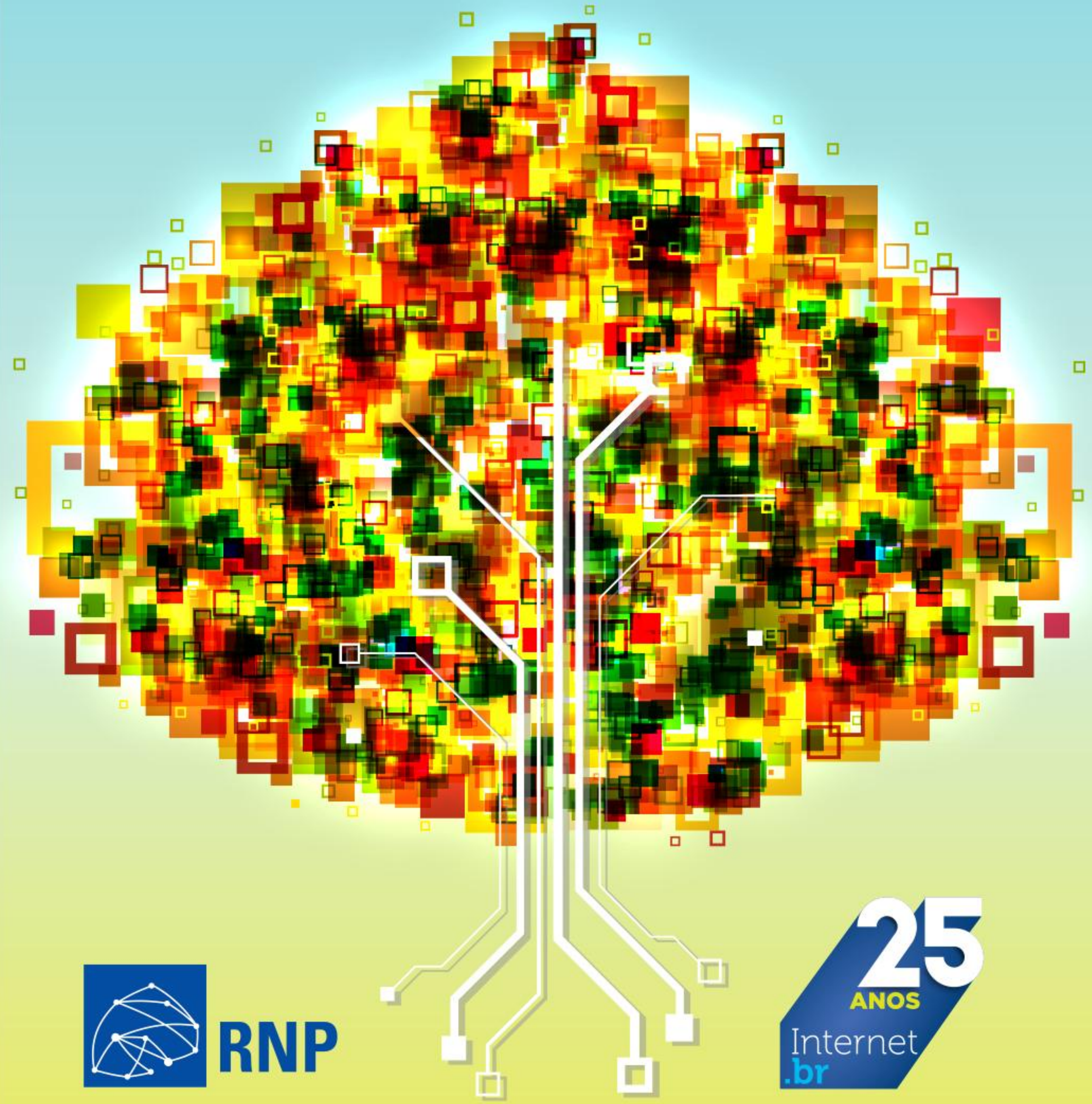


FORUMRNP 2017

25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS

Michelle Wangham

Universidade do Vale do Itajaí (UNIVALI)

Ponto de Vista dos Usuários

✓Segurança é importante e deve ser provida pela instituição (“*obrigação*”)

✓Conectividade, sempre e em qualquer lugar!

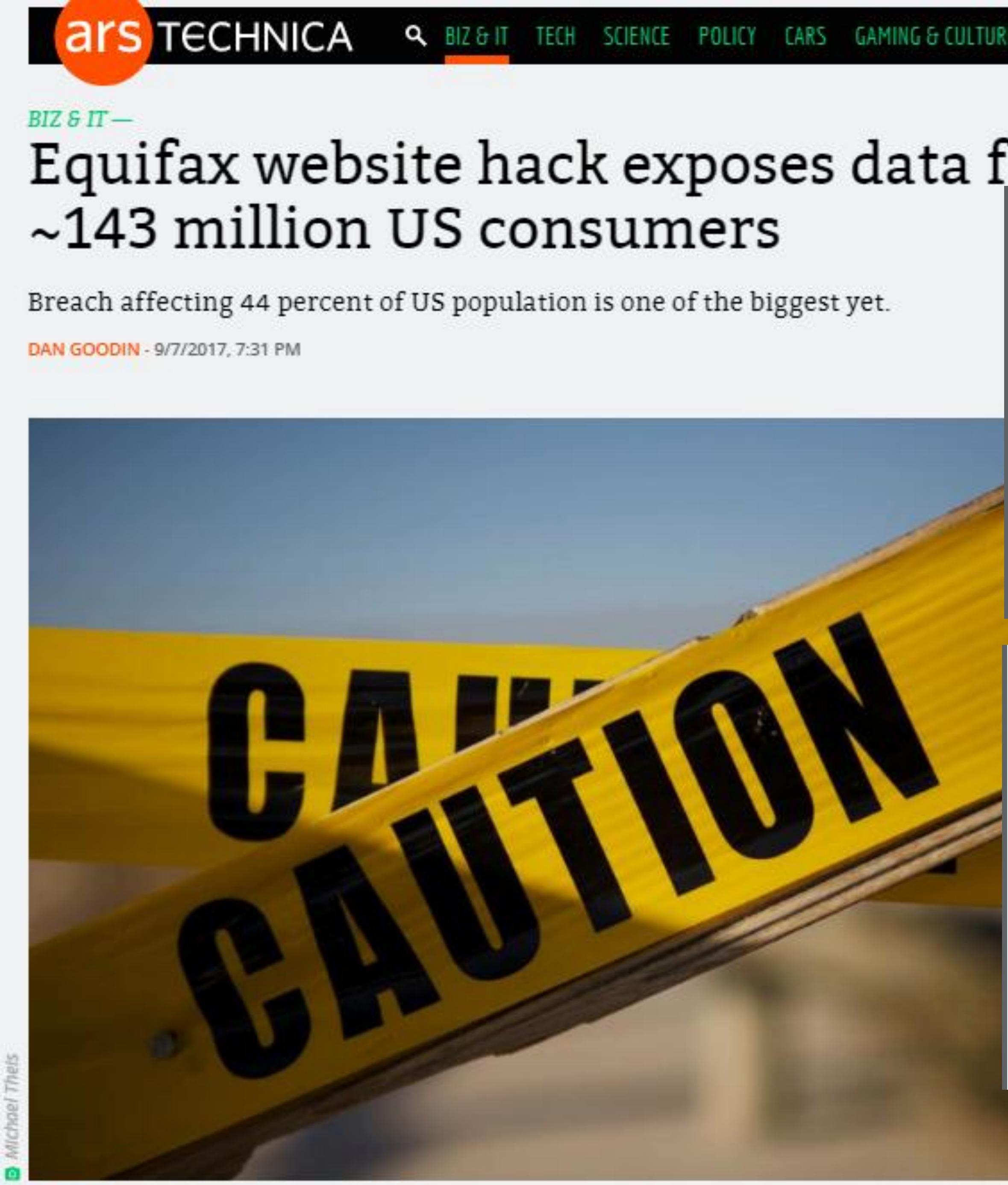
✓ Aplicações, serviços, redes de acesso, Internet eficientes

✓ Armazenamento e aplicações na nuvem (Dropbox, Sharelatex, GoogleDocs, etc)

✓Autenticação única (SSO) e federada (Periodico CAPES, ORCID SP, etc)

✓ Necessidade de desenvolver pesquisa experimental (*testbeds*)

✓Usabilidade prejudicada (políticas e mecanismos)

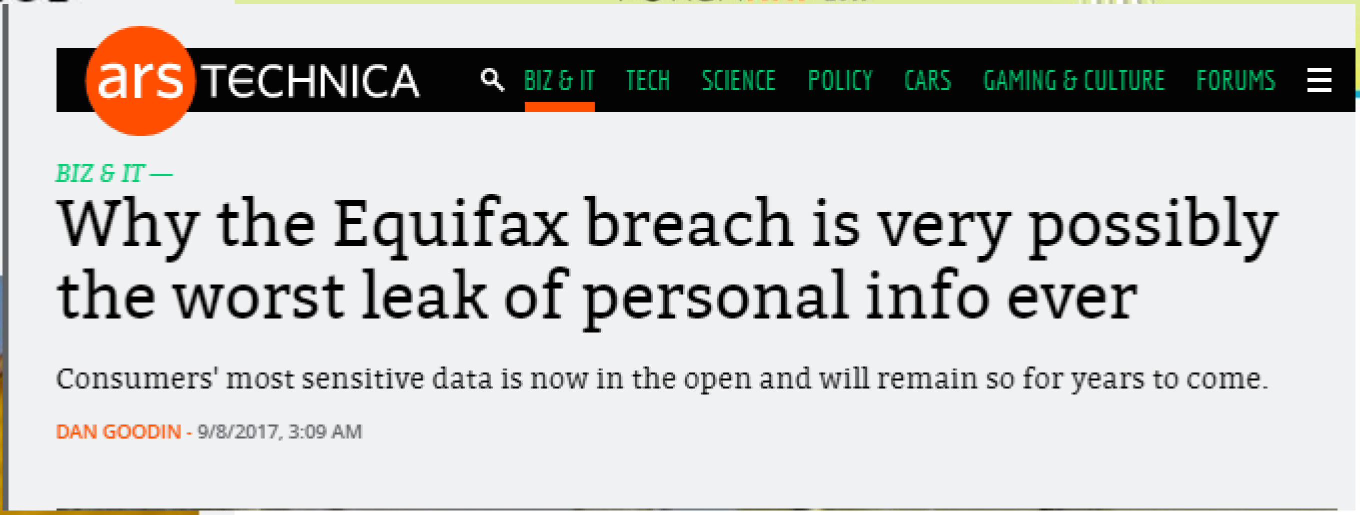


BIZ & IT —

Equifax website hack exposes data for ~143 million US consumers

Breach affecting 44 percent of US population is one of the biggest yet.

DAN GOODIN - 9/7/2017, 7:31 PM

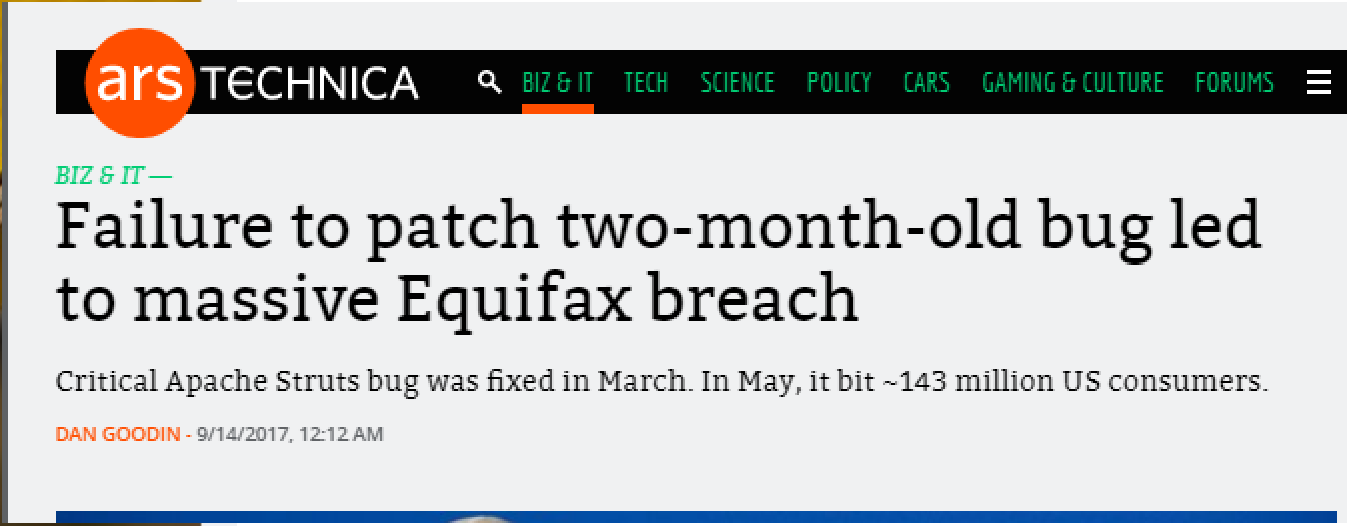


BIZ & IT —

Why the Equifax breach is very possibly the worst leak of personal info ever

Consumers' most sensitive data is now in the open and will remain so for years to come.

DAN GOODIN - 9/8/2017, 3:09 AM



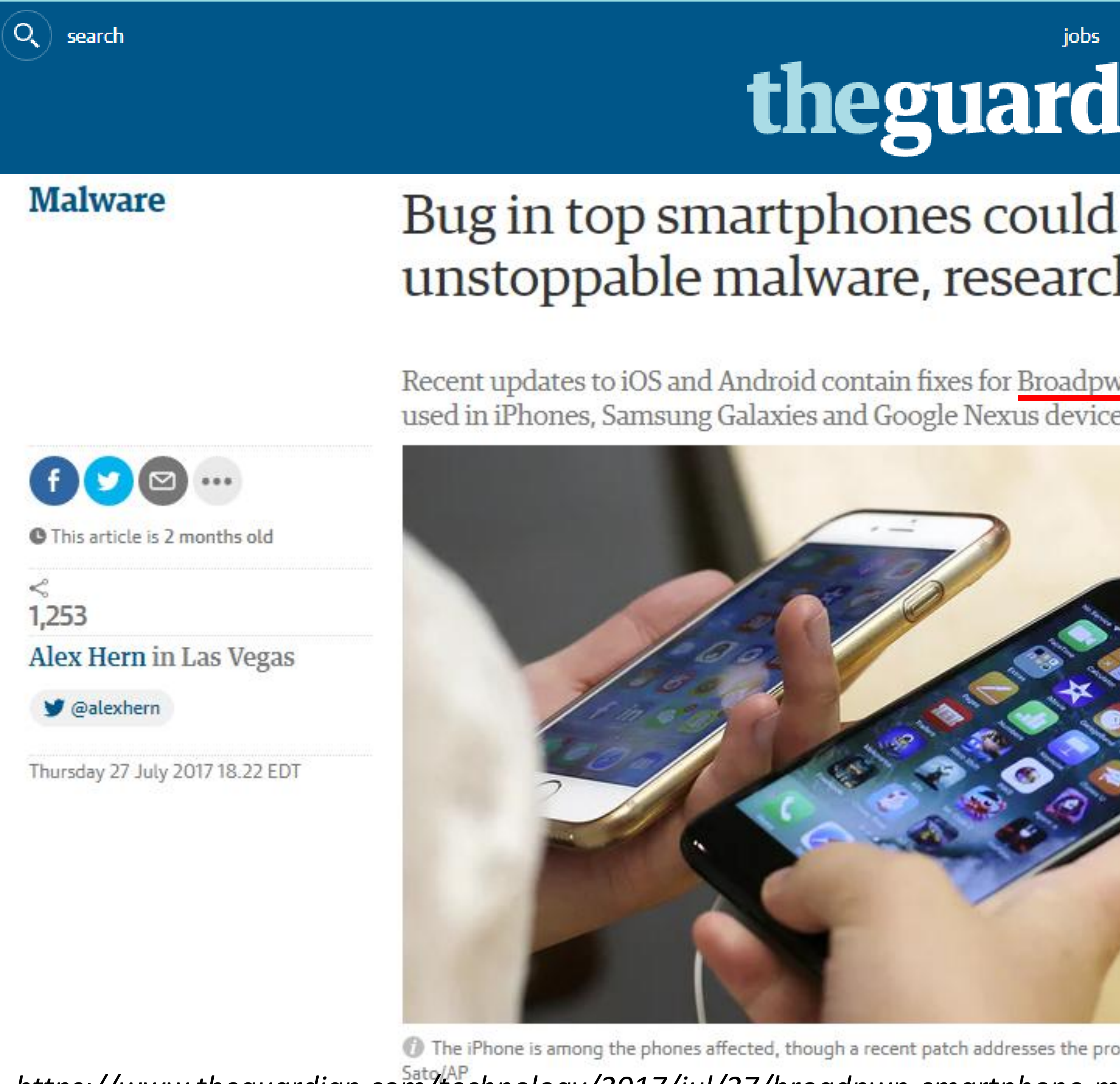
BIZ & IT —

Failure to patch two-month-old bug led to massive Equifax breach

Critical Apache Struts bug was fixed in March. In May, it bit ~143 million US consumers.

DAN GOODIN - 9/14/2017, 12:12 AM

Enlarge https://arstechnica.com/information-technology/2017/09/equifax-website-hack-exposes-data-for-143-million-us-consumers/



Malware

Bug in top smartphones could lead to unstoppable malware, researcher says

Recent updates to iOS and Android contain fixes for Broadpwn, found in chips used in iPhones, Samsung Galaxies and Google Nexus devices

This article is 2 months old

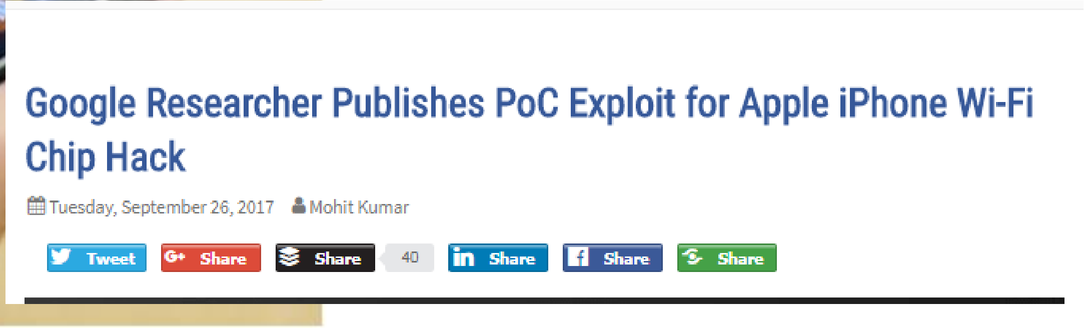
1,253

Alex Hern in Las Vegas

@alexhern

Thursday 27 July 2017 18.22 EDT

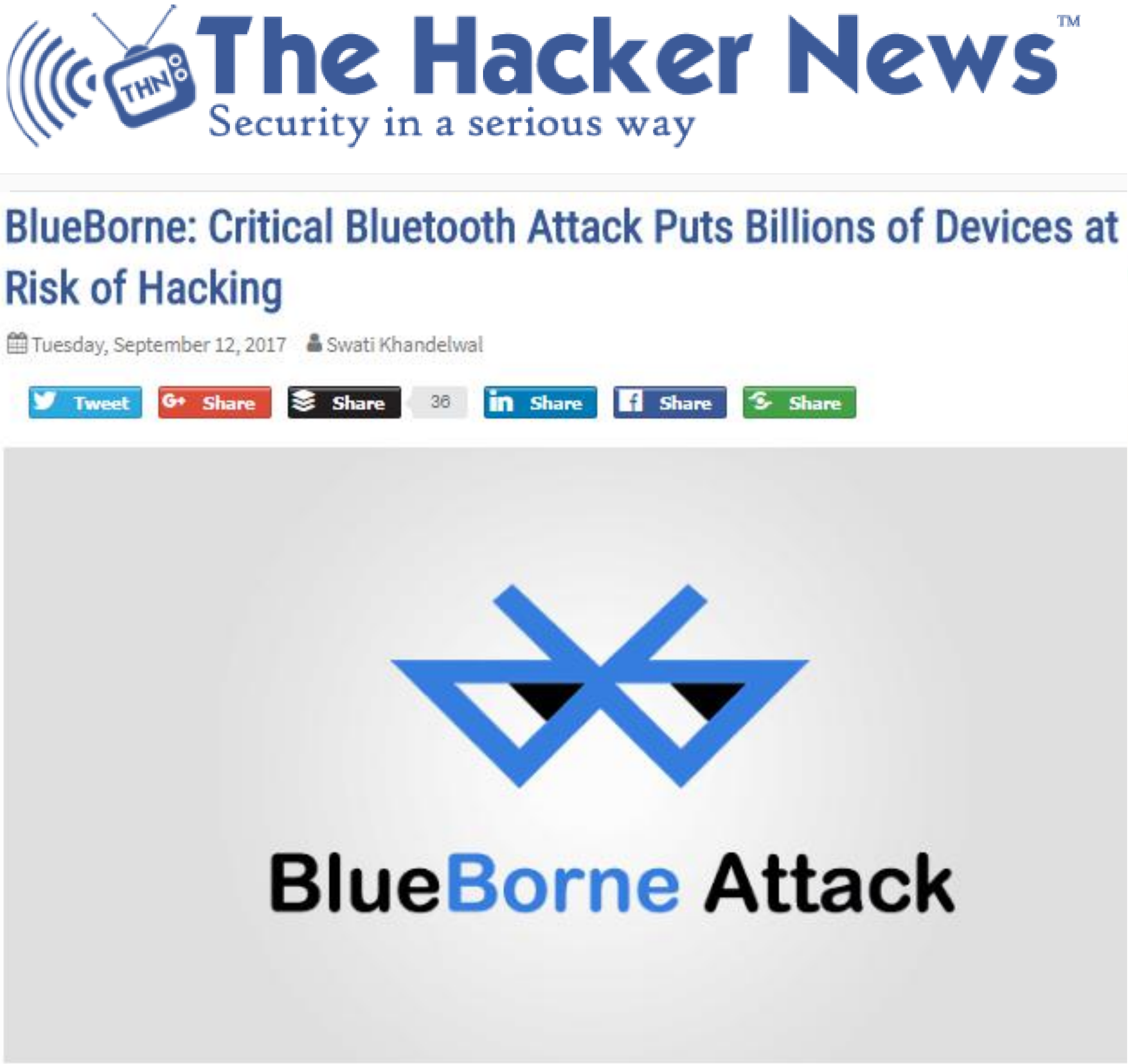
The iPhone is among the phones affected, though a recent patch addresses the problem. Photograph: Kiichiro Sato/AP



Google Researcher Publishes PoC Exploit for Apple iPhone Wi-Fi Chip Hack

Tuesday, September 26, 2017 Mohit Kumar

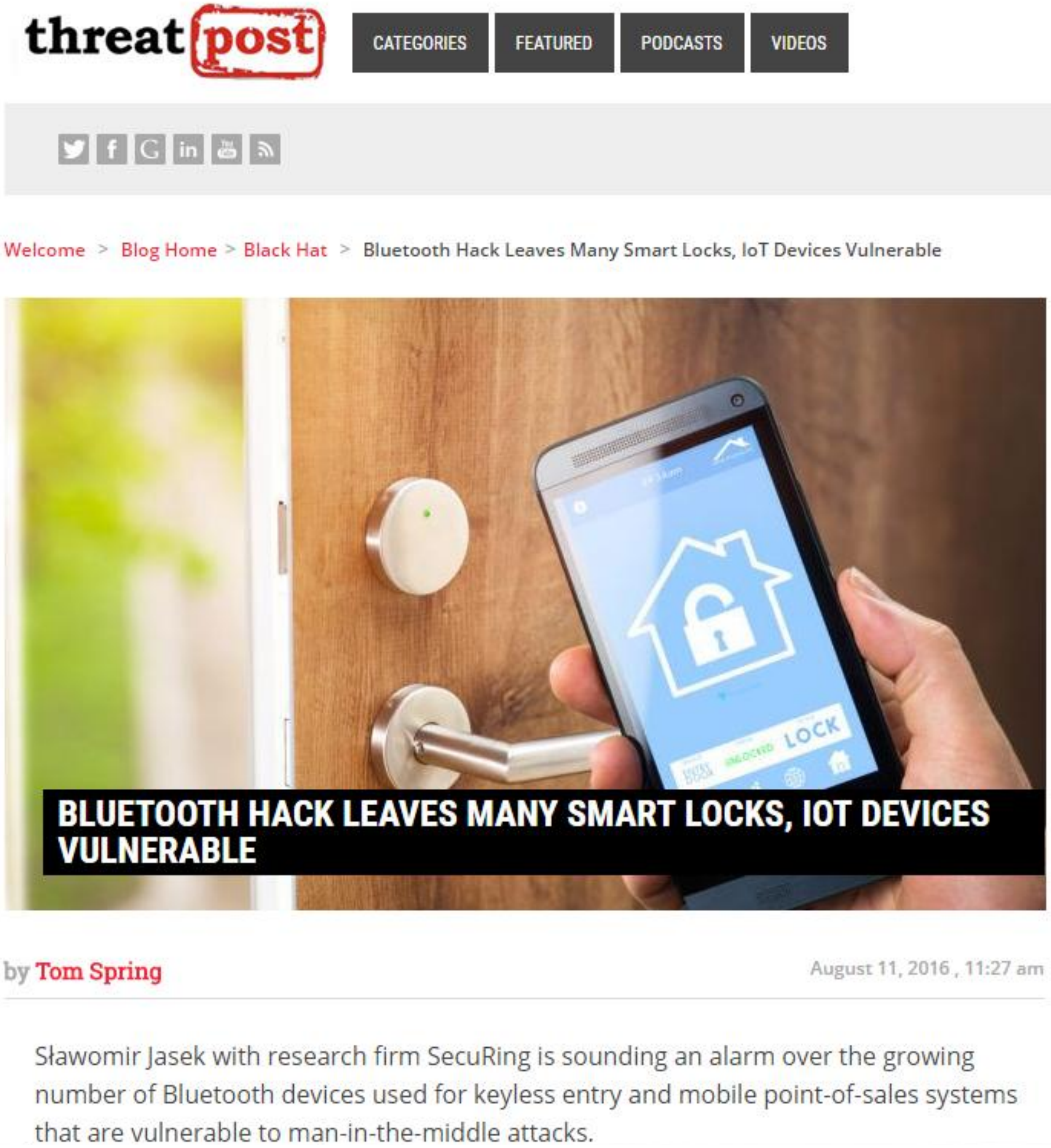
https://www.theguardian.com/technology/2017/jul/27/broadpwn-smartphone-malware-bug-iphone-samsung-google



BlueBorne: Critical Bluetooth Attack Puts Billions of Devices at Risk of Hacking

Tuesday, September 12, 2017 Swati Khandelwal

https://thehackernews.com/2017/09/blueborne-bluetooth-hacking.html



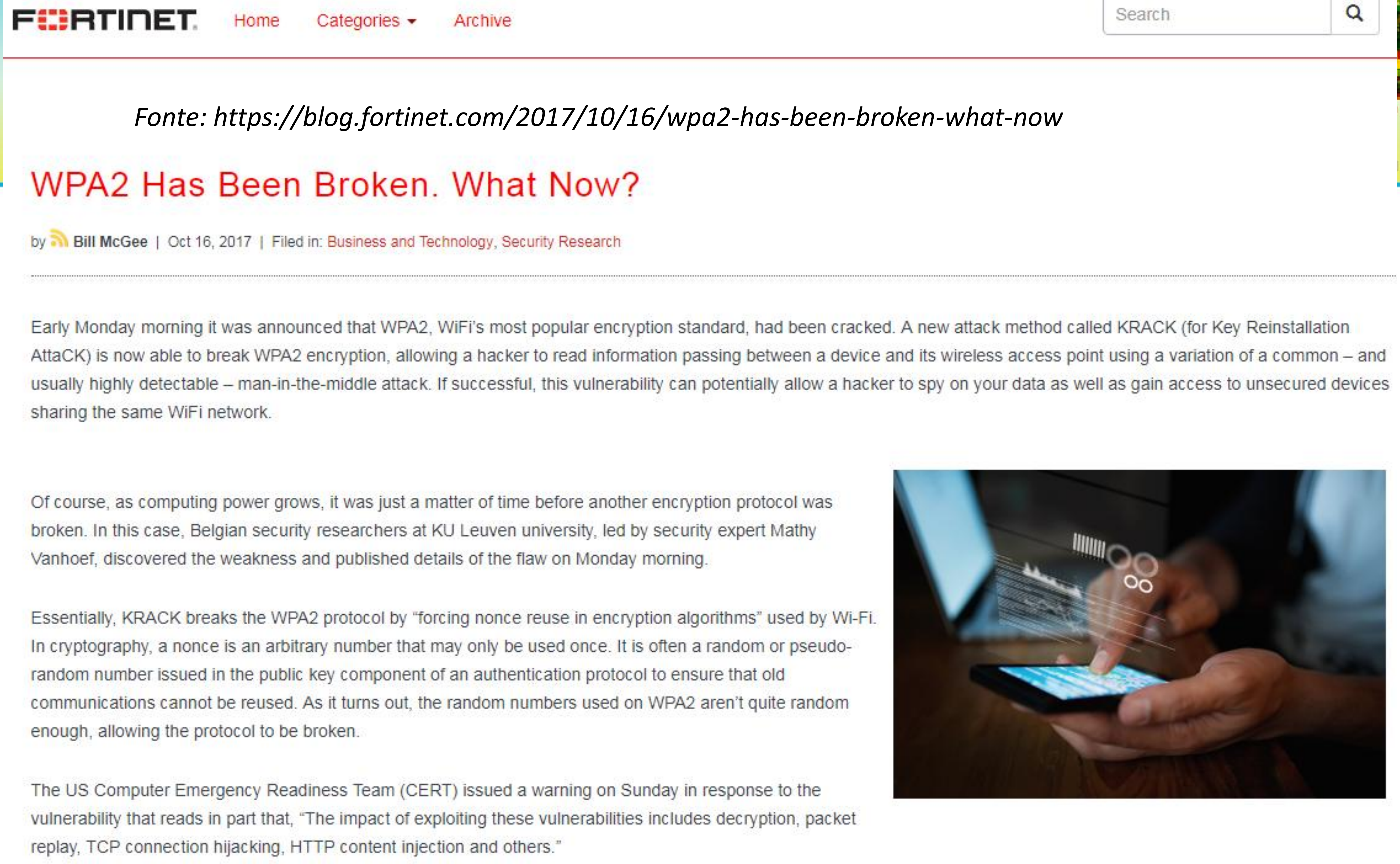
Welcome > Blog Home > Black Hat > Bluetooth Hack Leaves Many Smart Locks, IoT Devices Vulnerable

BLUETOOTH HACK LEAVES MANY SMART LOCKS, IOT DEVICES VULNERABLE

by Tom Spring August 11, 2016 , 11:27 am

Sławomir Jasek with research firm SecuRing is sounding an alarm over the growing number of Bluetooth devices used for keyless entry and mobile point-of-sales systems that are vulnerable to man-in-the-middle attacks.

https://threatpost.com/bluetooth-hack-leaves-many-smart-locks-iot-devices-vulnerable/119825/



Fonte: https://blog.fortinet.com/2017/10/16/wpa2-has-been-broken-what-now

WPA2 Has Been Broken. What Now?

by Bill McGee | Oct 16, 2017 | Filed in: Business and Technology, Security Research

Early Monday morning it was announced that WPA2, WiFi's most popular encryption standard, had been cracked. A new attack method called KRACK (for Key Reinstallation AttaCK) is now able to break WPA2 encryption, allowing a hacker to read information passing between a device and its wireless access point using a variation of a common – and usually highly detectable – man-in-the-middle attack. If successful, this vulnerability can potentially allow a hacker to spy on your data as well as gain access to unsecured devices sharing the same WiFi network.

Of course, as computing power grows, it was just a matter of time before another encryption protocol was broken. In this case, Belgian security researchers at KU Leuven university, led by security expert Mathy Vanhoef, discovered the weakness and published details of the flaw on Monday morning.

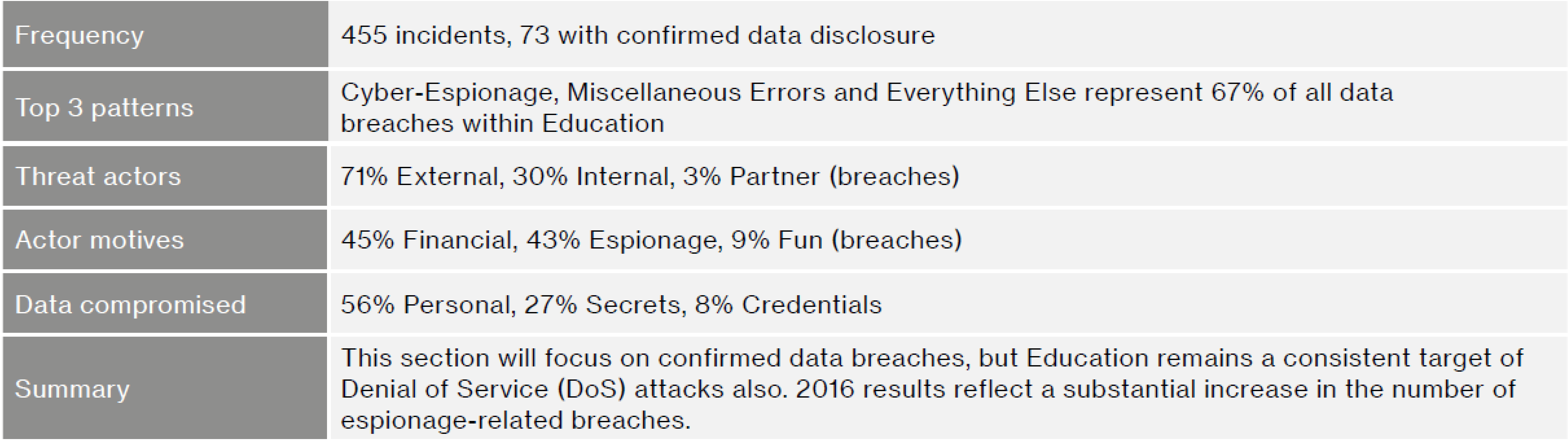
Essentially, KRACK breaks the WPA2 protocol by "forcing nonce reuse in encryption algorithms" used by Wi-Fi. In cryptography, a nonce is an arbitrary number that may only be used once. It is often a random or pseudo-random number issued in the public key component of an authentication protocol to ensure that old communications cannot be reused. As it turns out, the random numbers used on WPA2 aren't quite random enough, allowing the protocol to be broken.

The US Computer Emergency Readiness Team (CERT) issued a warning on Sunday in response to the vulnerability that reads in part that, "The impact of exploiting these vulnerabilities includes decryption, packet replay, TCP connection hijacking, HTTP content injection and others."

Educational Services

2017 Data Breach Investigations Report

10th Edition

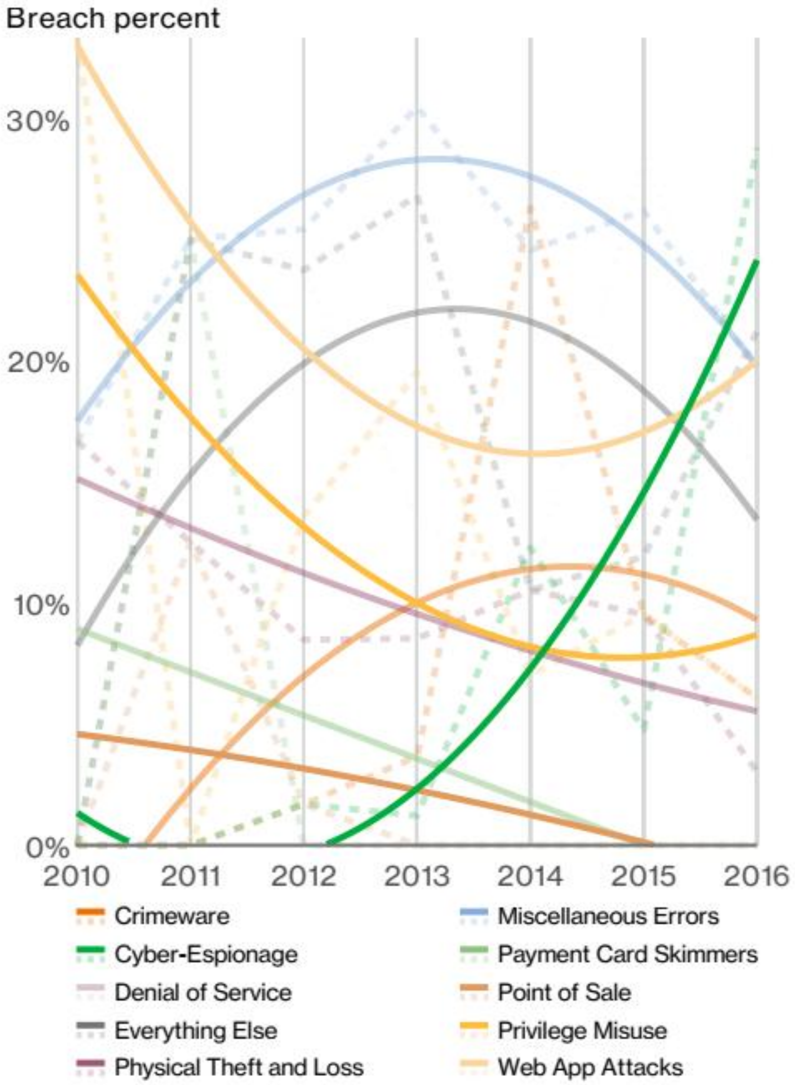


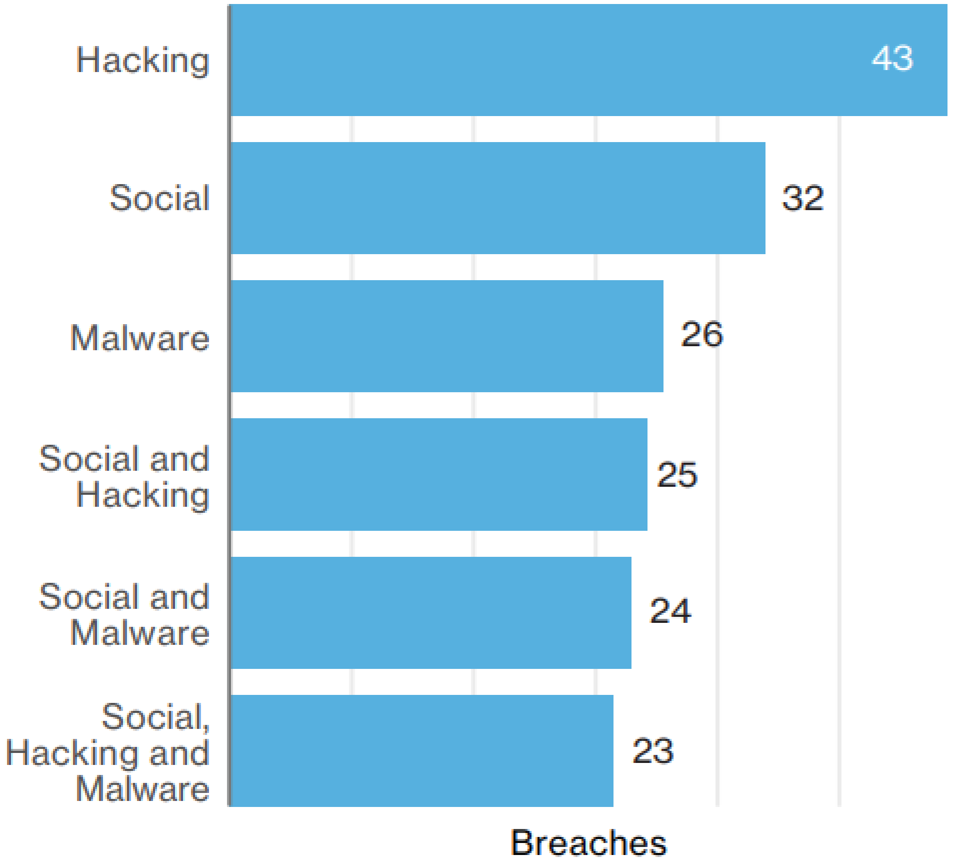
Frequency	455 incidents, 73 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Miscellaneous Errors and Everything Else represent 67% of all data breaches within Education
Threat actors	71% External, 30% Internal, 3% Partner (breaches)
Actor motives	45% Financial, 43% Espionage, 9% Fun (breaches)
Data compromised	56% Personal, 27% Secrets, 8% Credentials
Summary	This section will focus on confirmed data breaches, but Education remains a consistent target of Denial of Service (DoS) attacks also. 2016 results reflect a substantial increase in the number of espionage-related breaches.

Fonte: 2017 Data Breach Investigations Report – Verizon
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

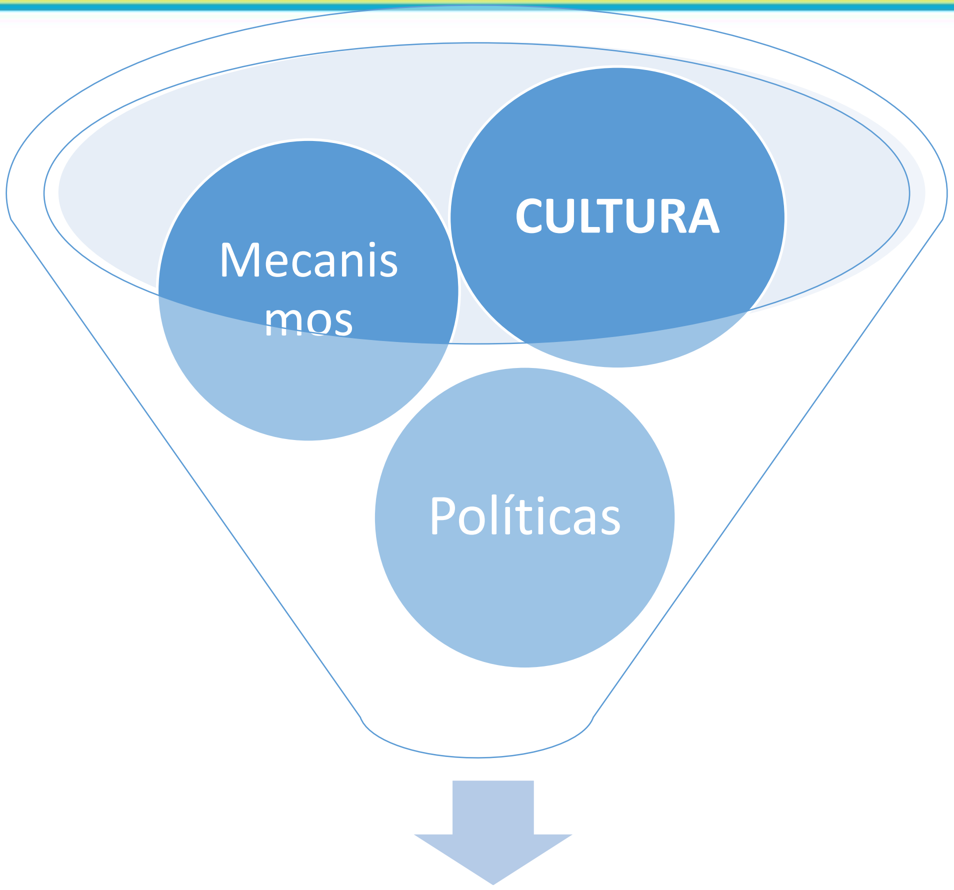
Cenário Atual

Fonte: 2017 Data Breach Investigations Report - Verizon





Em busca da Segurança da informação nos Campi



Segurança

Desafios e Preocupações

- ✓Cultura da segurança (conscientização e treinamento constates)
- ✓BYOD e uso de serviços sem autorização (Shadow IT)
- ✓Campus Inteligente (novas preocupações, velhos problemas)
- ✓ Autenticação federada – única credencial comprometida
- ✓ Propriedade Intelectual
- ✓ Privacidade

Michelle Wangham

wangham@univali.br