
29th ANNUAL
FIRST
CONFERENCE
SAN JUAN
PUERTO RICO
JUNE 11-16, 2017
FIGHTING PIRATES AND PRIVATEERS
WWW.FIRST.ORG

GOING UNDETECTED:

HOW CYBERCRIMINALS, HACKTIVISTS, AND NATION STATES MISUSE DIGITAL CERTIFICATES

Kevin Bocek

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO

The Future: Machines

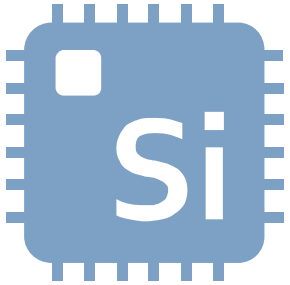
The future is machines

Adversaries exploiting machine identities

Good news: guidance exists

- Reduce risk
- Build in agility
- Respond faster

What Are Machines?



Device

Code

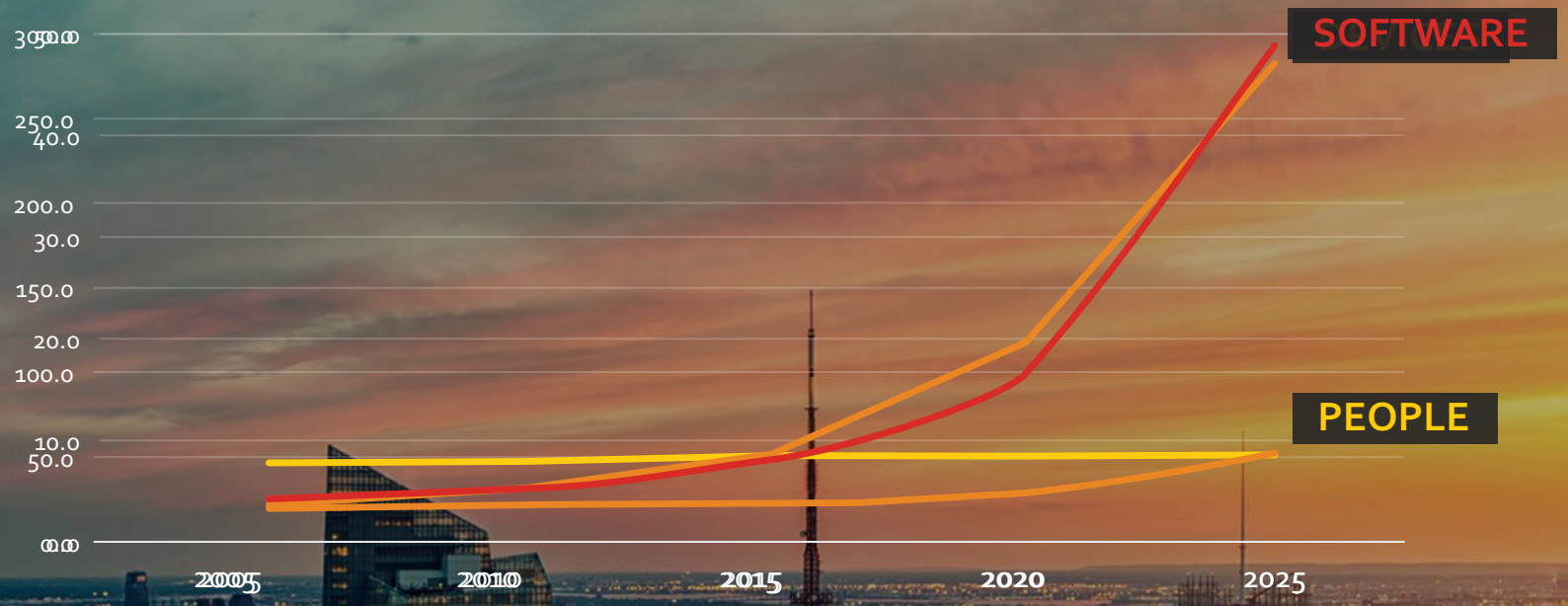
v = argmaxb∈{Yes,No}
Pr(b) Q i Pr(ai | b)

Algorithm

Service

SOFTWARE AND DEVICES EXPLODING

(EST. IN BILLIONS)

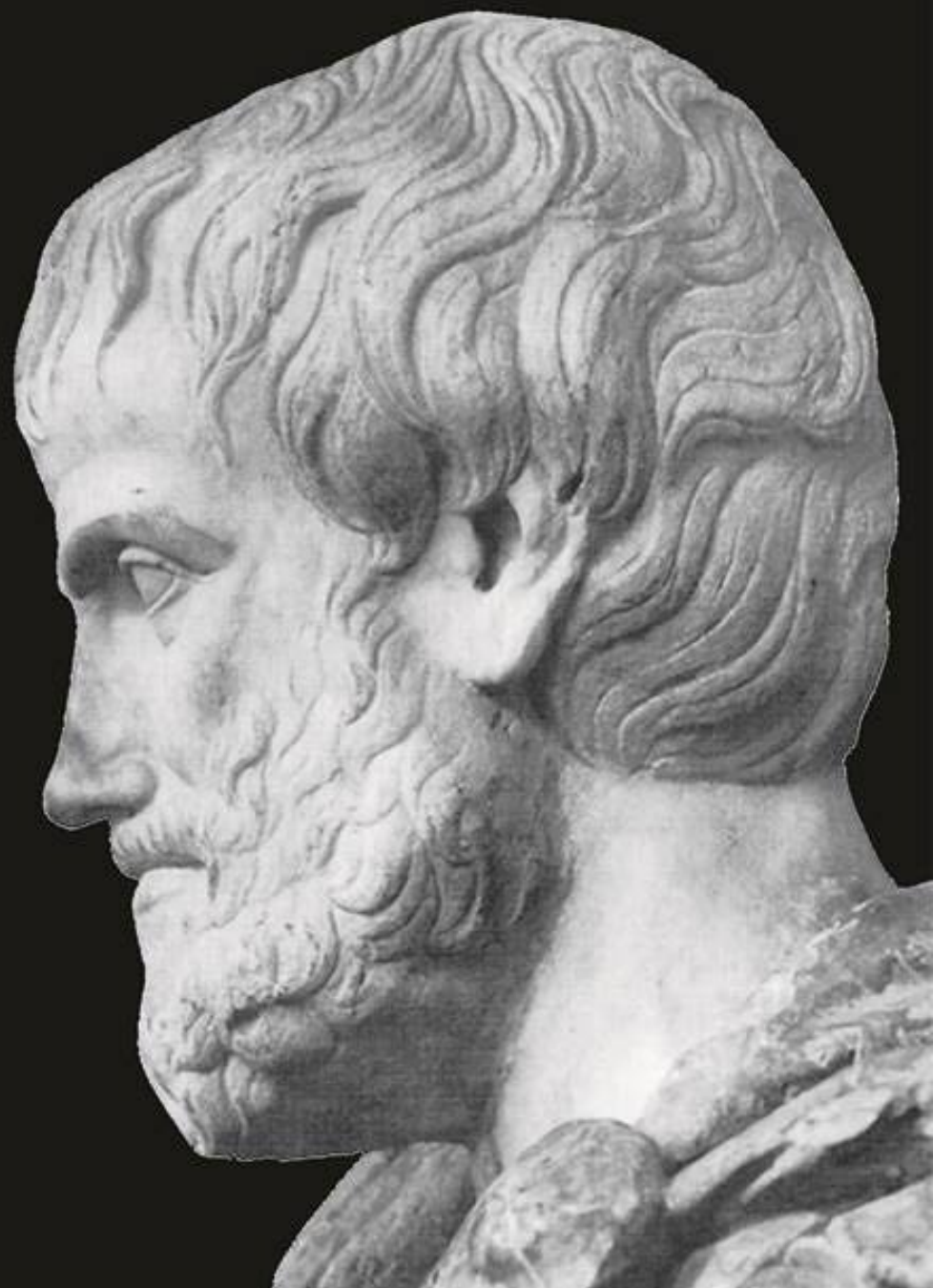


An entity without an identity cannot exist because it would be nothing

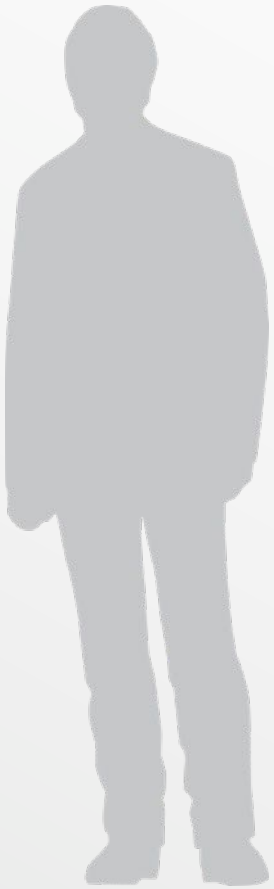
Aristotle

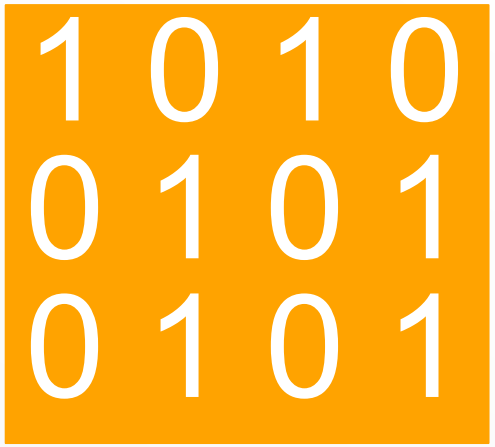
Law of Identity

Metaphysics, Book IV, Part 4



Machine Identities





HUMANS

User name, Password, Biometric

MACHINES

What are Machine Identities?

Encrypted Tunnel

Authentication

Execution

SSL/TLS Certificates

SSH Keys

TwL2iGABf9DHoTf09
kqeF8tAmbihY

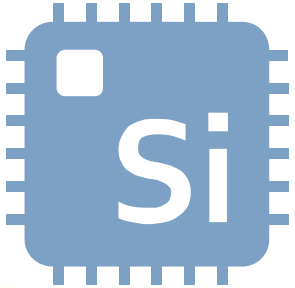
API Keys

Code Signing Certificates

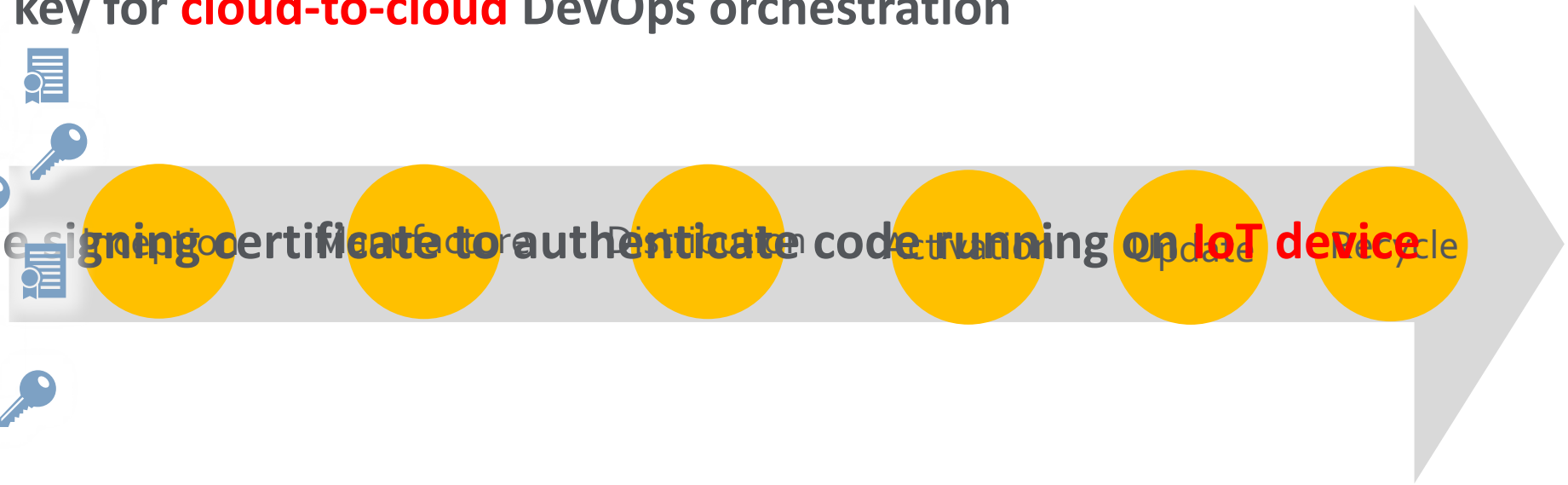

CD-8LCA
CD-8LCA


T50
127.116.27.251
E5847
T-44
T84
T14
T53
T18
174.229.37.129
172.229.99.114
125.201.98.217

Role & Lifecycle Leaves Identities Vulnerable



SSH key for **cloud-to-cloud** DevOps orchestration



TLS certificate to authenticate **cloud app** to **IoT devices**

Misuse of Machine Identities

TAKE ON TRUSTED IDENTITY

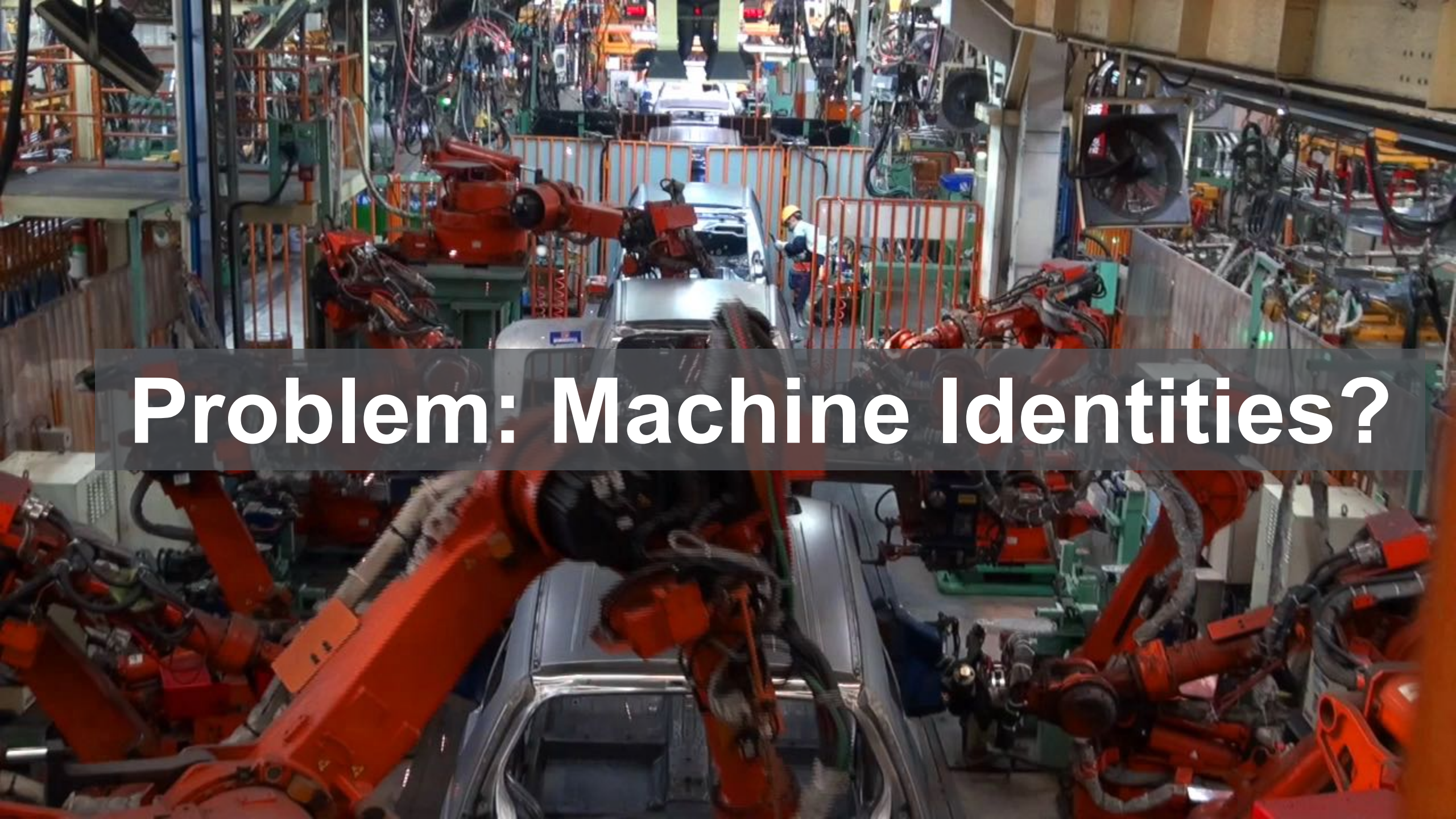
Phishing effectiveness
Malicious code execution

ESTABLISH TRUSTED IDENTITY

Create backdoors
Build privilege

RUN WITHOUT IDENTITY

Hide, stealth, cloak



Problem: Machine Identities?

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

VENAFI

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**

Would your organization tolerate

24,000 user IDs & passwords

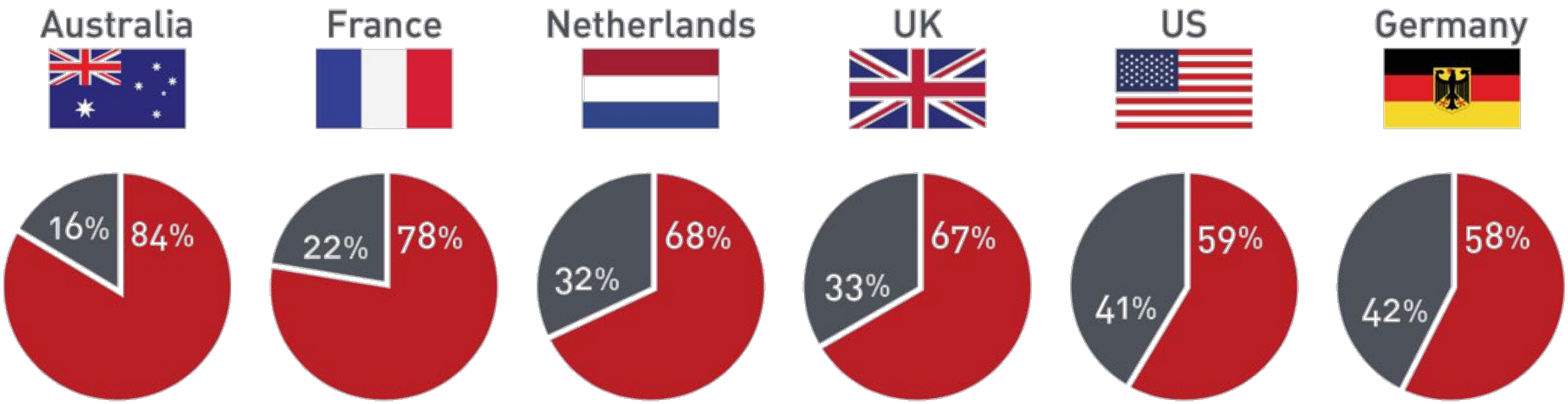
with no awareness, policies, or control?

Would your organization tolerate

24,000 user keys & certificates

with no awareness, policies, or control?

Heartbleed: T+1 Year



RED= % NOT HEARTBLEED REMEDIATED

Take On Trusted Identity

Louis Motorrad | Bekleic

louis.de

Website identification

GeoTrust Global CA has identified this site as

www.louis.de

Your connection to the server is encrypted.

Should I trust this site?

Bestelltelefon: 040 - 734 193 60

2 J

otorrad & Freizeit

Mein Bike

Sale % Markenshops Service

Top-Marken bei Louis

Louis Motorrad | Bekleic

louis.fail

Kostenloser Rückversand

Bestelltelefon: 040 - 734 193 60

2 J

FUN COMPANY Louis

Europas Nr.1 für Motorrad & Freizeit

Suchbegriff

Mein Bike

Bekleidung & Helme Technik & Freizeit Sale % Markenshops Service

Sie sind hier: Startseite

Top-Marken bei Louis

Louis Motorrad | Bekleid

louis.de

Kostenloser Rückversand | Bestelltelefon: 040 - 734 193 60 | 2 J

FUN COMPANY Louis

Europas Nr.1 für Motorrad & Freizeit

Suchbegriff | Mein Bike

Bekleidung & Helme | Technik & Freizeit | Sale % | Markenshops | Service

Sie sind hier: Startseite

Top-Marken bei Louis

cardo | SHOEI | TOMTOM | rukka

Louis Motorrad | Bekleid

louis.fail

Website identification

DST Root CA X3 has identified this site as

louis.fail

Your connection to the server is encrypted.

Should I trust this site?

Bestelltelefon: 040 - 734 193 60 | 2 J

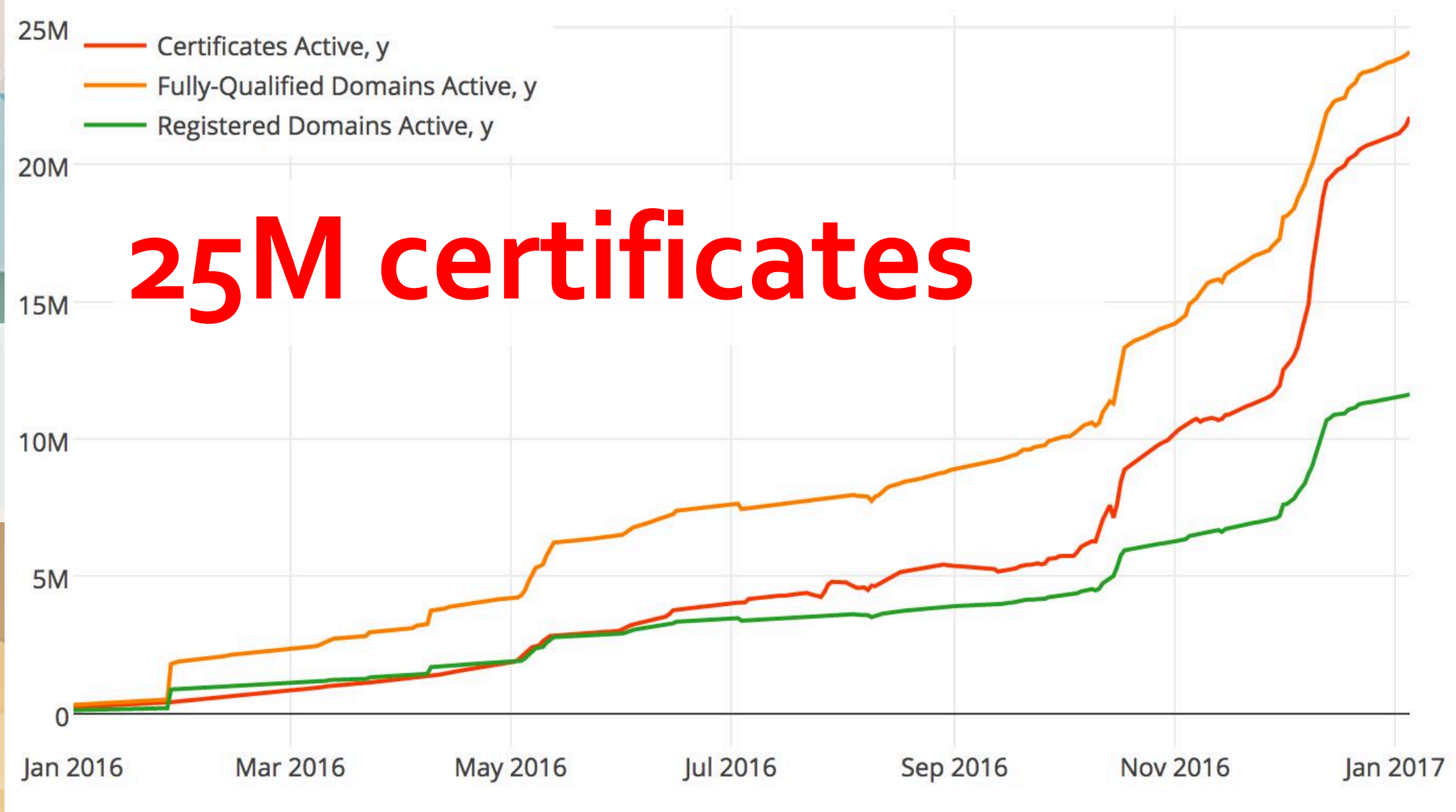
Europas Nr.1 für Motorrad & Freizeit

Mein Bike

Sale % | Markenshops | Service

Top-Marken bei Louis

cardo | SHOEI | TOMTOM | rukka



25M certificates

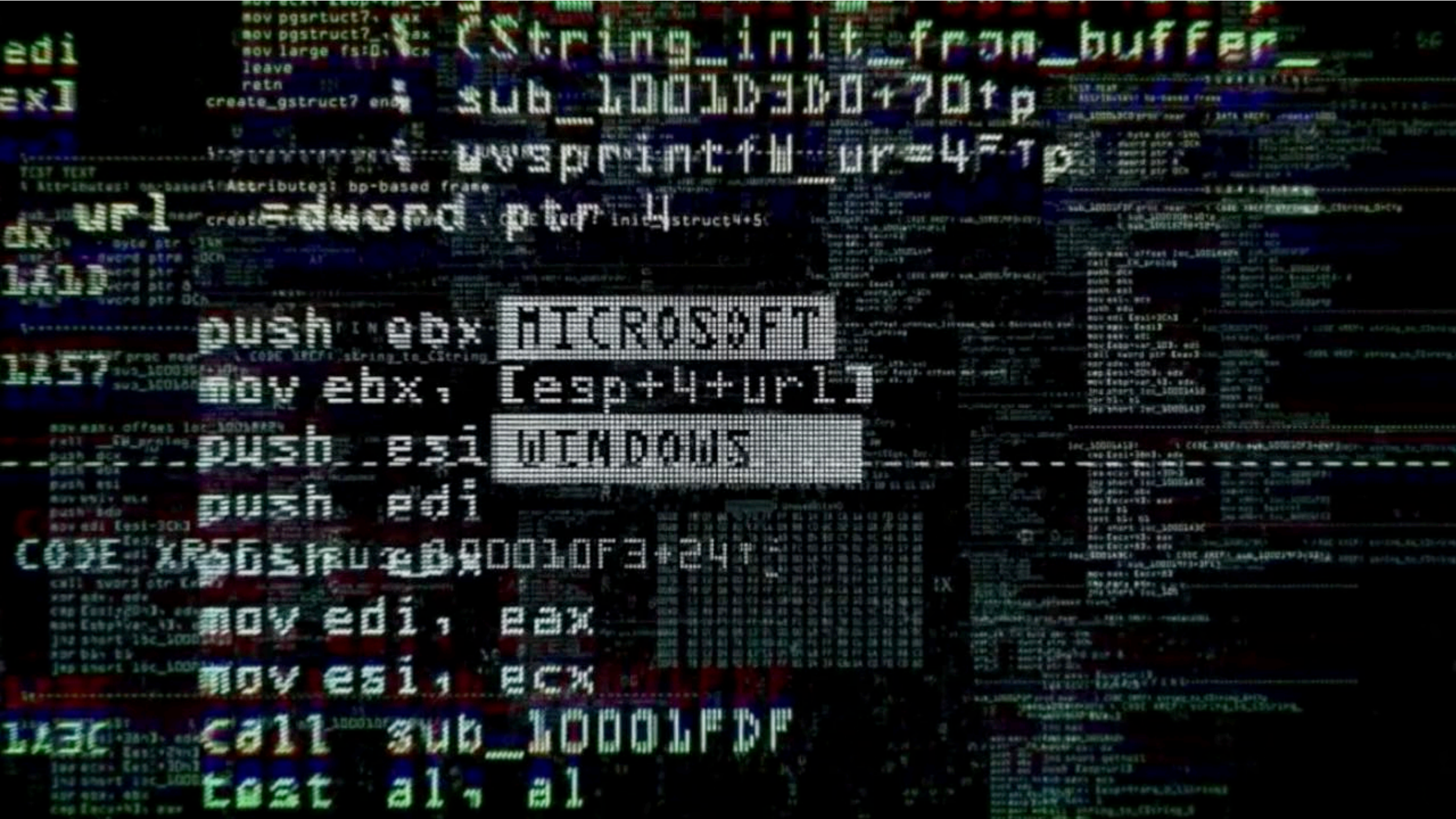
Let's Encrypt Hands Out 15,000 Fraudulent Security Certificates to Phishers

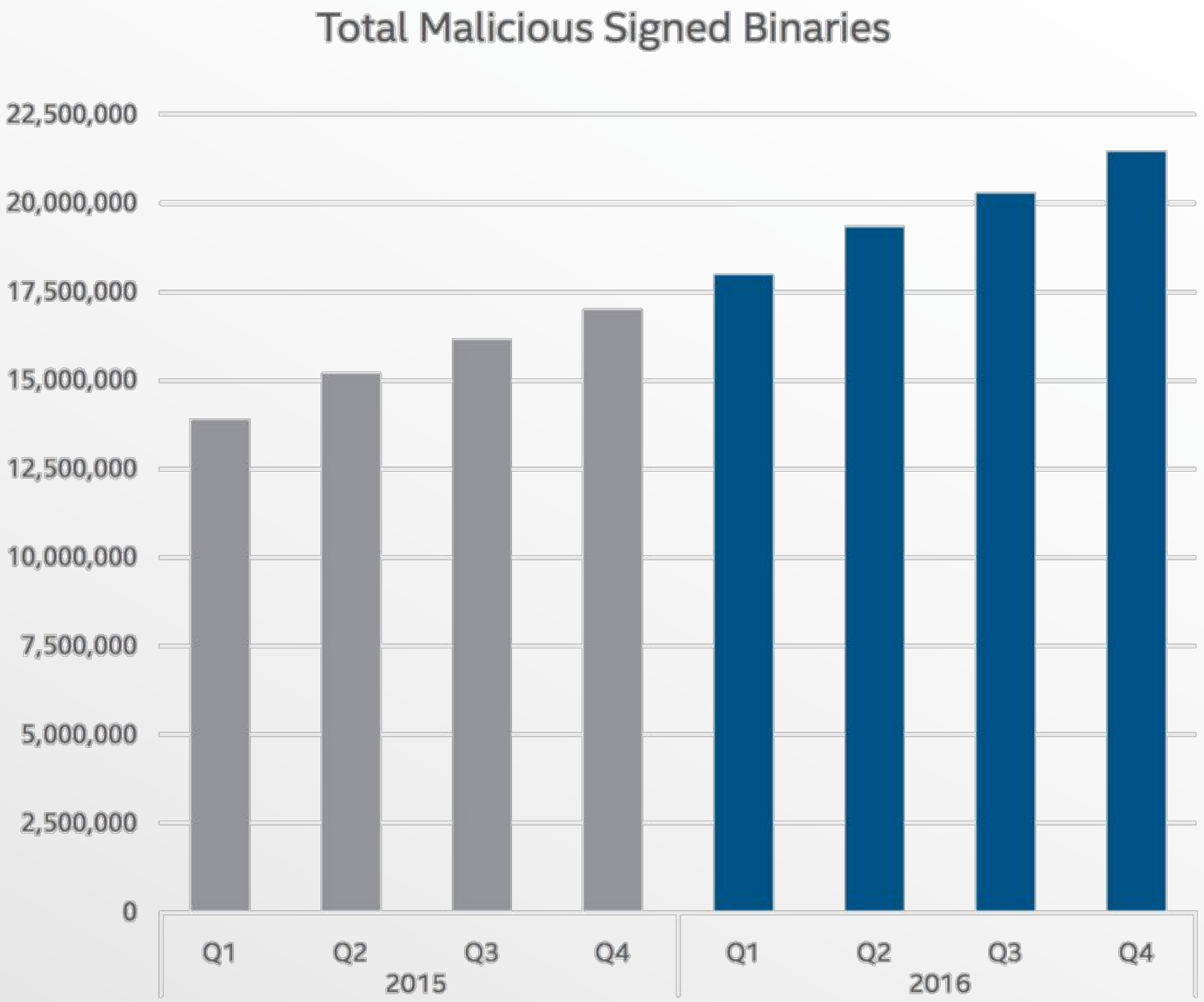
In the span of a year, Let's Encrypt managed to make people across the Internet feel safe on phishing sites

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

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

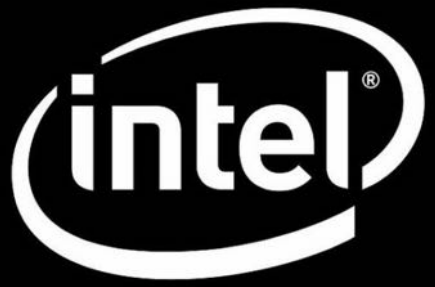
The discovery was made by encryption expert Vincent Lynch, who says 96.7% of the 15,270 security certificates featuring the term "PayPal" issued by Let's Encrypt in the past year have been for phishing sites. The highest density of certificates was issued starting in November 2016, data shows.


CString_init_from_buffer_
sub_10013310+70↑p
dword ptr 4
push ebx
MICROSOFT
mov ebx, [esp+4+url]
push esi
WINDOWS
push edi
mov edi, eax
mov esi, ecx
call sub_10001FBF
test al, al



McAfee™ by Intel

“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 будет 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 #

SenseCy
Sensing Cyber

Establishing a trusted identity

MANDIANT®

APT1

Exposing One of China's Cyber Espionage Units

CONTENTS

MANDIANT®

APT1

Exposing One of China's Cyber Espionage Units

APPENDIX F: APT1 SSL CERTIFICAT

For the full report visit
http://www.mandiant.com/apt1

APPENDIX F: APT1 SSL CERTIFICATES

The following self-signed X.509 certificates are used by APT1 to encrypt malware communications using SSL. Detection of these SSL certificates may indicate an APT1 malware infection.

VIRTUALLYTHERE

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Some-State, O=www.virtuallythere.com, OU=new, CN=new
        Validity
            Not Before: Oct 23 03:25:49 2007 GMT
            Not After : Oct 22 03:25:49 2008 GMT
        Subject: C=US, ST=Some-State, O=www.virtuallythere.com, OU=new, CN=new
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:ee:48:13:76:f1:76:4b:6a:fe:6d:8c:5e:60:44:
                    19:b1:0a:b1:9e:bb:63:80:8f:c8:43:c8:73:ae:77:
                    4e:16:01:4e:8f:88:f8:a2:8c:4d:2e:b2:3d:6b:bd:
                    2e:cc:1b:b0:c3:5d:d6:a6:bc:1e:1a:31:b2:27:84:
                    64:9c:0b:b7:1e:b0:5e:82:96:e8:71:f6:ca:95:cf:
                    e1:40:bd:45:05:94:25:74:a0:90:ce:61:b9:8e:ba:
                    ed:aa:62:d4:10:79:68:eb:fb:31:63:0c:7b:11:2d:
                    8f:cf:57:a8:c4:6c:fd:77:c4:04:f5:46:84:e4:24:
                    c6:fe:dc:3a:06:9c:3e:ed:f9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                1B:C5:98:18:EB:D2:1F:3A:5B:F9:07:E0:BF:4E:C5:59:9E:FD:51:29
            X509v3 Authority Key Identifier:
                keyid:EA:D7:8A:29:DB:FB:0A:0C:C0:85:B3:BA:8A:C3:D7:80:95:26:11:90
                DirName:/C=US/ST=Some-State/O=www.virtuallythere.com/OU=new/CN=new
                serial:F2:1E:60:49:18:68:08:B6
    Signature Algorithm: sha1WithRSAEncryption
        b8:2c:50:58:a8:29:ce:d1:f3:02:a3:0c:9b:56:9f:45:24:f1:
        48:d3:53:88:d7:2e:61:67:aa:08:e4:7d:d5:50:62:ae:00:d5:
        1a:91:61:01:94:5e:ab:62:e8:53:a5:0d:6a:f4:41:81:ee:2b:
        60:8d:e2:a6:3a:12:2d:aa:08:a5:5a:f4:d2:9e:b2:43:38:57:
        f1:c1:45:54:33:d1:05:8c:e4:37:ad:00:a8:b3:92:3f:2d:21:
        a0:20:ea:0f:48:05:9f:2a:2c:88:da:eb:8b:12:bb:1d:73:85:
        4d:be:7e:36:ac:ad:6b:b4:ae:17:bf:06:d2:df:cd:a9:28:69:
        28:9e
```

IBM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 290 (0x122)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Some-State, O=Internet Widgits Pty Ltd, CN=IBM
```

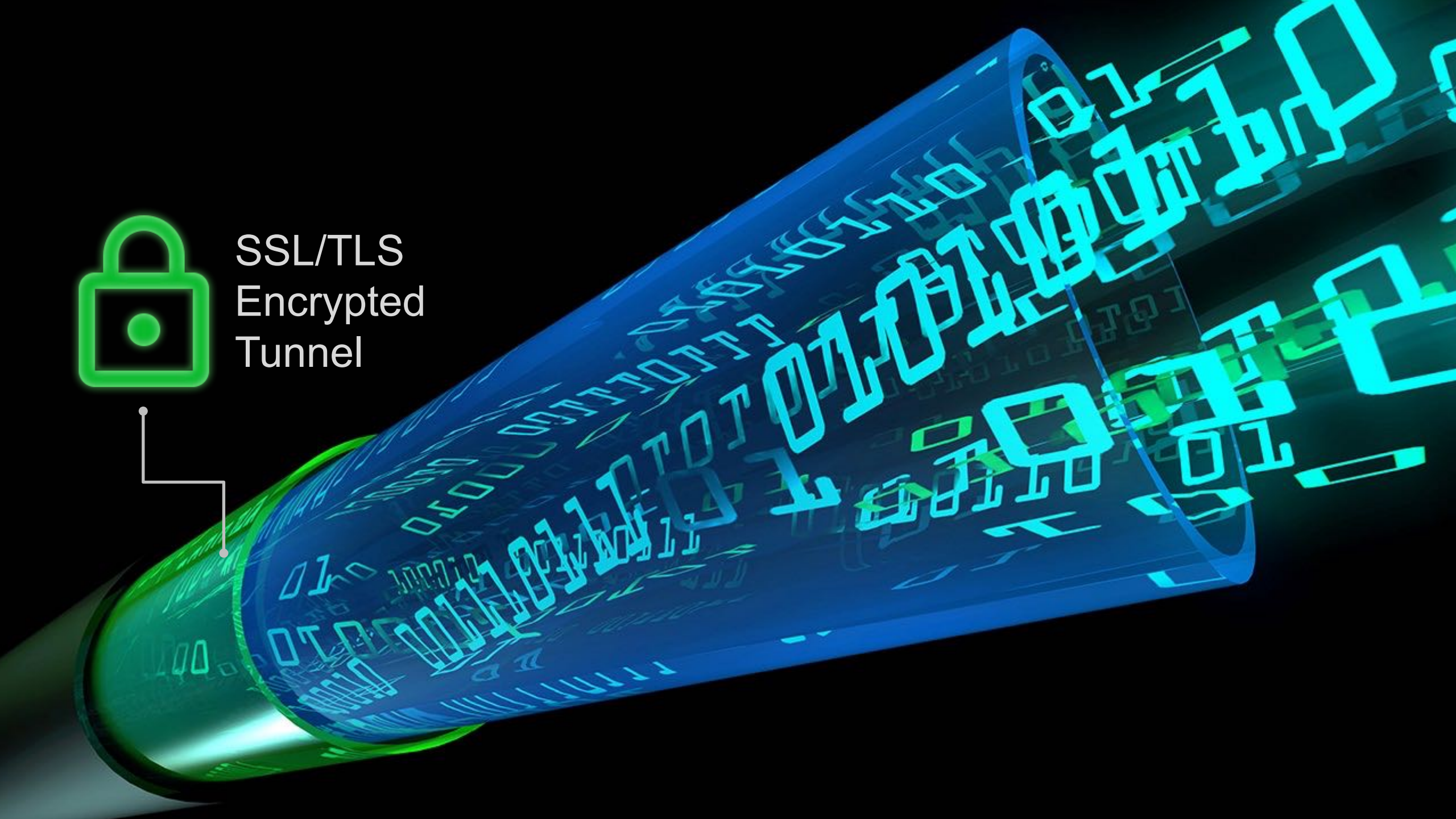
As you can see in Figure 4, this version of Dropbear SSH will authenticate the user if the password passDs5Bu9Te7 was entered. The same situation applies to authentication by key pair – the server contains a pre-defined constant public key and it allows authentication only if a particular private key is used.


```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAsrGnWG3XPW4tO8tRLhF+XQyuM5ZcL19tIsnlMyIUXwp
tcU29hGpzMWVmbAy+18EEEXKtyXIlxOKqp7CWgEJWWxjsvXKB66Gp/sVcizX+qbV2P0PfVMRwZ144Ui
0ffrpGxWMOnp7rrByANQSPdGtJ1Q/yqqFFgiM2u7i1LsREQHSGsV6Lib8krnf0BrcwQ08MD3q7tNq3H
3FEt0LPithBiCpRTuA9emsowt3gtVo745Qt1GVChYLA9GilmVmBO49HAnceZA9bVFA58Keq3Jy5W1DU
v3HoWJkWBHkUn2IH1LSKurVr/xjNEi9Hez7uQP9j44xk/V/kA9Kh4E3czOCDxQ== rsa-key-201311
```


Figure 5 – The embedded RSA public key in SSH server

Every business and government has the same lack of awareness and control over SSH keys


Run Without An Identity


SSL/TLS
Encrypted
Tunnel

"70% OF MALWARE ATTACKS WILL USE SSL BY 2020"

Gartner®

LESS THAN 20%

Of Organizations with a FW, IPS/IDS, or UTM decrypt SSL/TLS traffic

Gartner®

VENAFI

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**

BLIND TO ATTACK

One Unknown Certificate

=

Encrypted tunnel

=

Can’t see what’s coming

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

Preparing Your Plans

Gartner

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 and risk management leaders must prepare for these events by crafting agile response plans.

Crypto-Agility

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

Security leaders

Crypto-agility

Recommendations

Security and risk management leaders responsible for application security:

- Build crypto-agility into application development or application procurement workflow. Ask vendors specifically about how security incidents are communicated and who is responsible for incident response.
- Inventory the applications that use cryptography, thereby evaluating your dependence on such algorithms. This will give your organization a way to scope the impact of a break, and allow you to determine the risk to specific applications and prioritize incident response plans accordingly.
- Include cryptographic alternatives and an algorithm swap-out procedure in your incident response plans.

NIST

CA Recovery Plan

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

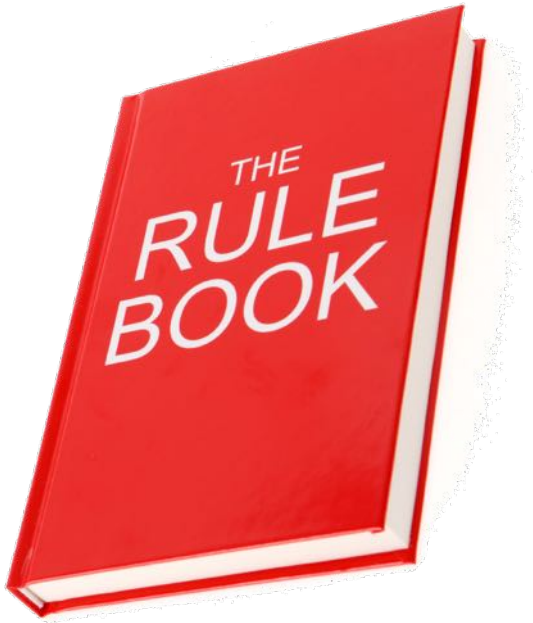
Elaine Barker, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

1. Executive Summary

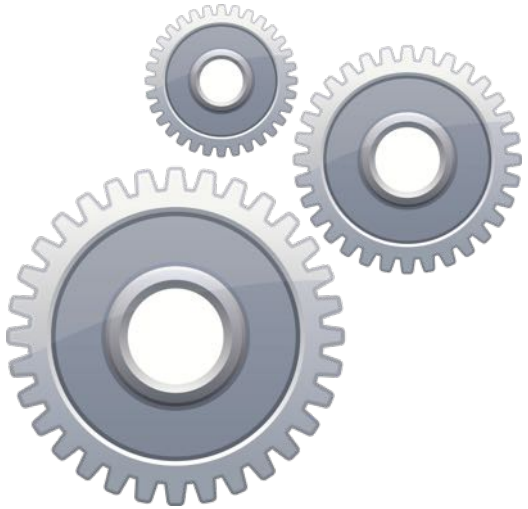
As the use of Public Key Infrastructure (PKI) and digital certificates (e.g., the use of Transport Layer Security [TLS] and Secure Sockets Layer [SSL]) for the security of systems has increased, the certification authorities (CAs) that issue certificates have increasingly become targets for sophisticated 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
CAs and must also be prepared to resp

Find What's Out There



Set, Enforce a Policy



Automate Response

Good News: this can be business as usual process

Roadmap: Control of Machine Identities

Level 0:

Chaos

Have unquantified security risk, outages, expensive and manual processes, and compliance challenges

Level 1:

Control

Build a security foundation with focus on **known and trusted keys and certificates**

Level 2:

Critical Systems

Secure and protect all keys and certificates **on business-critical infrastructure**

Level 3:

Enterprise Protection

Protect and automate **all keys and certificates enterprise-wide** and further reduce costs and extract more business value

Level 4:

Machine Identity Protection

Rapidly respond to internal and external threats and security incidents related to keys and certificates

Endpoint/Mobile
Servers
Virtual Machines
Cloud

Start 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
- And keeping asking more…

GOING UNDETECTED:

HOW CYBERCRIMINALS, HACKTIVISTS, AND NATION STATES MISUSE DIGITAL CERTIFICATES

Kevin Bocek

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO


29th ANNUAL
FIRST
CONFERENCE
SAN JUAN
PUERTO RICO
JUNE 11-16, 2017
FIGHTING PIRATES AND PRIVATEERS
WWW.FIRST.ORG

Threats of the Future

Taking Action

Keys and Certificates
Are the Foundation of Your Security Infrastructure

- SSL/TLS Encryption
- WiFi & VPN Access
- Cloud
- DevOps
- Mobility
- Internet of Things
- SSH Privileged Access