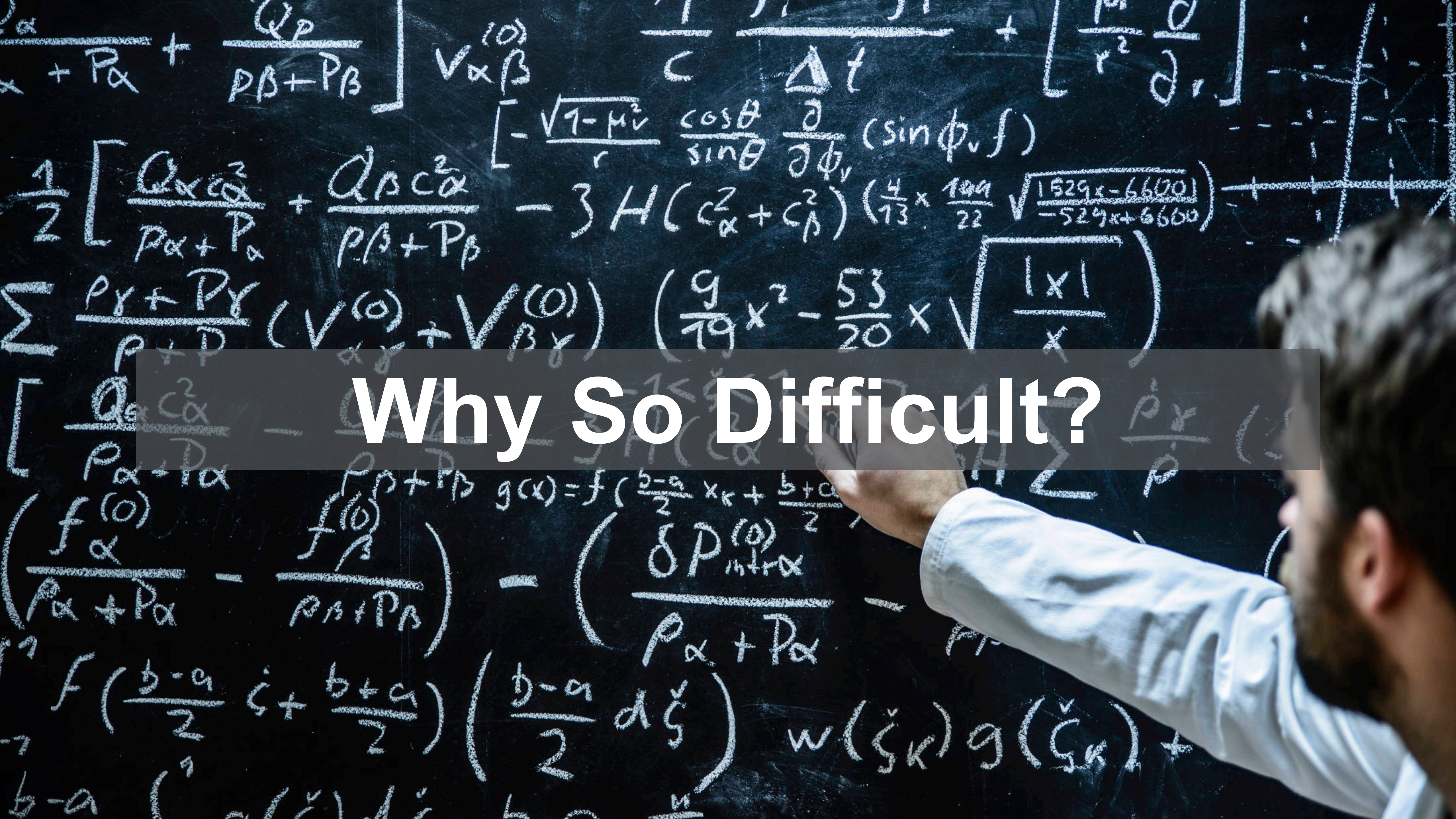


Automate Operations

Good News: this can be business as usual process

Starting Change

- Who is responsible?
- How do we enforce policies?
- How do we monitor Let's Encrypt and other CAs?
- How will we automate for IoT, DevOps, cloud?
- How would we respond to?
  - CA compromise
  - SSH key theft
  - Symantec replacement
- And keeping asking more…



Why So Difficult?

Danke