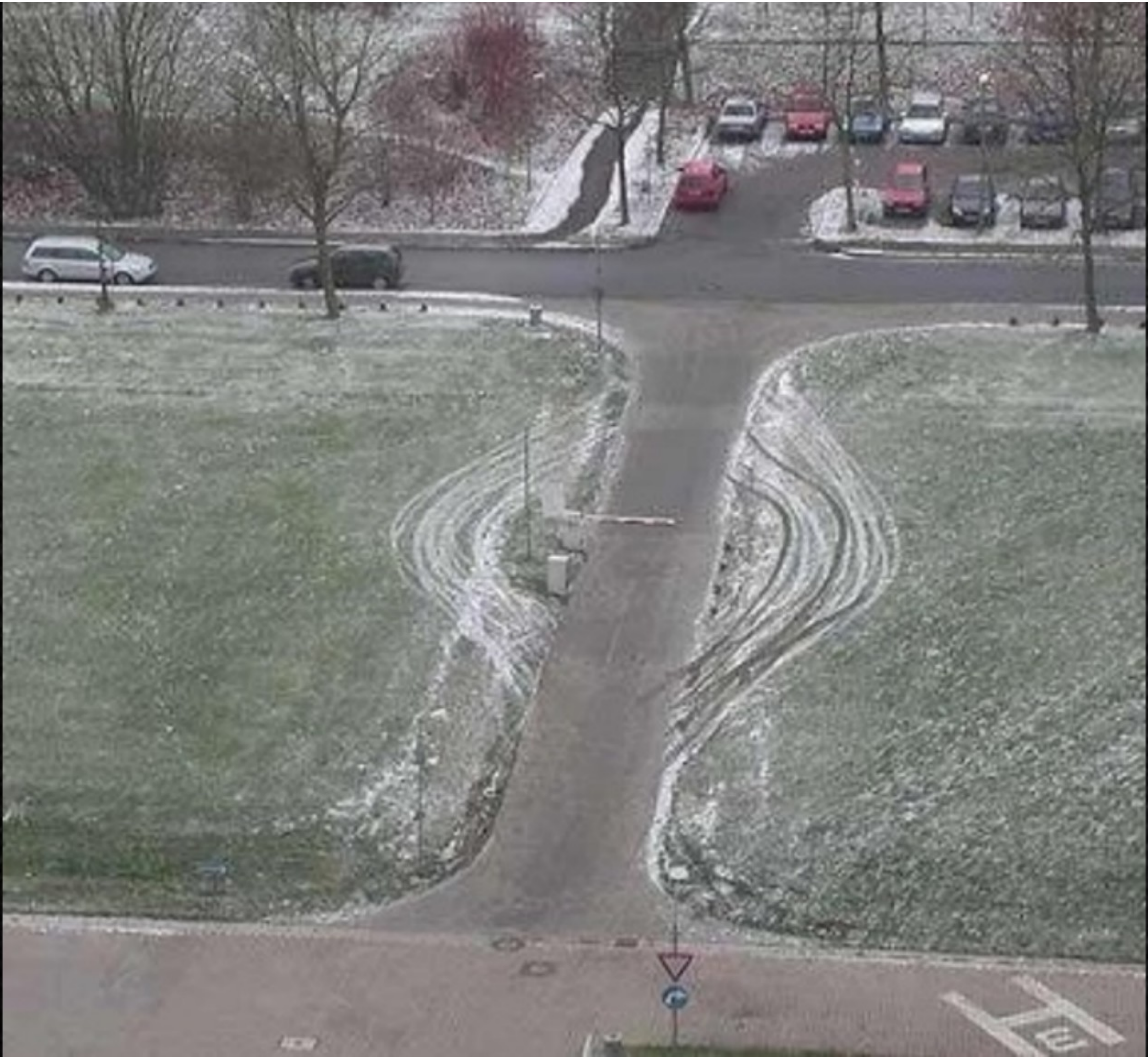
"Security is a Mission not an Intermission"

David Balcar

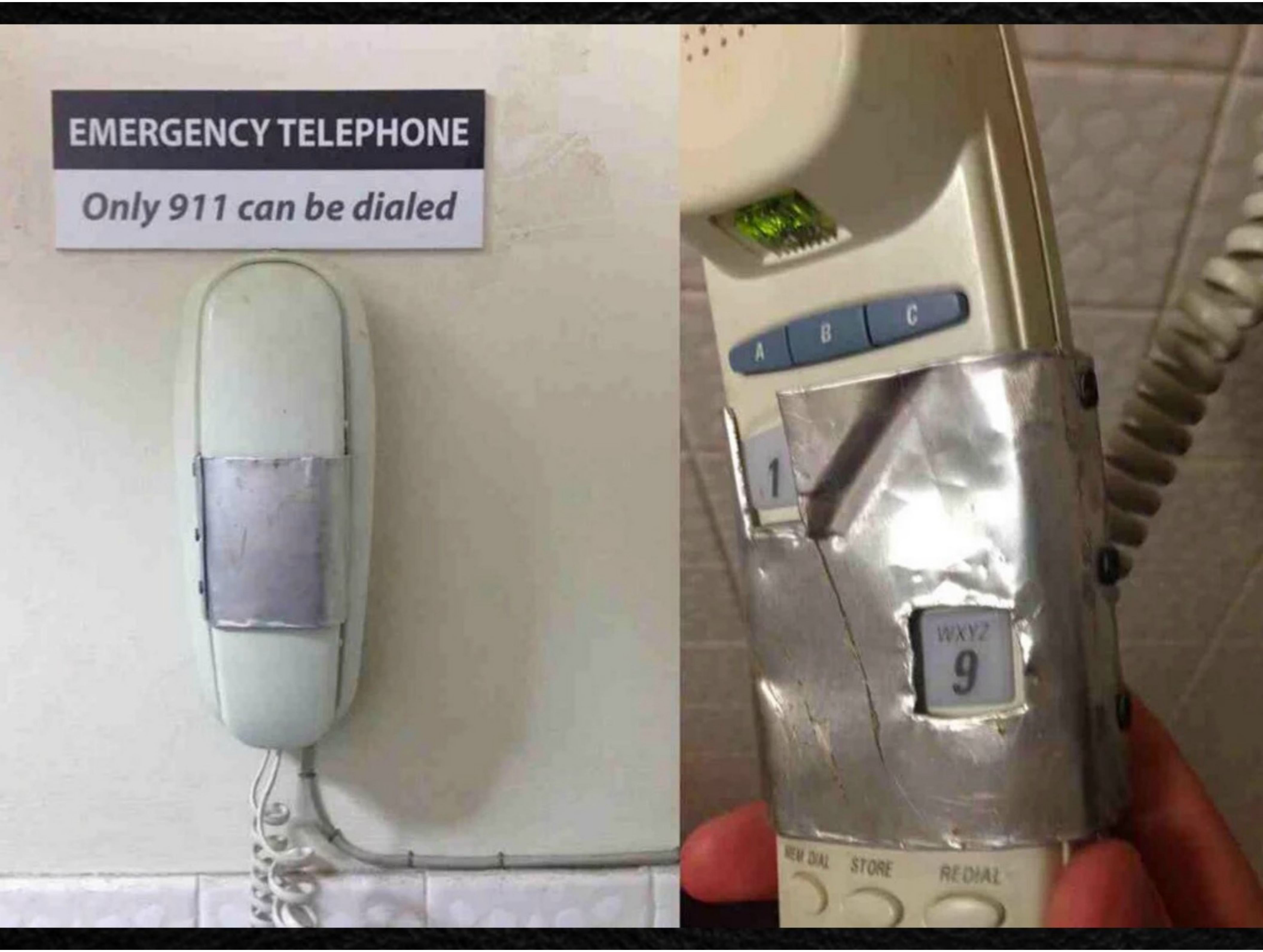
Security Strategist
dbalcar@carbonblack.com

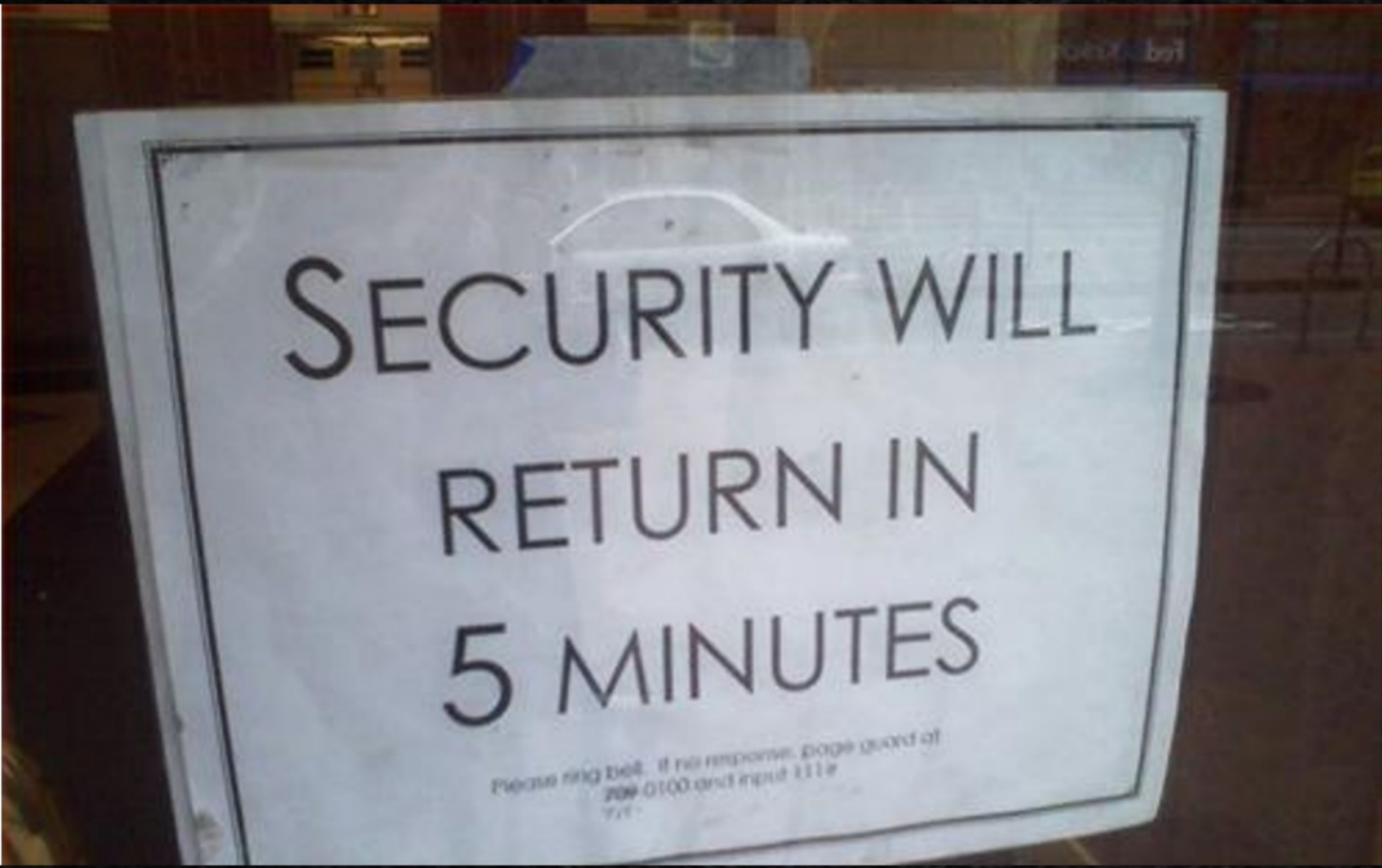
@network232

Threat Landscape



Served
All Day
Regular 6" Flatbread or Subs
Regular 12" Flatbread or Subs
11am
2.00 $3.00 $5.00
2.50 $3.50 $5.50
$4.75 $6.75

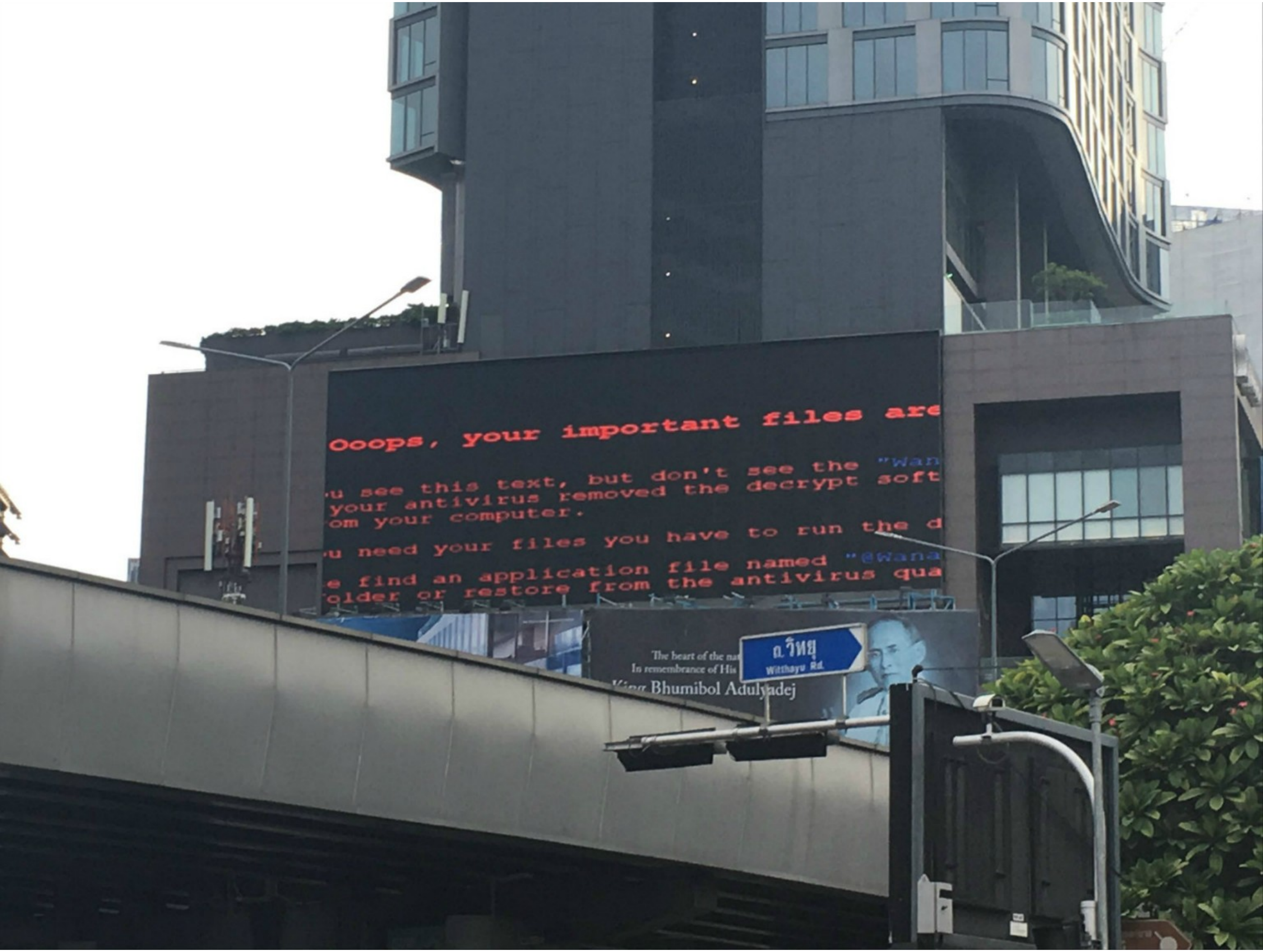

EMERGENCY TELEPHONE
Only 911 can be dialed
A
B
C
1
WXYZ
9
NEW DIAL
STORE
REDIAL



SECURITY WILL
RETURN IN
5 MINUTES

Please ring bell. If no response, page guard at
209-0100 and input 111#

SECURIT
DELTA
SKY PRIORITY
Currency Exchange
MAC
EXIT



Ooops, your important files are

u see this text, but don't see the "wan
your antivirus removed the decrypt soft
om your computer.

u need your files you have to run the d

e find an application file named "@wana
older or restore from the antivirus qua

Enterprise Security Trends for 2018

Ransomware

Most advanced threats
targeting basic vulnerabilities
and the human factor

Availability and with low
prices for [illegible]
Cybercrime-as-a-Service
(CaaS) - (RaaS)

Perimeter Security
is overestimated

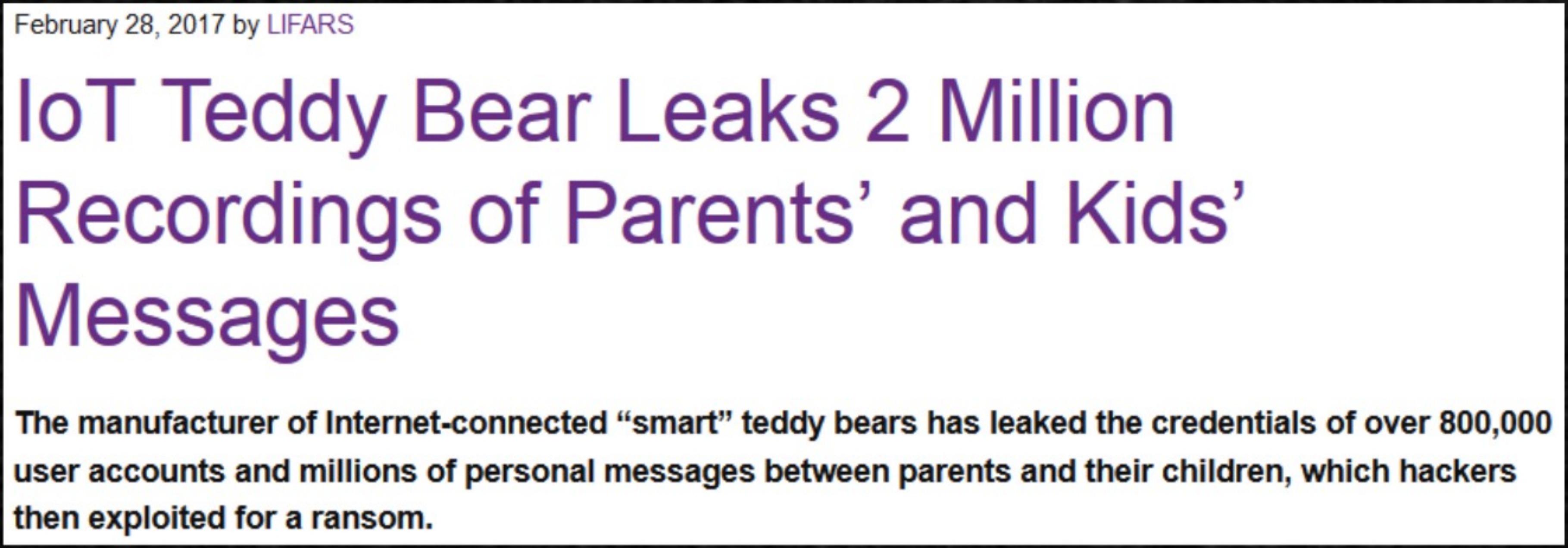
Visibility gap and lack
of operational information with
growing IT sophistication

Attacks on 3rd party
providers: SMBs can become
a part of the attack chain

Targeted Attacks could be
undetected for many months
and even years with traditional
security solutions

Just the Facts!

Just the Facts!

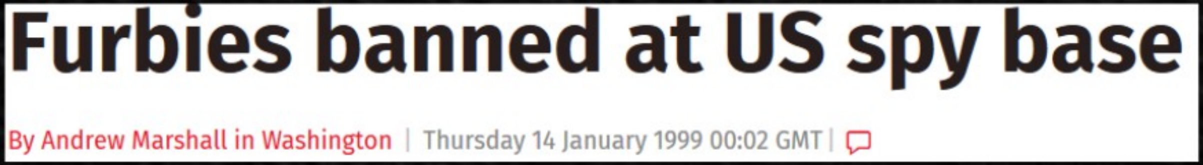


February 28, 2017 by LIFARS

IoT Teddy Bear Leaks 2 Million Recordings of Parents' and Kids' Messages

The manufacturer of Internet-connected "smart" teddy bears has leaked the credentials of over 800,000 user accounts and millions of personal messages between parents and their children, which hackers then exploited for a ransom.

Researchers found CloudPets could be hacked via their unsecured Bluetooth connection



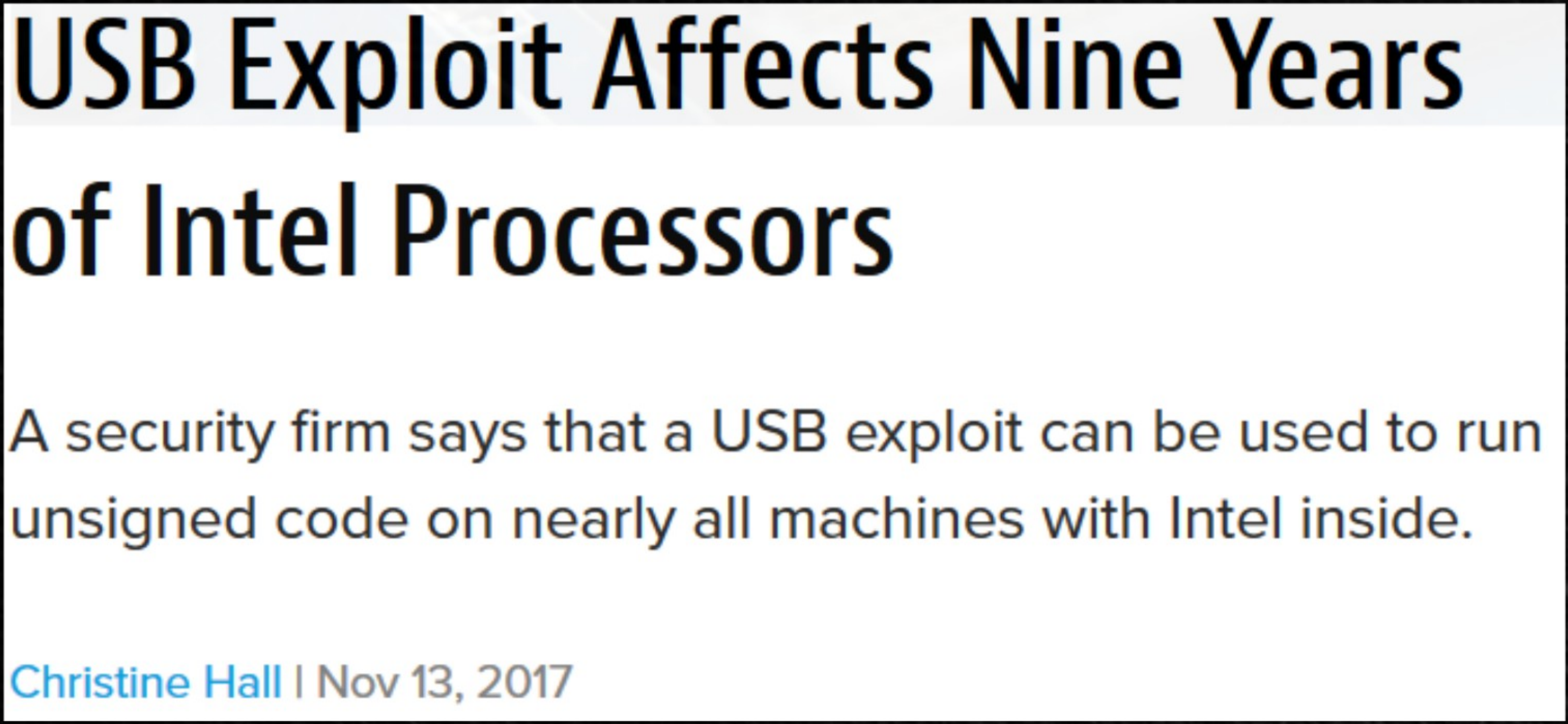
Furbies banned at US spy base

By Andrew Marshall in Washington | Thursday 14 January 1999 00:02 GMT |

Internet of Threats...

https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children

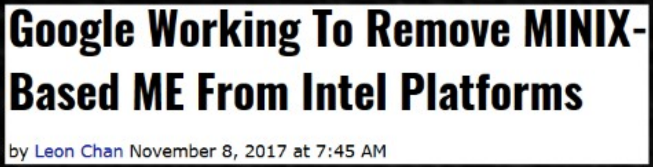
It's getting ridiculous...



USB Exploit Affects Nine Years of Intel Processors

A security firm says that a USB exploit can be used to run unsigned code on nearly all machines with Intel inside.

Christine Hall | Nov 13, 2017



Google Working To Remove MINIX-Based ME From Intel Platforms

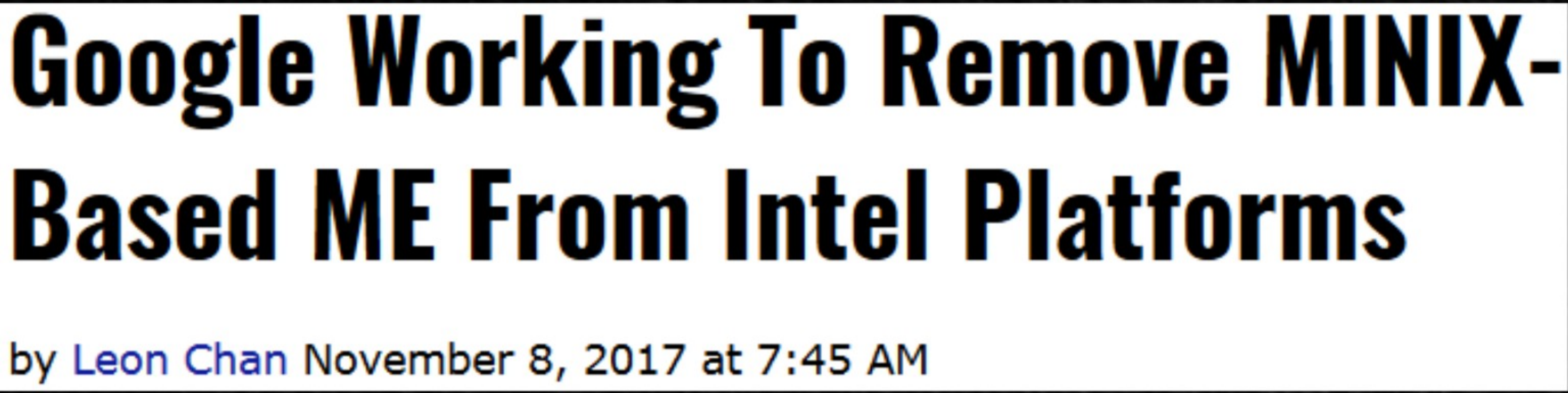
by Leon Chan November 8, 2017 at 7:45 AM

https://www.networkworld.com/article/3236064/servers/minix-the-most-popular-os-in-the-world-thanks-to-intel.html

http://www.tomshardware.com/news/google-removing-minix-management-engine-intel,35876.html

https://boingboing.net/2016/06/15/intel-x86-processors-ship-with.html

017



Google Working To Remove MINIX-Based ME From Intel Platforms

by Leon Chan November 8, 2017 at 7:45 AM

3236064/servers/minix-the-most-popul

oogle-removing-minix-management-e

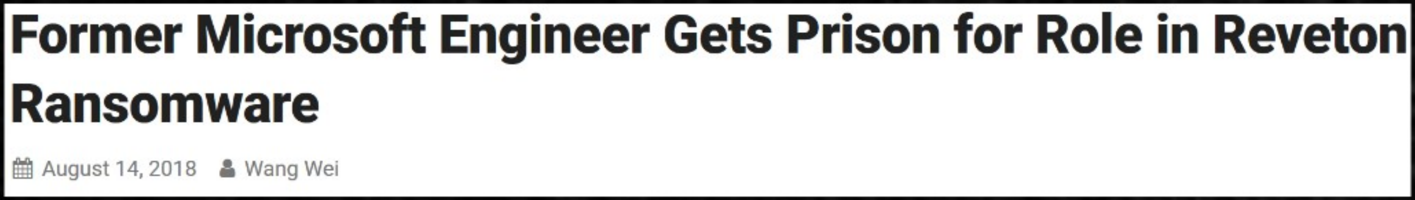
New meaning to locking up the cyber criminals...

© Ohio Office of the Inspector General

n analysis of the hard drives found on the computers reveal that prisoners also used he technology to search records of fellow inmates, acquire official passes to access ertain restricted areas in the prison, research tax fraud, and apply for credit cards. Th omputers were able to be installed without detection because some inmates articipating in special community-related programs at the Marion Correctional nstitution were not constantly monitored.

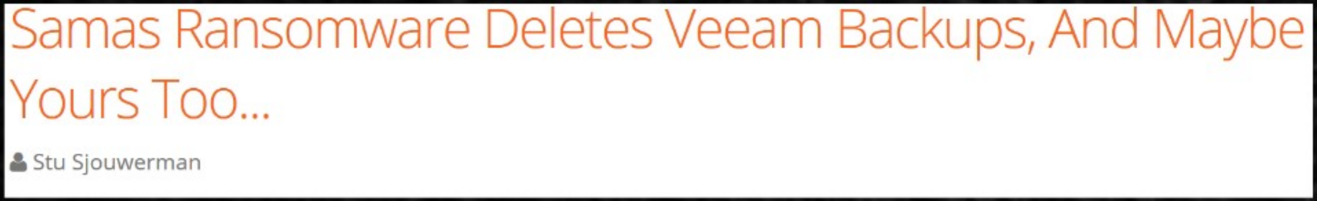
http://www.wjla.com/news/nation-wo http://dailycaller.com/2017/04/13/report-inmates-built-their-own-computers-to-watch-porn-hack-prison-network/

In the News...



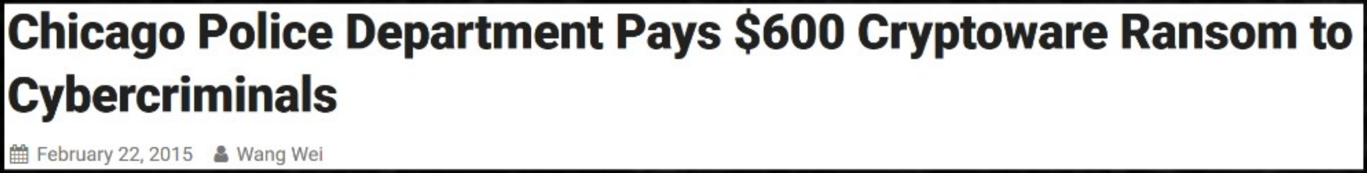
Former Microsoft Engineer Gets Prison for Role in Reveton Ransomware

August 14, 2018 Wang Wei



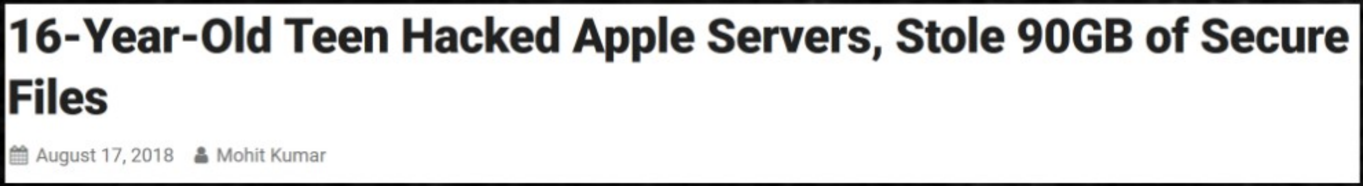
Samas Ransomware Deletes Veeam Backups, And Maybe Yours Too...

Stu Sjouwerman



Chicago Police Department Pays $600 Cryptoware Ransom to Cybercriminals

February 22, 2015 Wang Wei



16-Year-Old Teen Hacked Apple Servers, Stole 90GB of Secure Files

August 17, 2018 Mohit Kumar

In the News...

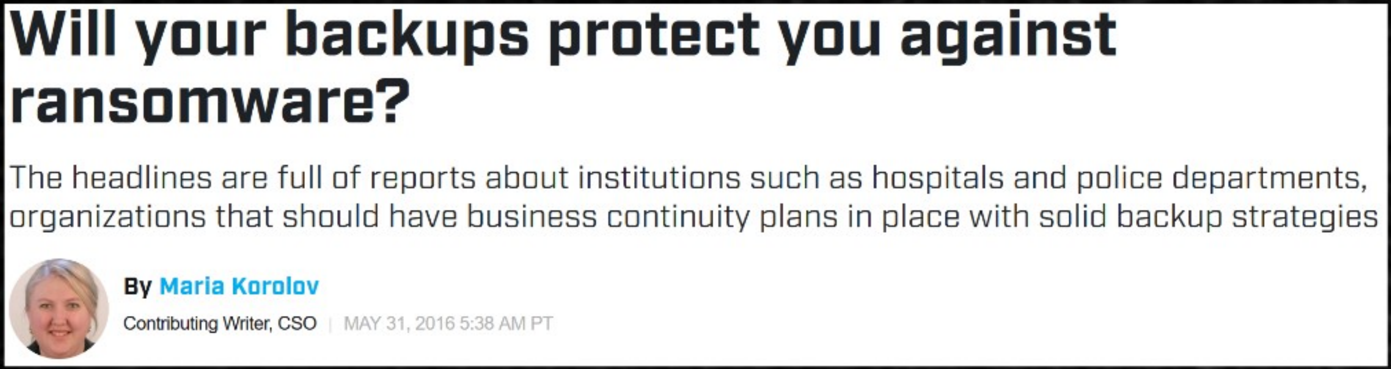
Ransomware Attack Wipes Out Police and Fire Department Data

MAY 13TH, 2018 WAQAS MALWARE, SECURITY 0 COMMENTS

In the city of Riverside's case, it is unclear if there was any ransom demand from the attackers though Carpenter confirmed that attackers were able to wipe out eight hours worth of data from the server. The good news, however, is that the city kept a back up of its data.

"Everything was backed-up, but we lost about eight hours worth of information we have to re-enter," he said. "It was our police and fire records, so we just re-enter the reports," said Carpenter.

In the News...



Will your backups protect you against ransomware?

The headlines are full of reports about institutions such as hospitals and police departments, organizations that should have business continuity plans in place with solid backup strategies

By Maria Korolov

Contributing Writer, CSO | MAY 31, 2016 5:38 AM PT

The Police Department in Cockrell Hill, Texas, admitted in a press release that they lost 8 years' worth of evidence after the department's server was infected with ransomware.

The lost evidence includes all body camera video, and sections of in-car video, in-house surveillance video, photographs, and all their Microsoft Office documents. OUCH.

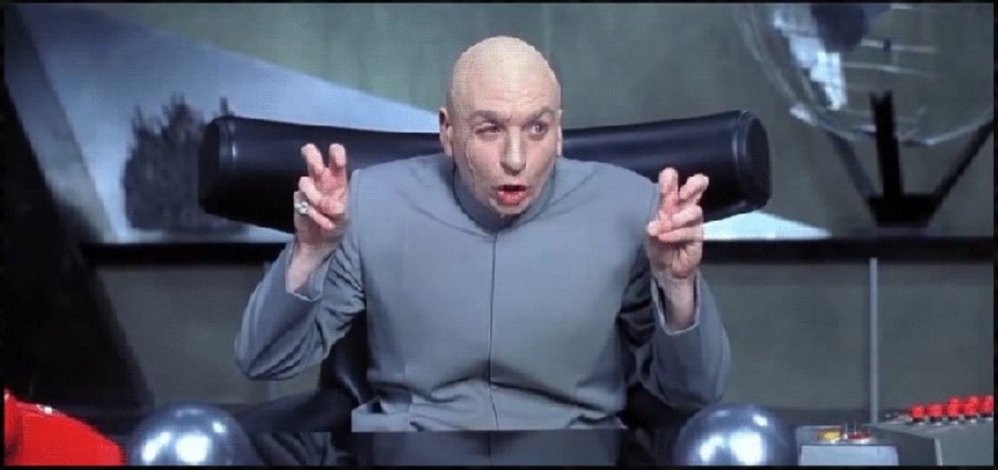
The department says the infection was discovered on December 12, last year, and the crooks asked fo a $4,000 ransom fee to unlock the files.

After consulting with the FBI's cyber-crime unit, the department decided to wipe their data server and reinstall everything. Data could not be recovered from backups, as the backup procedure kicked in shortly after the ransomware took root, and backed up copies of the encrypted files.

s://www.netgainit.com/ransomware-wipes-out-police-evidence-and-more-security-headlines/

An advanced persistent threat is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. An APT usually targets organizations and/or nations for business or political motives. APT processes require a high degree of covertness over a long period of time

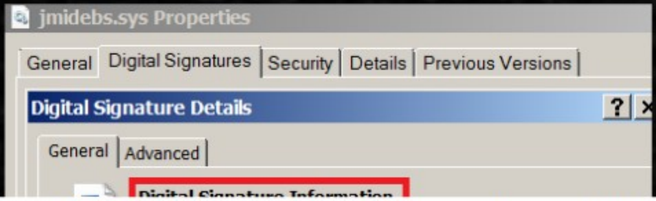
Yes I Know...



Way over used term...

Say it isn't so...

From stolen Digital Signatures to infected firmware to attached hardware devices.

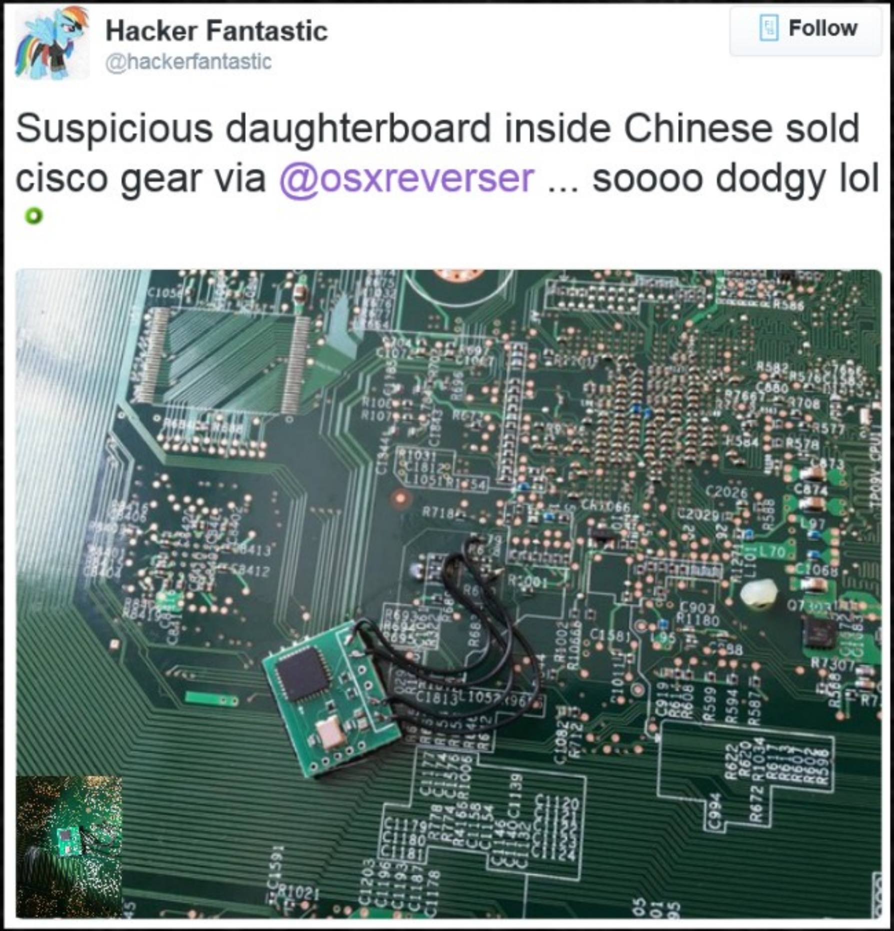


Code Signing Certificates Up for Sale on the Dark Web

By **Richard** - November 10, 2017

According to the findings, the certificates are readily available in dark web markets and are going for up to $1,200. This hefty price tag essentially means that the certificates are costlier than handguns, credit cards, as well as counterfeit United States passports.

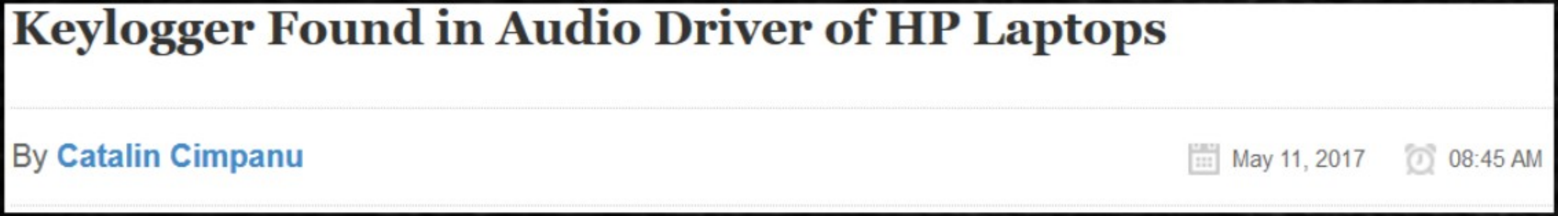
The World's Most Sophisticated Malware Ever Infects Hard Drive Firmware "Equation group" Feb 2015



Hacker Fantastic
@hackerfantastic

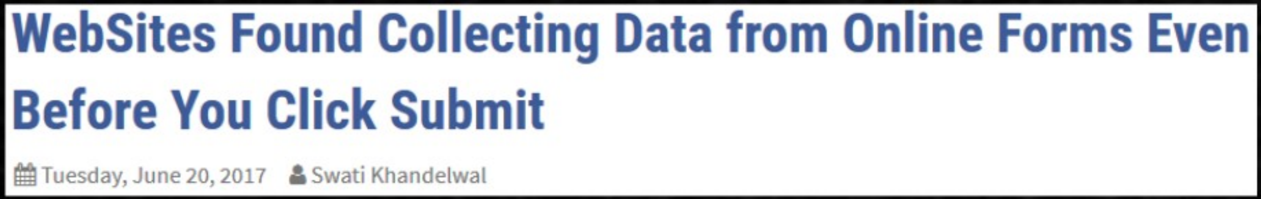
Suspicious daughterboard inside Chinese sold cisco gear via @osxreverser ... soooo dodgy lol

I can't make this stuff up...



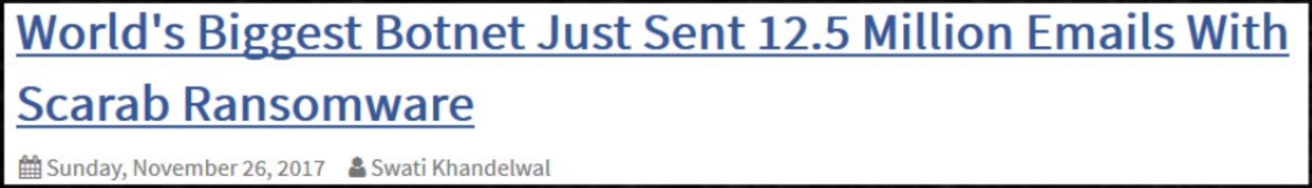
Keylogger Found in Audio Driver of HP Laptops

By **Catalin Cimpanu** May 11, 2017 08:45 AM



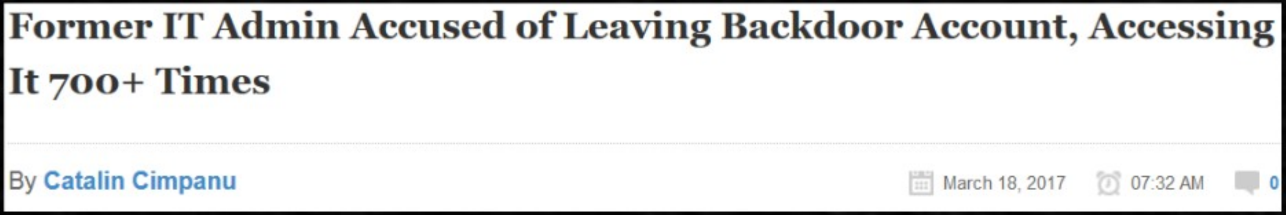
WebSites Found Collecting Data from Online Forms Even Before You Click Submit

Tuesday, June 20, 2017 Swati Khandelwal



World's Biggest Botnet Just Sent 12.5 Million Emails With Scarab Ransomware

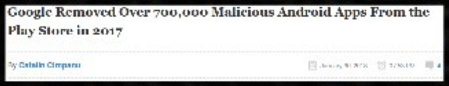
Sunday, November 26, 2017 Swati Khandelwal



Former IT Admin Accused of Leaving Backdoor Account, Accessing It 700+ Times

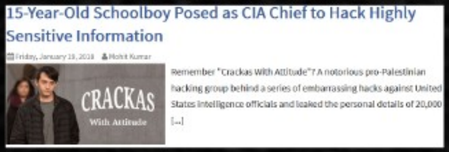
By **Catalin Cimpanu** March 18, 2017 07:32 AM 0

I can't make this stuff up...



Google Removed Over 700,000 Malicious Android Apps From the Play Store in 2017

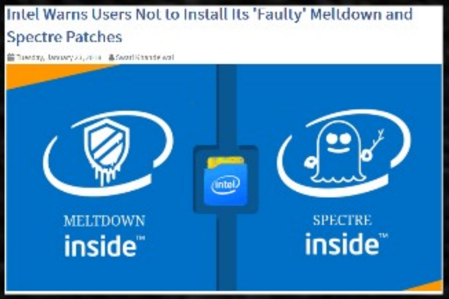
By Catalin Cimpanu [illegible]



15-Year-Old Schoolboy Posed as CIA Chief to Hack Highly Sensitive Information

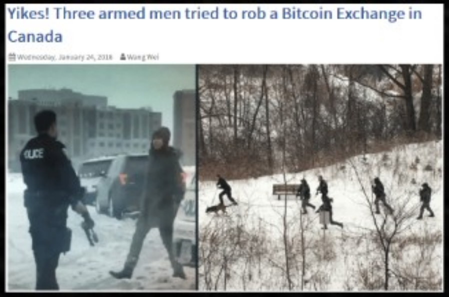
Friday, January 19, 2018 Mohit Kumar

Remember "Crackas With Attitude"? A notorious pro-Palestinian hacking group behind a series of embarrassing hacks against United States intelligence officials and leaked the personal details of 20,000 [...]



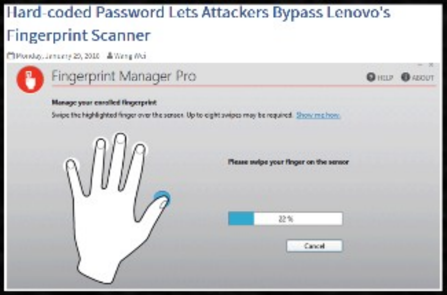
Intel Warns Users Not to Install Its 'Faulty' Meltdown and Spectre Patches

Tuesday, January 23, 2018 Swati Khandelwal



Yikes! Three armed men tried to rob a Bitcoin Exchange in Canada

Wednesday, January 24, 2018 Wang Wei



Hard-coded Password Lets Attackers Bypass Lenovo's Fingerprint Scanner

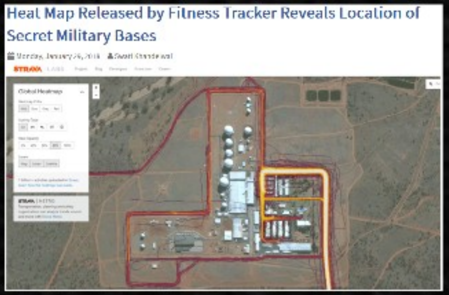
Monday, January 29, 2018 Wang Wei

Fingerprint Manager Pro

Manage your enrolled fingerprint

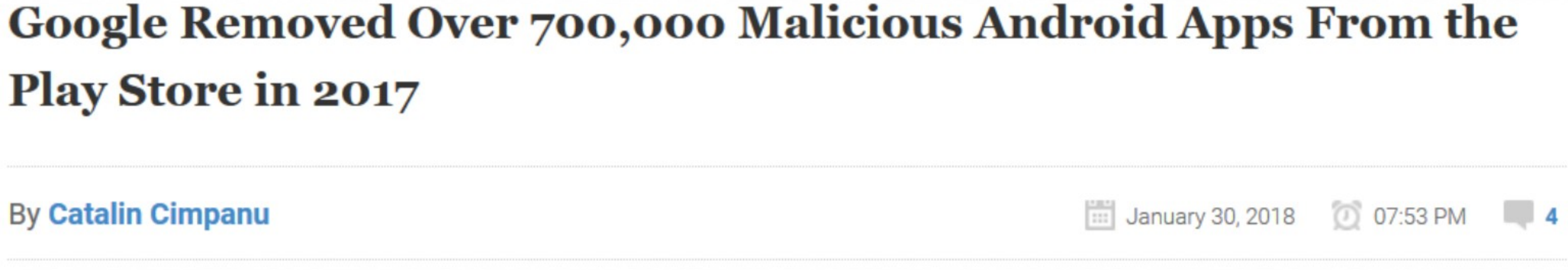
Swipe the highlighted finger over the sensor. Up to eight swipes may be required. Show me how.

Please swipe your finger on the sensor



Heat Map Released by Fitness Tracker Reveals Location of Secret Military Bases

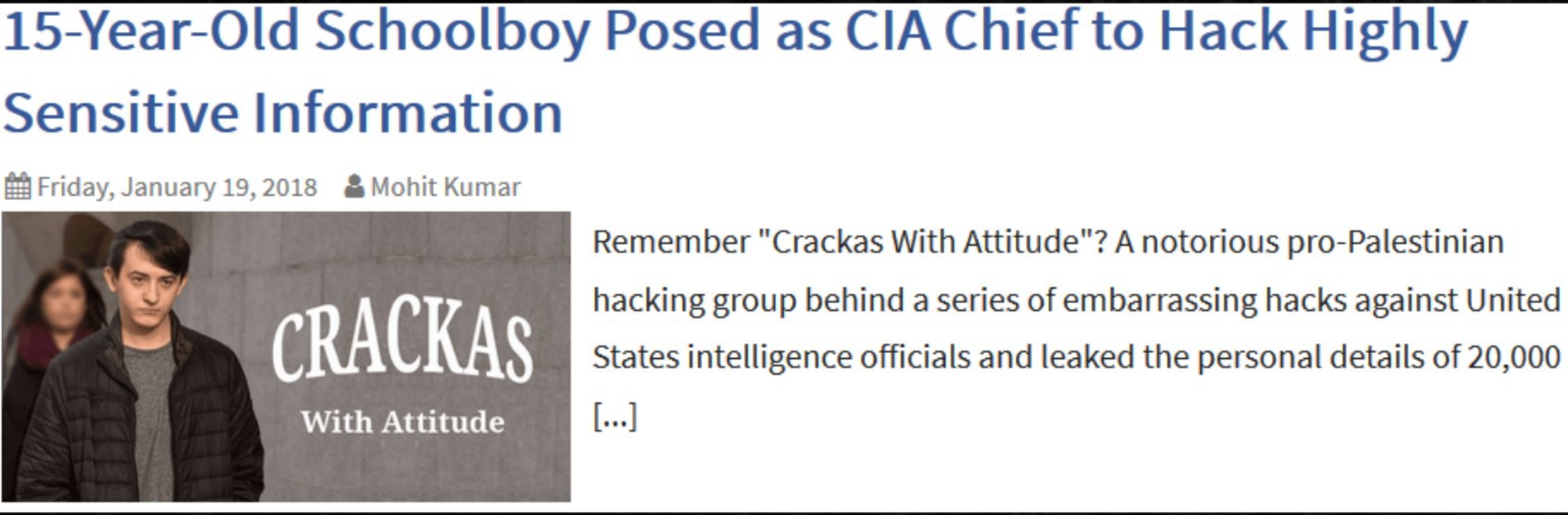
Monday, January 29, 2018 Swati Khandelwal



Google Removed Over 700,000 Malicious Android Apps From the Play Store in 2017

By Catalin Cimpanu

January 30, 2018 07:53 PM 4



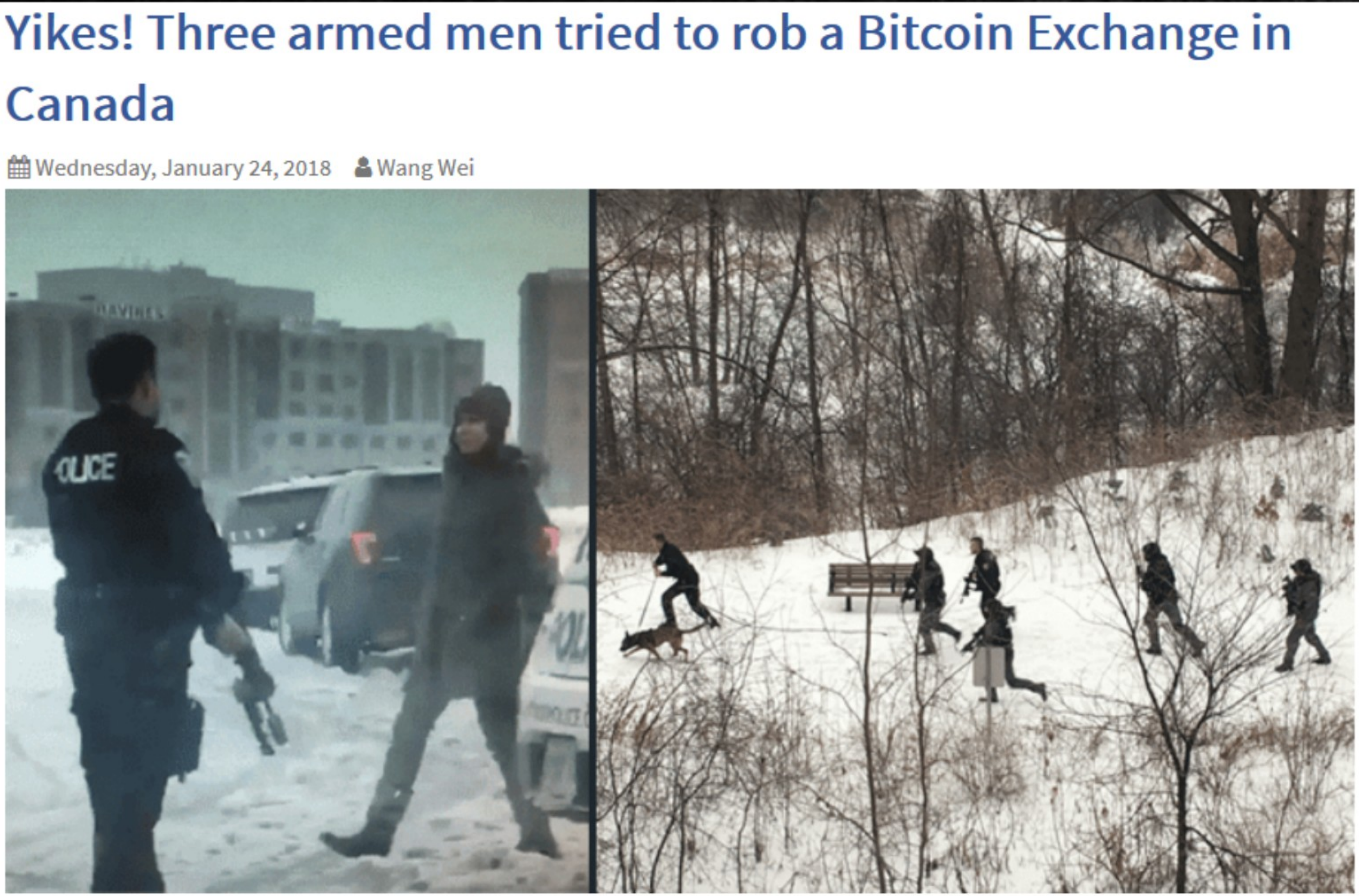
15-Year-Old Schoolboy Posed as CIA Chief to Hack Highly Sensitive Information

Friday, January 19, 2018 Mohit Kumar

Remember "Crackas With Attitude"? A notorious pro-Palestinian hacking group behind a series of embarrassing hacks against United States intelligence officials and leaked the personal details of 20,000 [...]

Intel Warns Users Not to Install Its 'Faulty' Meltdown and Spectre Patches

Tuesday, January 23, 2018 Swati Khandelwal

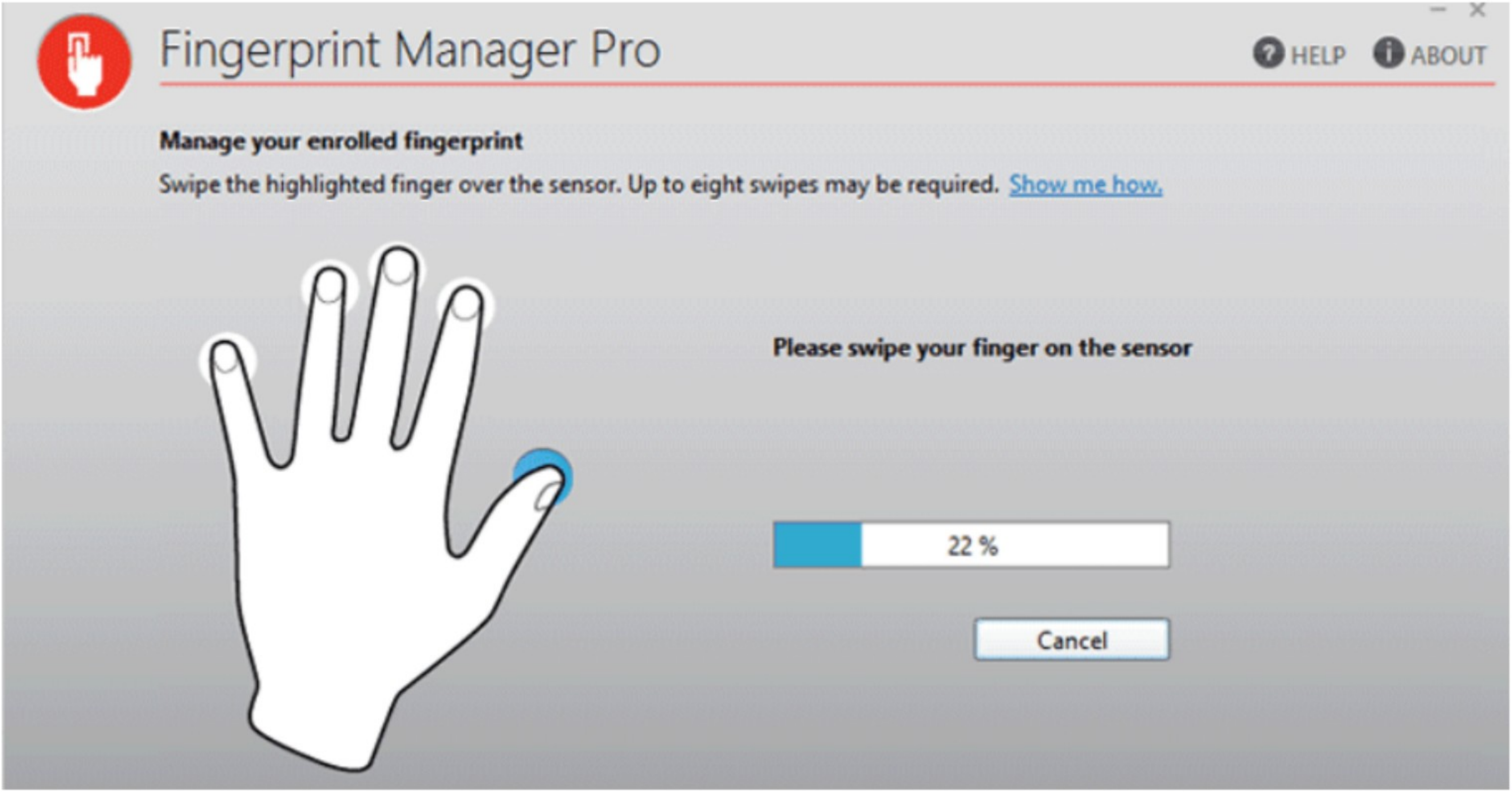


Yikes! Three armed men tried to rob a Bitcoin Exchange in Canada

Wednesday, January 24, 2018 Wang Wei

Hard-coded Password Lets Attackers Bypass Lenovo's Fingerprint Scanner

Monday, January 29, 2018 Wang Wei



Manage your enrolled fingerprint

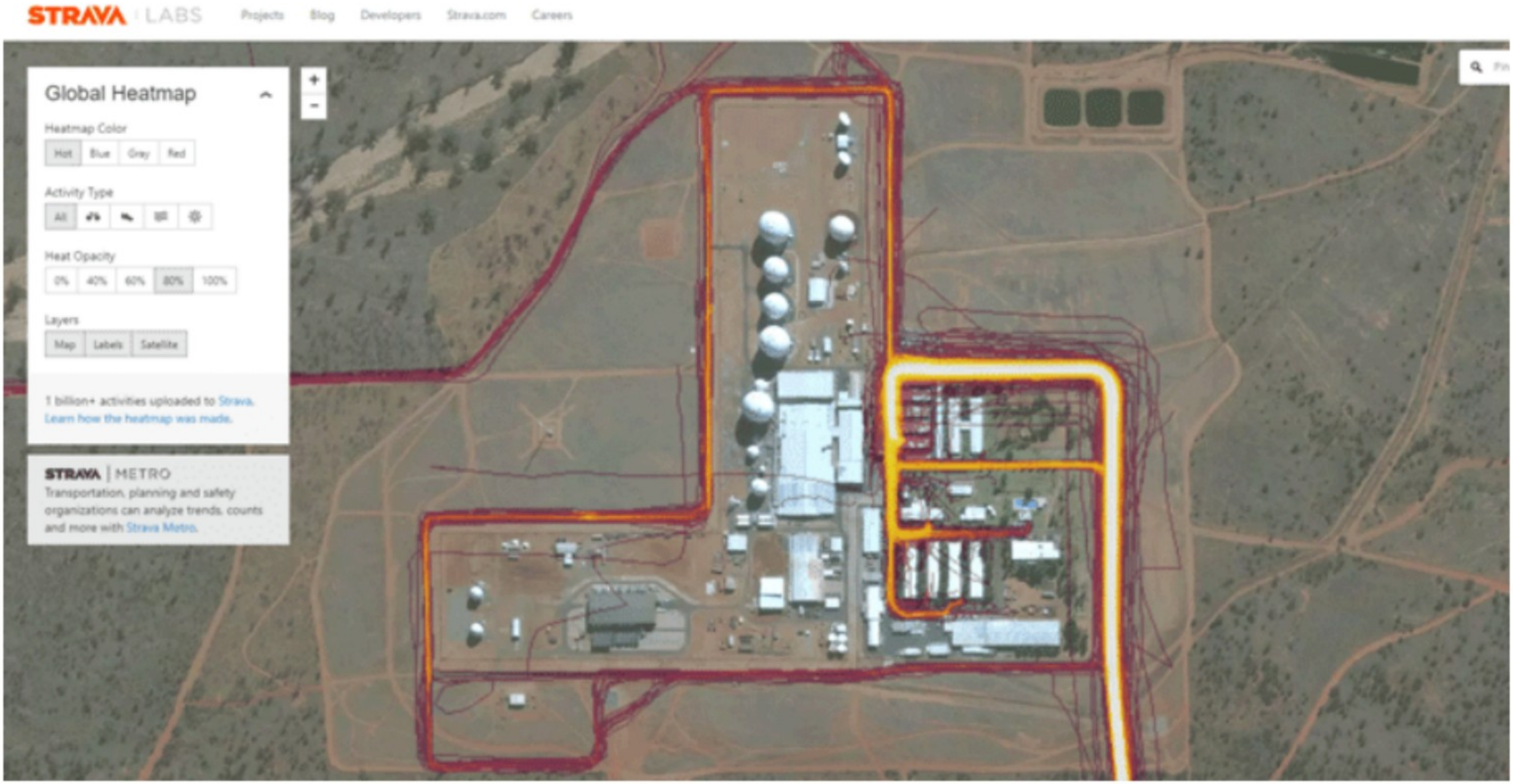
Swipe the highlighted finger over the sensor. Up to eight swipes may be required. Show me how.

Please swipe your finger on the sensor

22 %

Heat Map Released by Fitness Tracker Reveals Location of Secret Military Bases

📅 Monday, January 29, 2018 👤 Swati Khandelwal



Heatmap Color: Hot

Activity Type: All

Heat Opacity: 80%

1 billion+ activities uploaded to Strava.
Learn how the heatmap was made.

Transportation, planning and safety organizations can analyze trends, counts and more with Strava Metro.

Protect your Data!

Offsite?

Air gap?

Which media?

How many copies?

"This is not technically off-site storage"
"What, do I need a longer pole?"

DESIGNERHIPSTER.COM

ITRC
IDENTITY THEFT
RESOURCE CENTER

For 2017 the ITRC reported 1,579 breaches

As of Sept 5, 2018 there has been 864 reported breaches

https://www.idtheftcenter.org/wp-content/uploads/2018/09/2018-August-Data-Breach-Package.pdf

DAVE'S THE TOP TEN LIST

10. Treat your network as a hostile environment, always assume breached

9. Nobody is immune to malware infection so have your post breach strategy ready

8. Don't forget about the insider threat

7. Always do #2

6. Know your network & Log everything

DAVE'S

5. Backup, Backup then test your backups

4. Train your Security staff

3. Security awareness for everyone

2. Patch, Patch, & Patch...   Refer back to #7

1. Alec Baldwin was not available