Insider Threats

Stories from outside the cubicle!

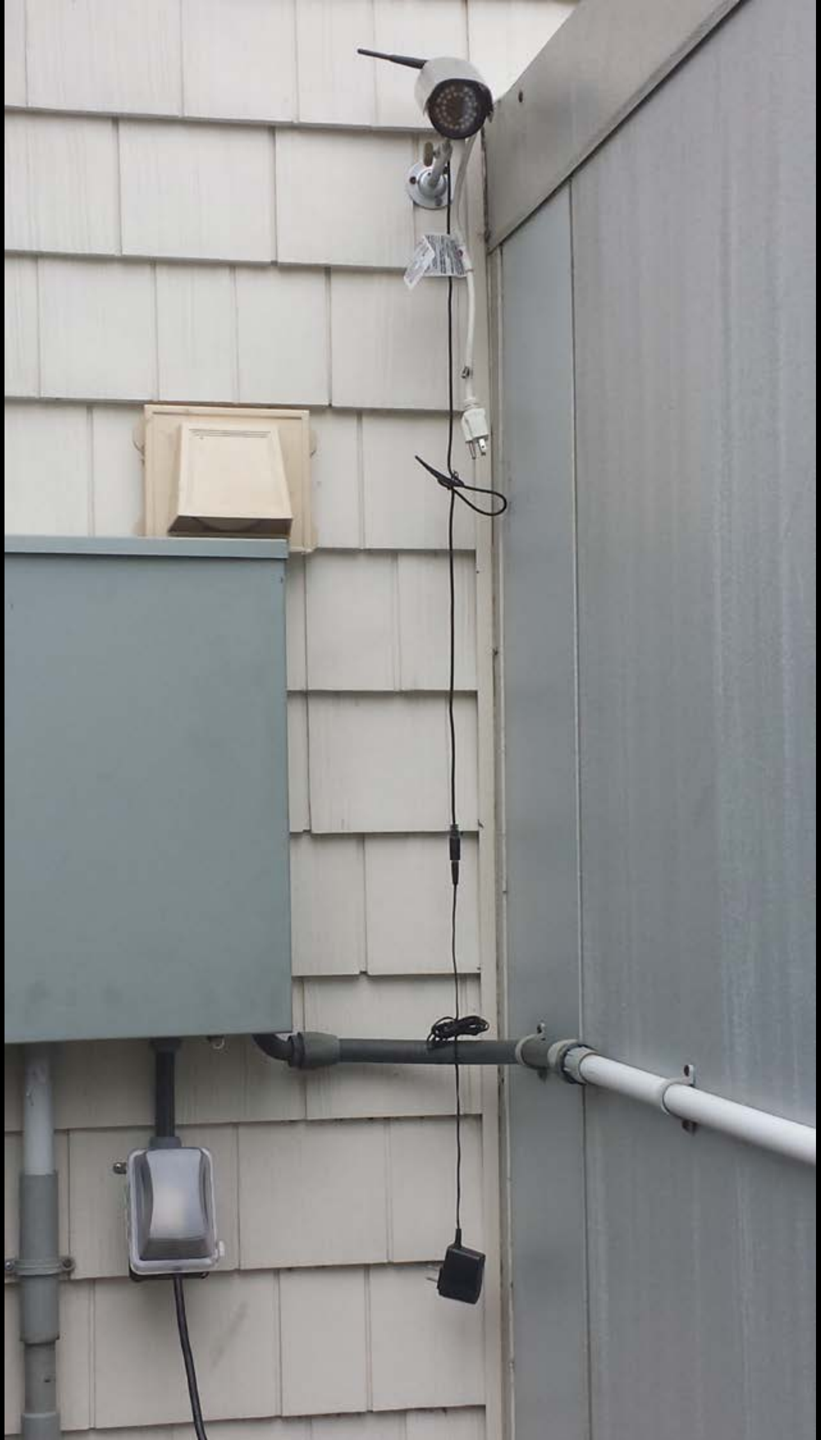
David Balcar
Security Strategist

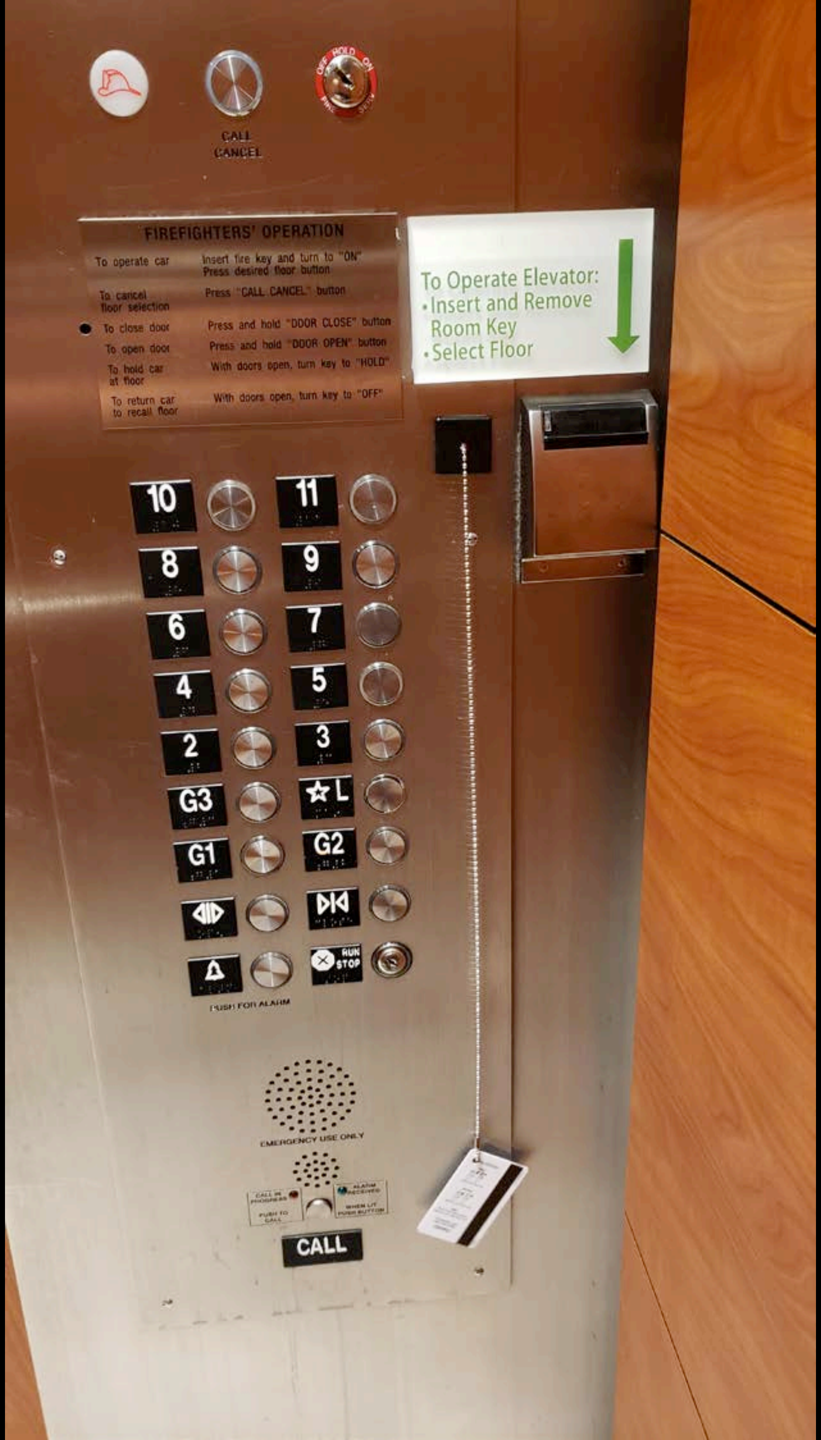
dbalcar@vmware.com

@network232

Toque vs Beanie?

Threat Landscape



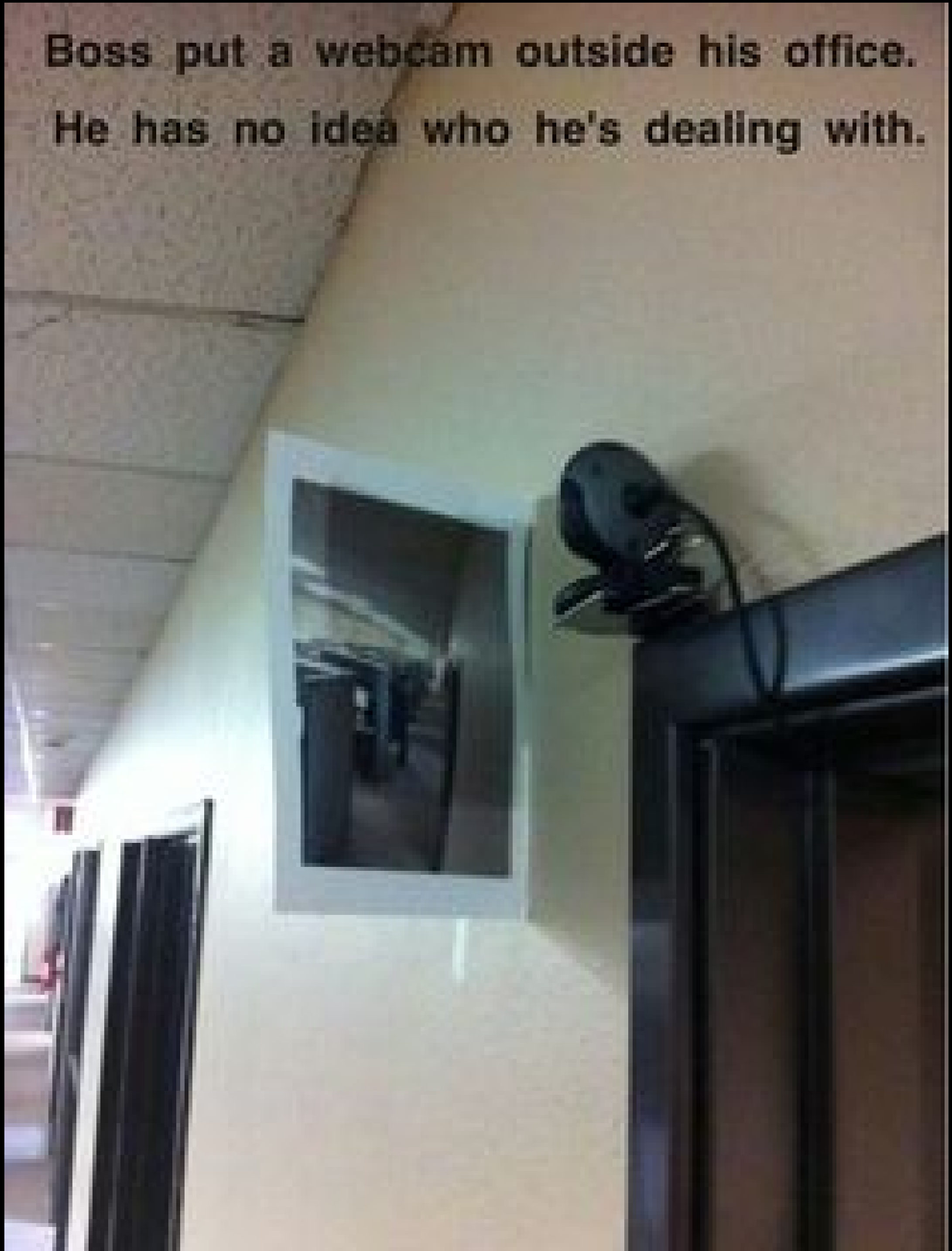


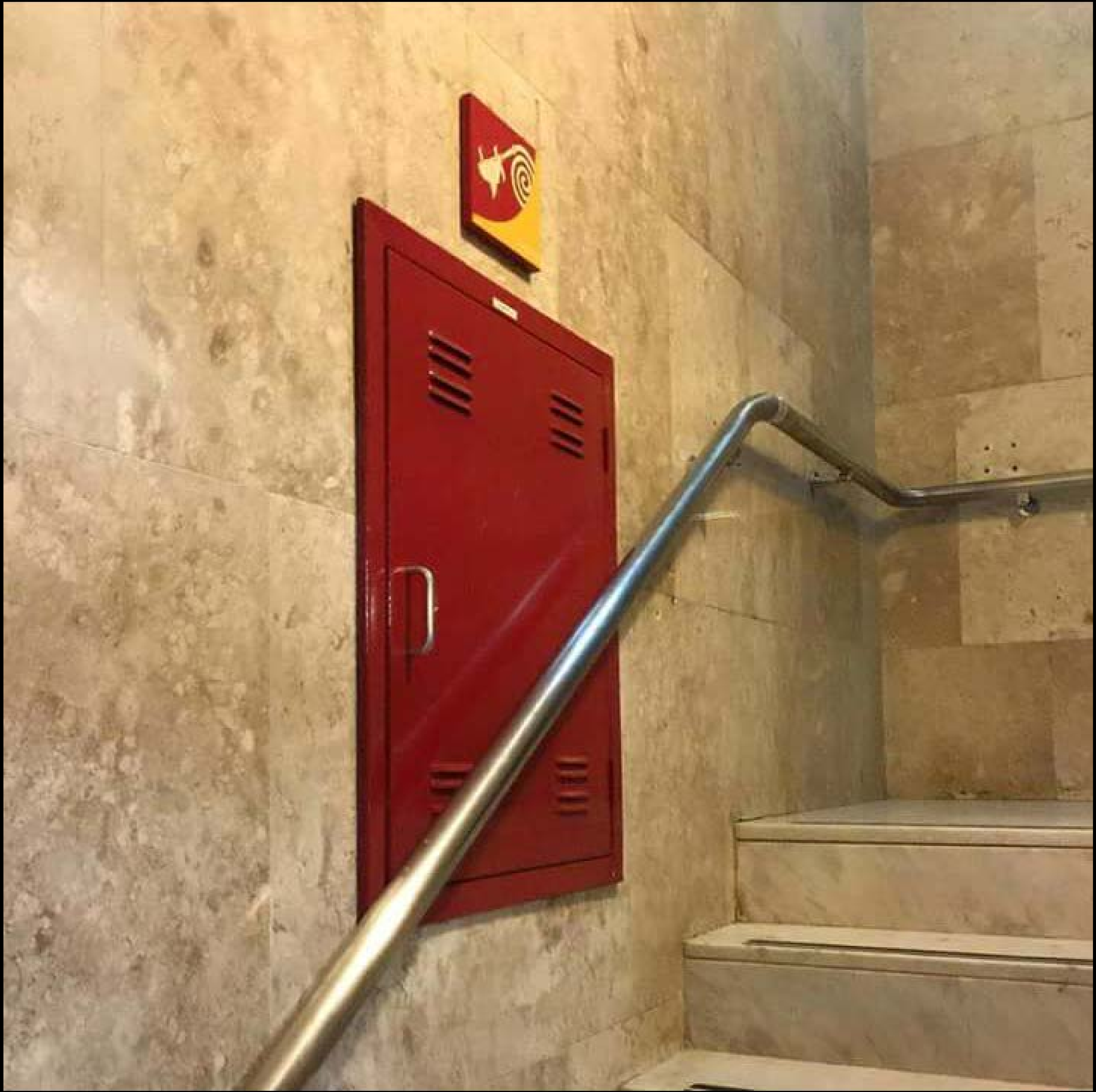
FIREFIGHTERS' OPERATION

To operate car	Insert fire key and turn to "ON" Press desired floor button
To cancel floor selection	Press "CALL CANCEL" button
To close door	Press and hold "DOOR CLOSE" button
To open door	Press and hold "DOOR OPEN" button
To hold car at floor	With doors open, turn key to "HOLD"
To return car to recall floor	With doors open, turn key to "OFF"

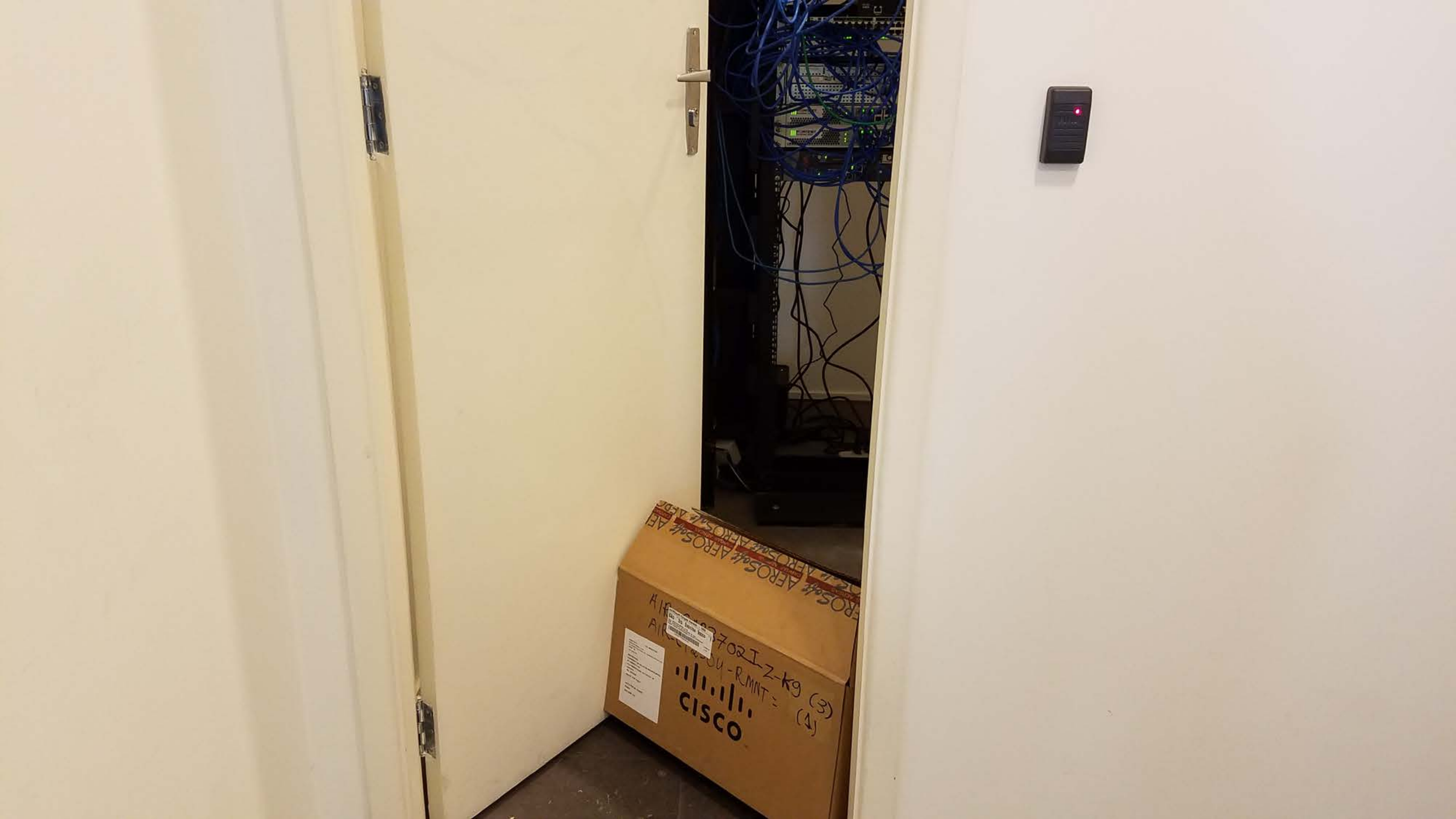
To Operate Elevator:

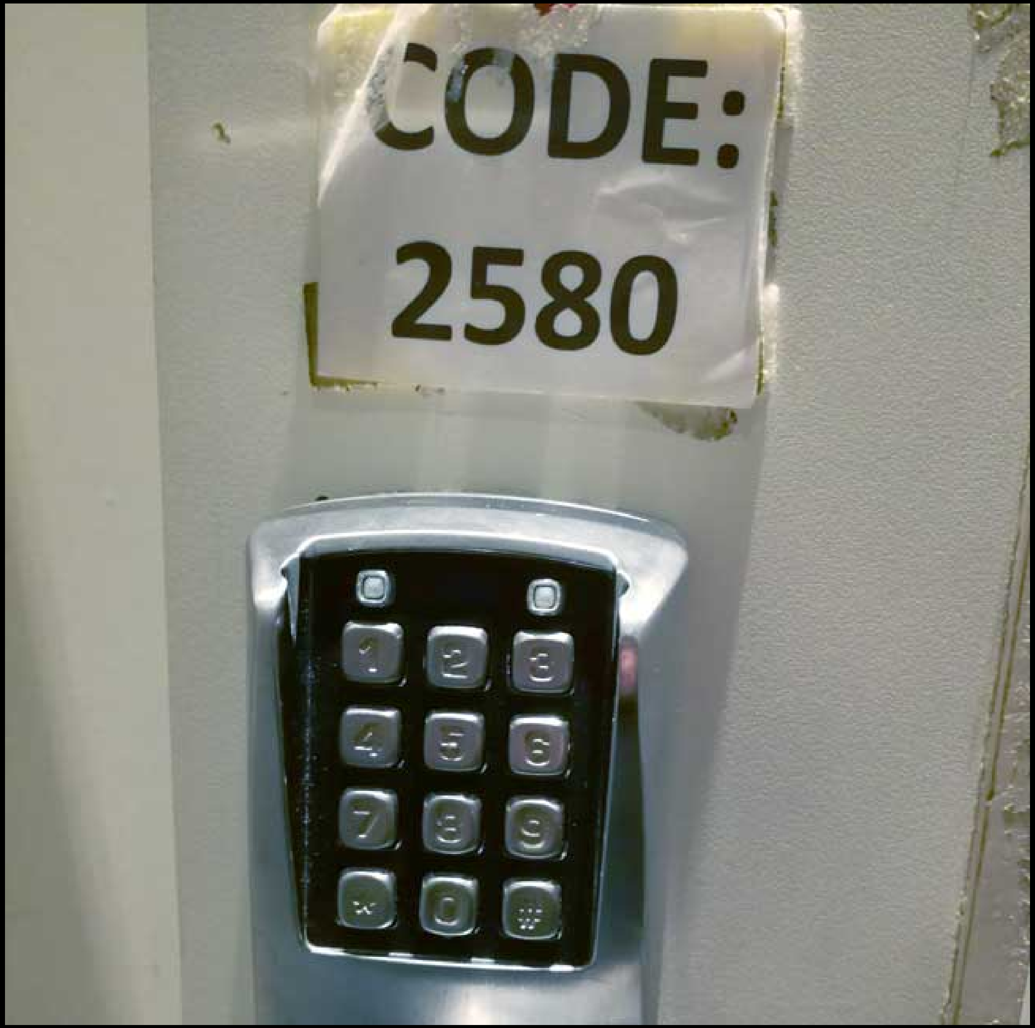
- Insert and Remove Room Key
- Select Floor

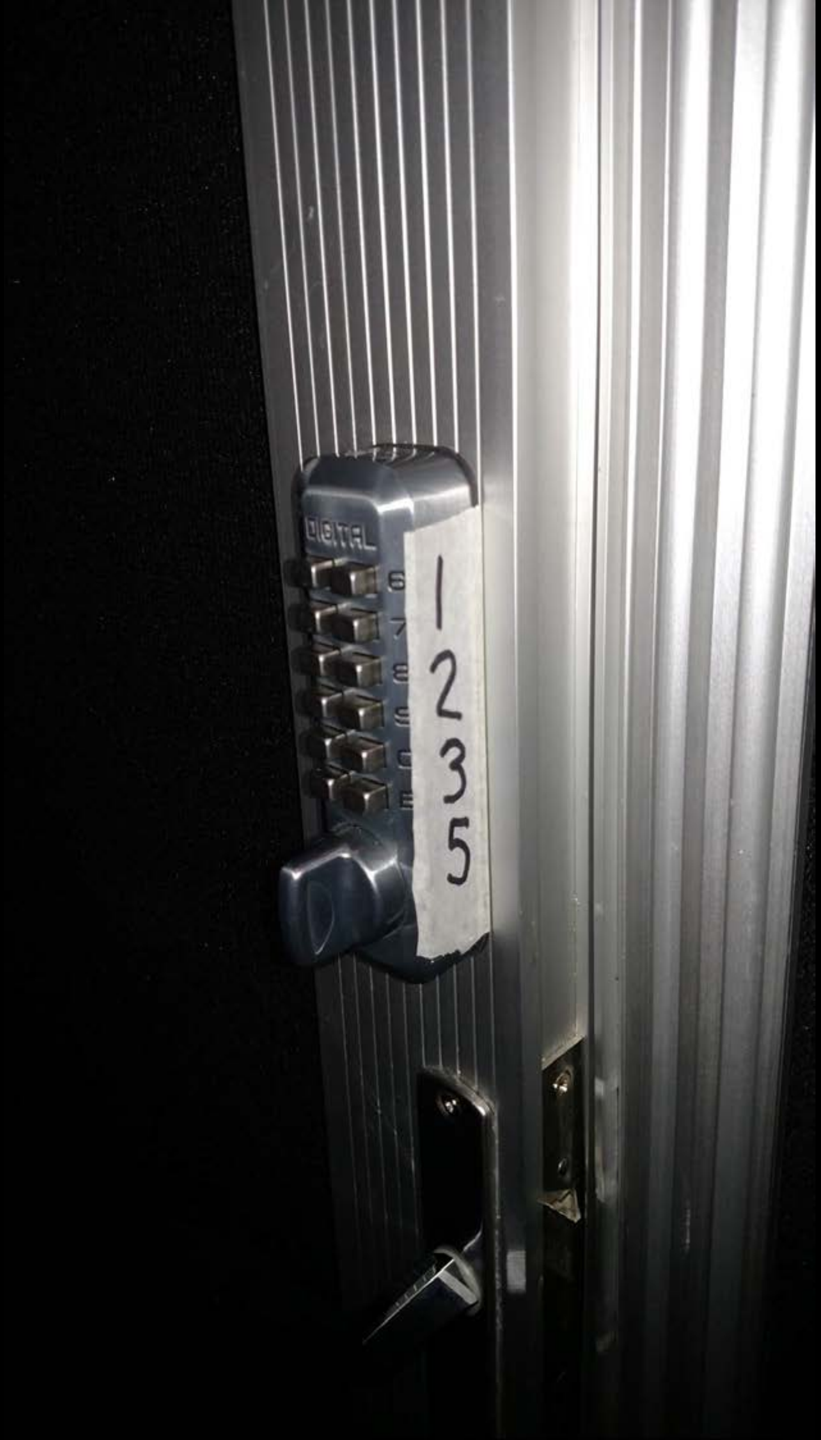

Boss put a webcam outside his office.
He has no idea who he's dealing with.

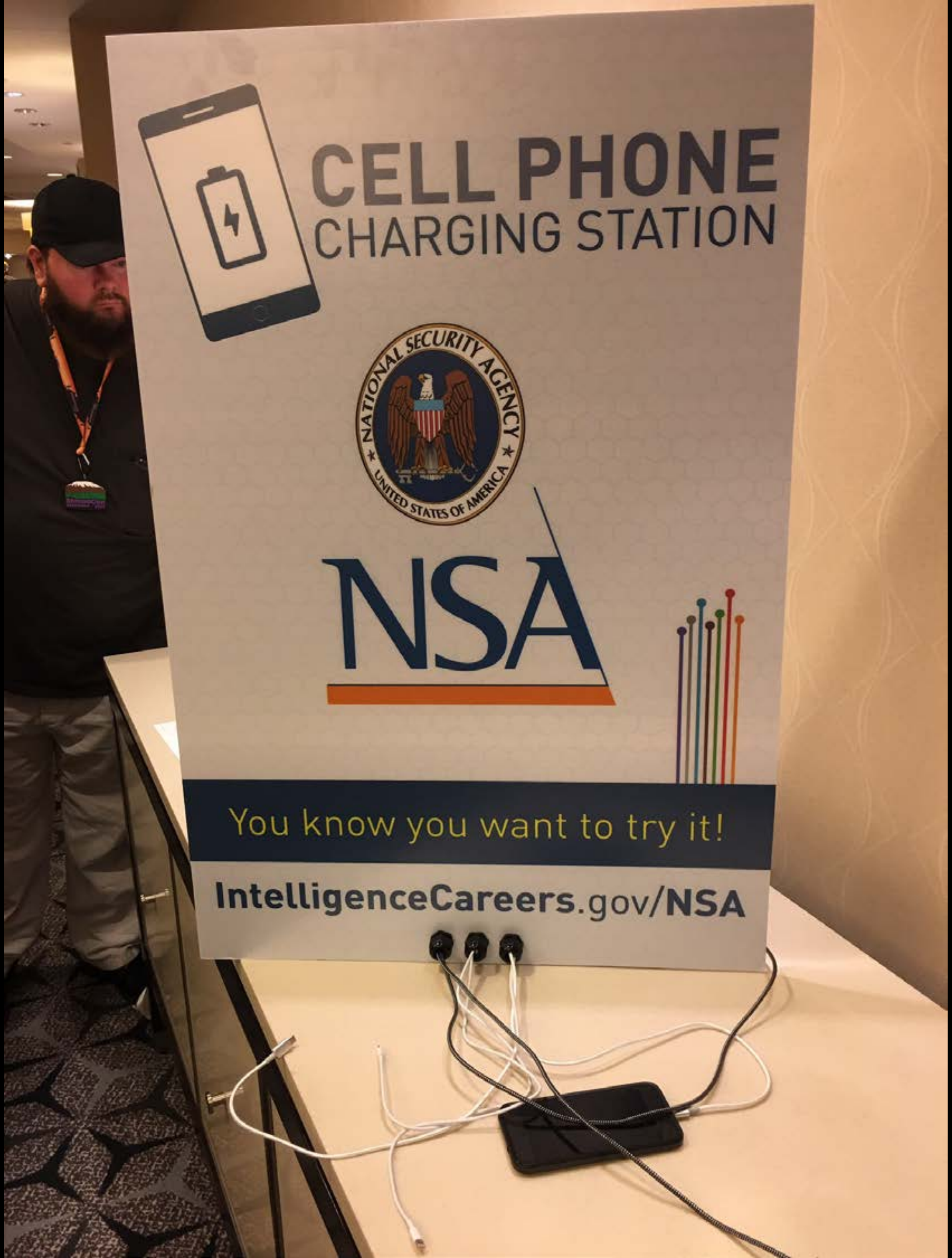


EMERGENCY TELEPHONE
Dial 999 for Coastguard,
Police, Fire or Ambulance
BT
1
2
3

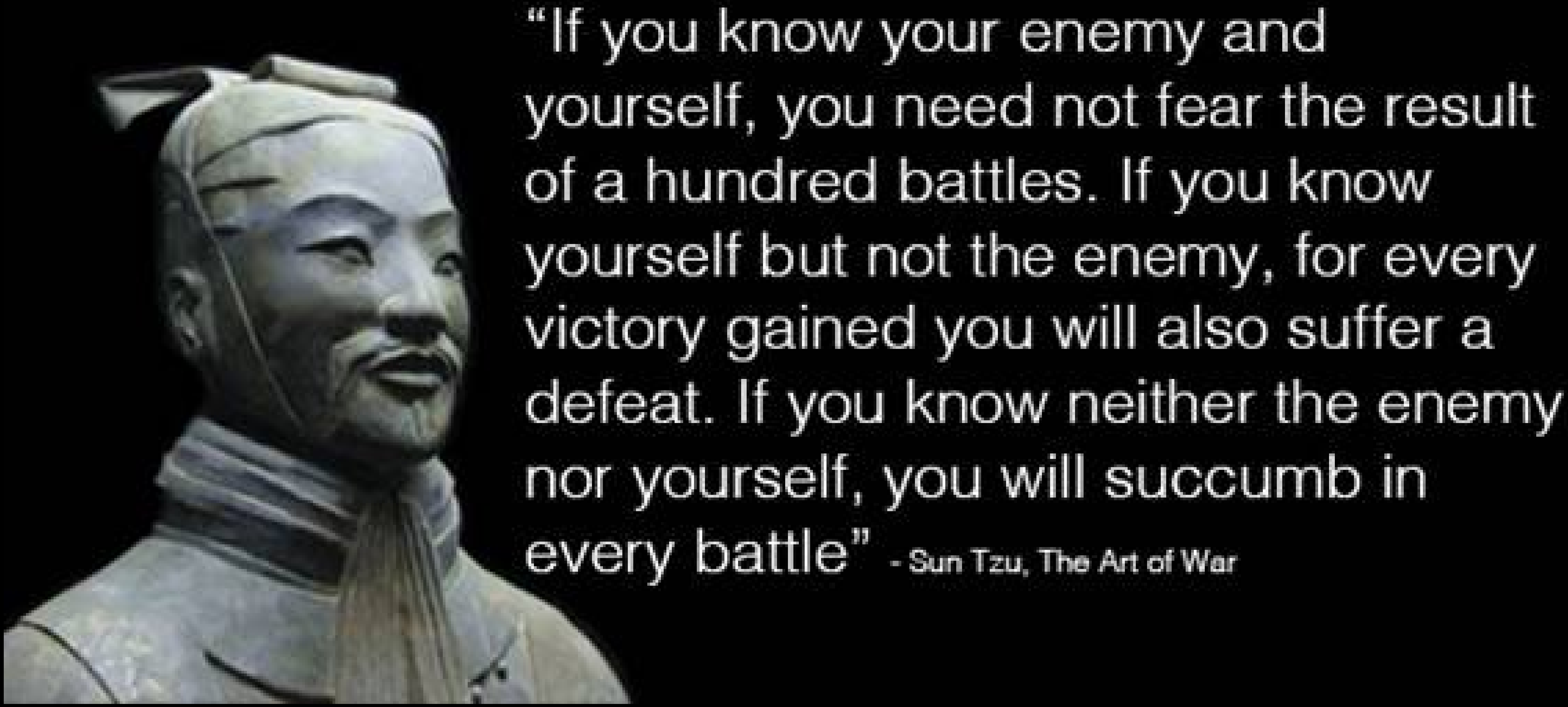

AEROSafe
AIR-C 3702I-Z-K9 (3)
AIR-CT2504-RMNT= (1)
CISCO


CODE:
2580
1 2 3
4 5 6
7 8 9
* 0 #


DIGITAL
1
2
3
5


CELL PHONE
CHARGING STATION
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
NSA
You know you want to try it!
IntelligenceCareers.gov/NSA

wikipedia...



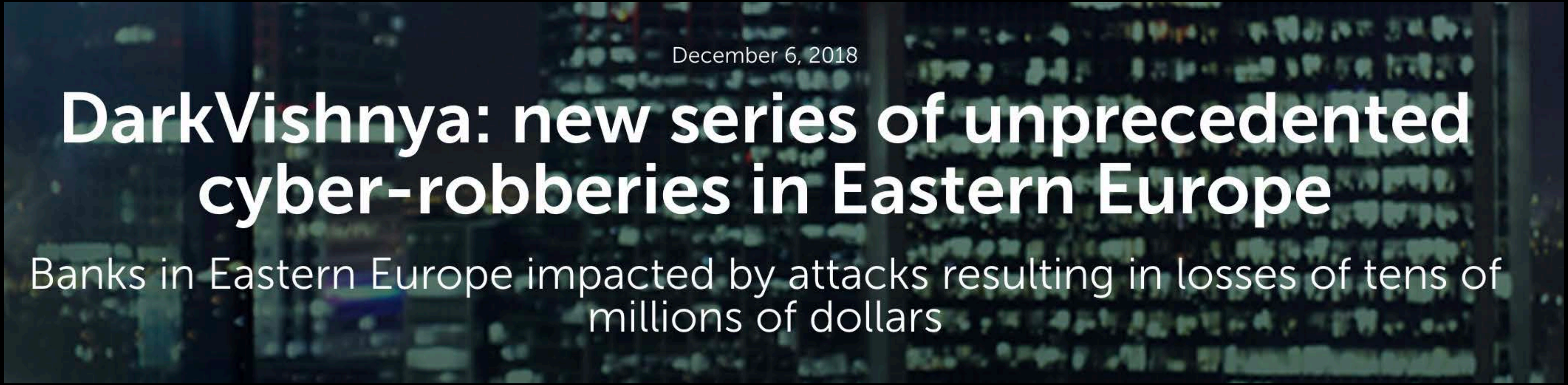
“If you know your enemy and yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle” - Sun Tzu, The Art of War

What does Hollywood say?

Espionage?

Whistleblower?

Say it isn't so...



December 6, 2018

DarkVishnya: new series of unprecedented cyber-robberies in Eastern Europe

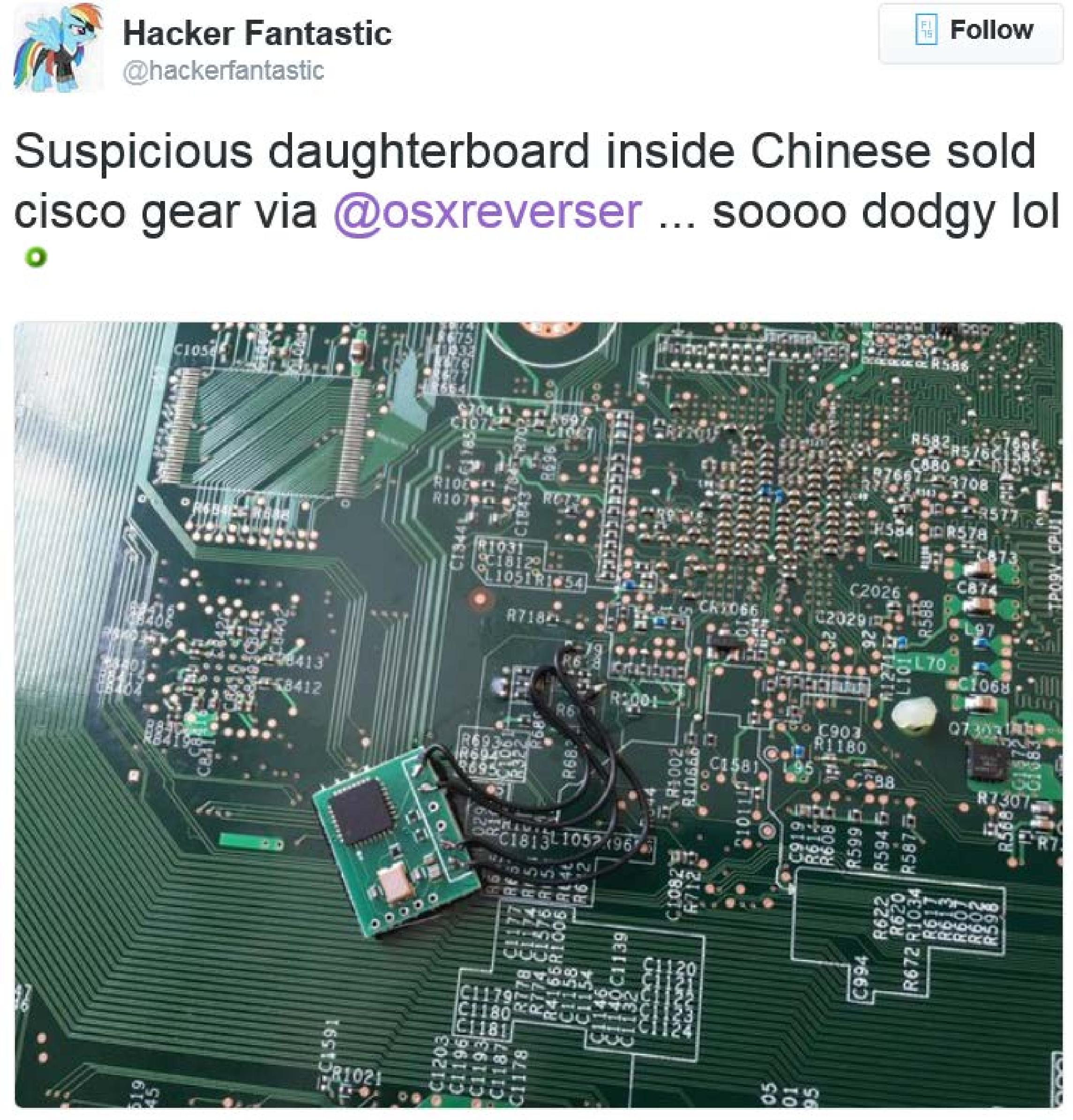
Banks in Eastern Europe impacted by attacks resulting in losses of tens of millions of dollars

Through Kaspersky Lab’s involvement in the incident response, researchers discovered that in each case the corporate network was breached through an unknown device, controlled by the attackers, which had been smuggled into a company building and connected to the network.

The attackers used three types of devices: a laptop, a Raspberry Pi (a single-board computer size of a credit card) or a Bash Bunny (a specially designed tool for automating and conducting USB attacks), equipped with a GPRS, 3G- or LTE- modem that allowed the attackers to penetrate remotely the corporate network of the financial organization.

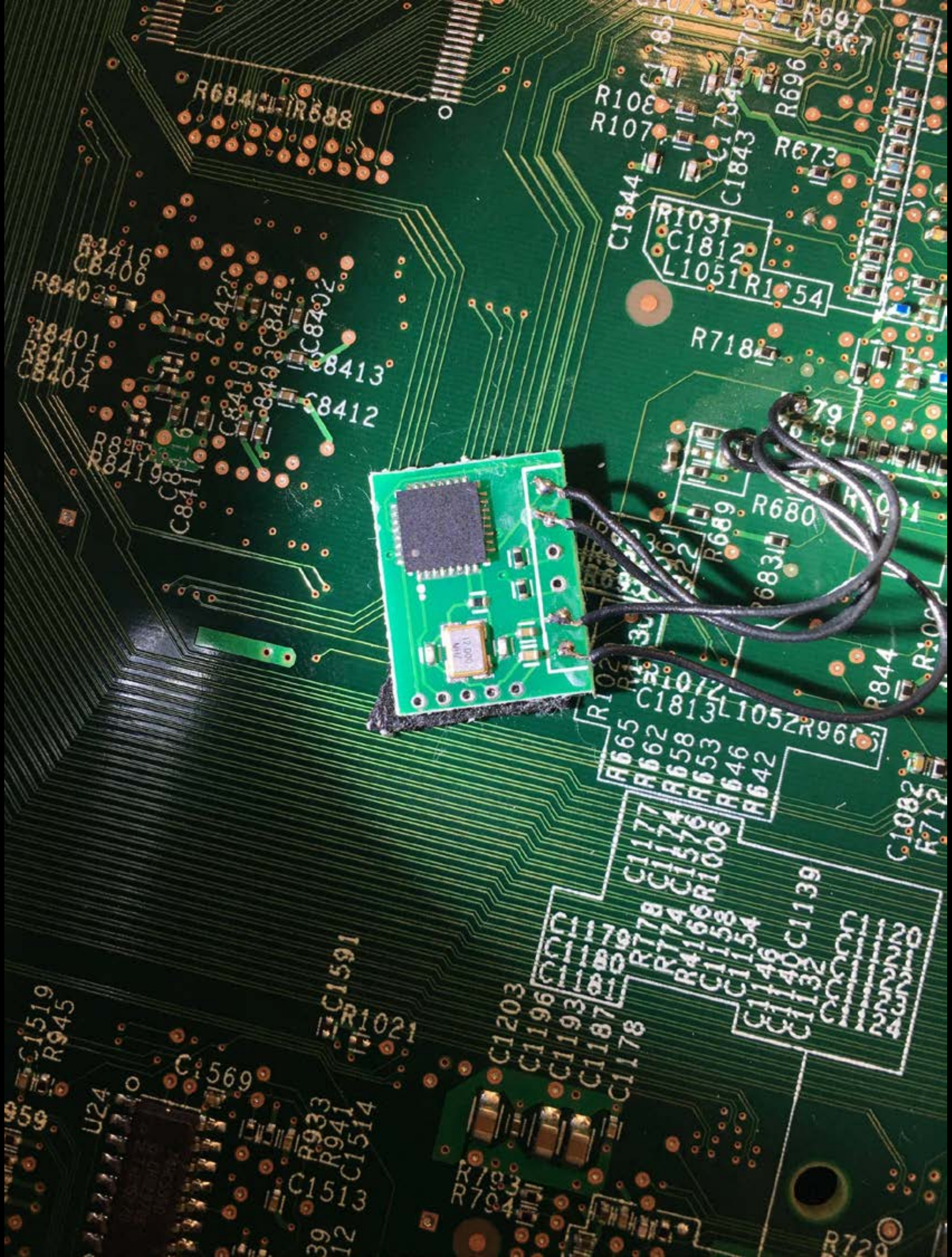
https://usa.kaspersky.com/about/press-releases/2018_darkvishnya-new-series-of-unprecedented-cyber-robberies-in-eastern-europe

Pictures are worth a thousand words...

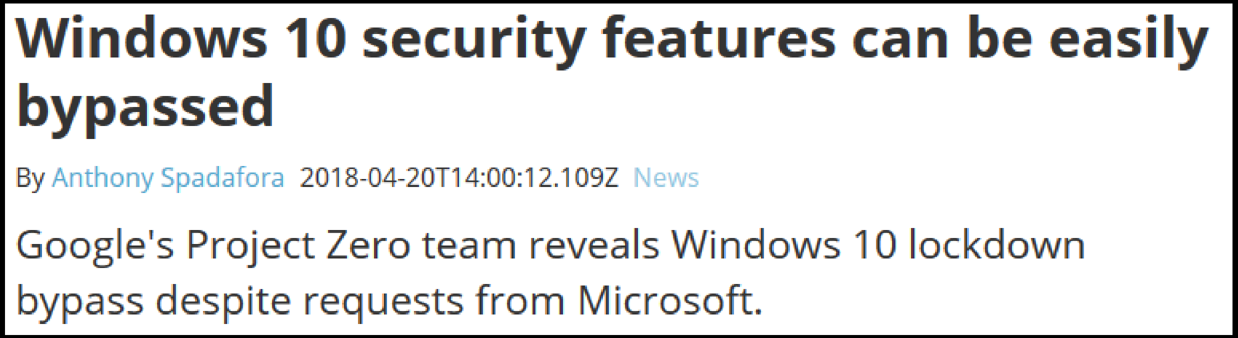


Hacker Fantastic
@hackerfantastic

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


R684
R688
R697
C1067
R696
R108
R107
C1843
R673
C1844
R1031
C1812
L1051
R1054
R8416
C8406
R8403
R8401
R8415
C8404
C8402
C8413
C8412
R8419
R718
R680
R689
R683
R844
C1813
L1052
R965
R665
R662
R658
R653
R646
R642
C1082
R712
C1177
C1174
C1175
R1006
C1139
C1179
C1180
C1181
R778
R774
R416
C1158
C1154
C1146
C1140
C1132
C1120
C1121
C1122
C1123
C1124
C1591
R1021
C1519
R945
C1569
U24
C1203
C1196
C1193
C1187
C1178
R933
R941
C1514
C1513
R793
R794
R729

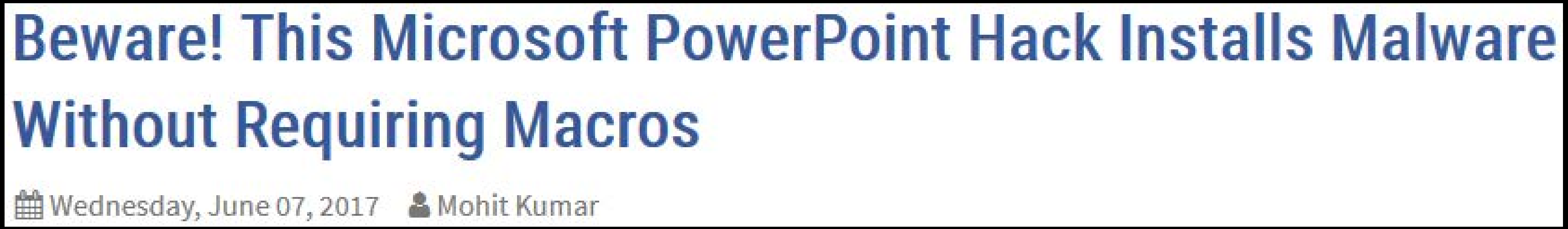
Just the Facts...



Windows 10 security features can be easily bypassed

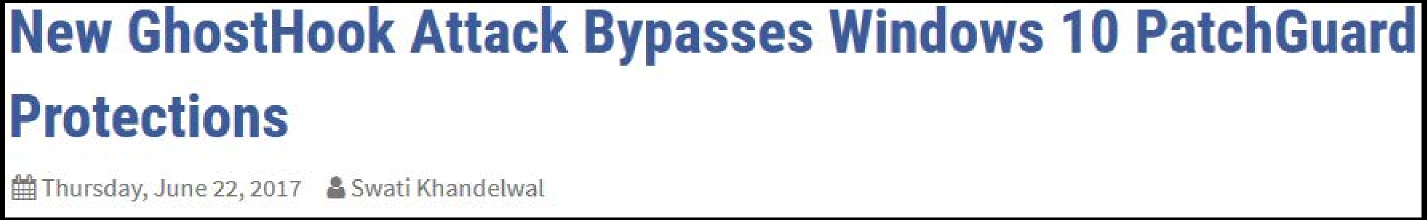
By Anthony Spadafora 2018-04-20T14:00:12.109Z News

Google's Project Zero team reveals Windows 10 lockdown bypass despite requests from Microsoft.



Beware! This Microsoft PowerPoint Hack Installs Malware Without Requiring Macros

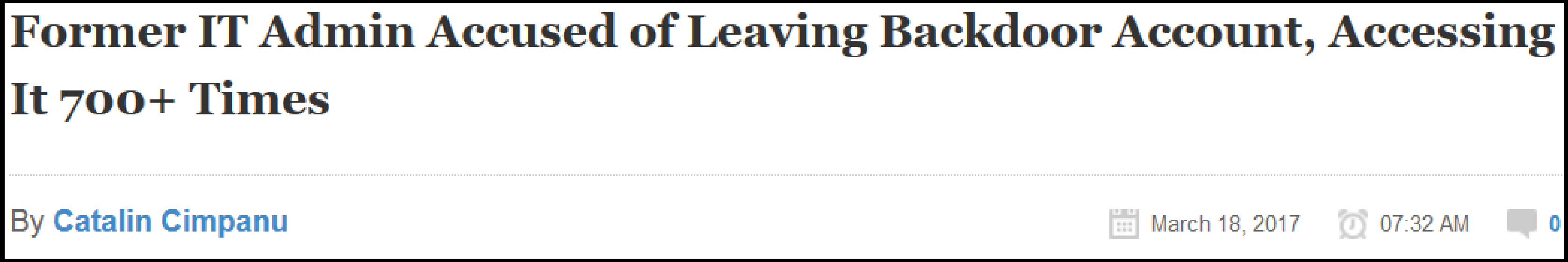
Wednesday, June 07, 2017 Mohit Kumar



New GhostHook Attack Bypasses Windows 10 PatchGuard Protections

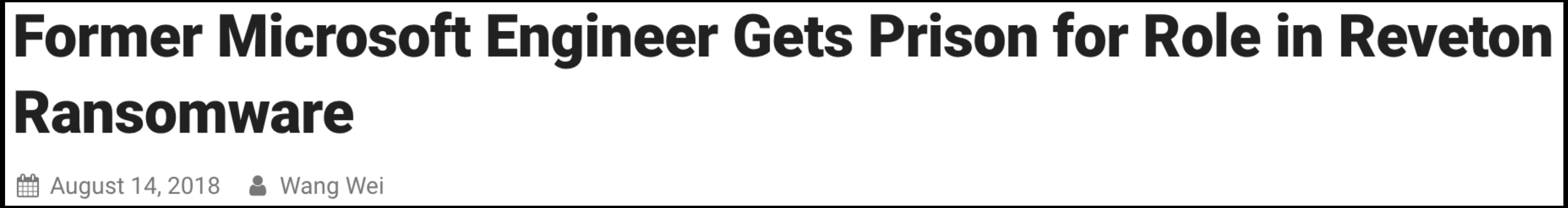
Thursday, June 22, 2017 Swati Khandelwal

In the News!



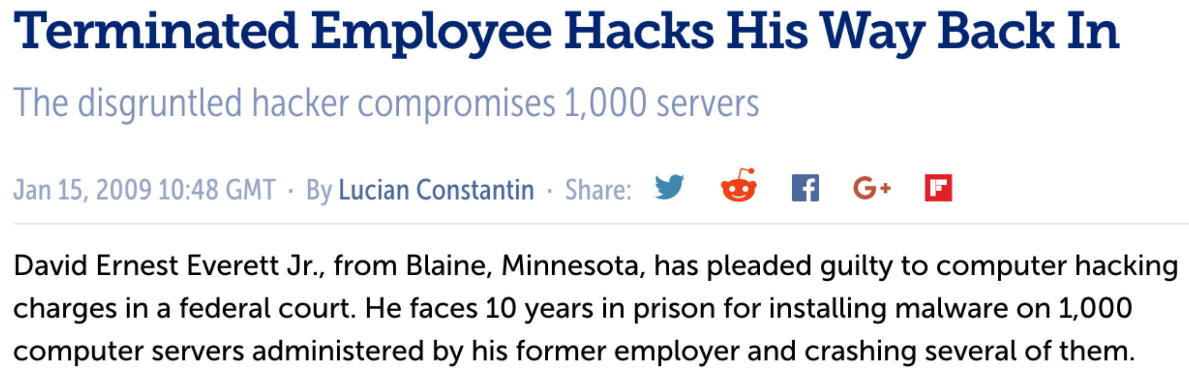
Former IT Admin Accused of Leaving Backdoor Account, Accessing It 700+ Times

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



Former Microsoft Engineer Gets Prison for Role in Reveton Ransomware

August 14, 2018 Wang Wei

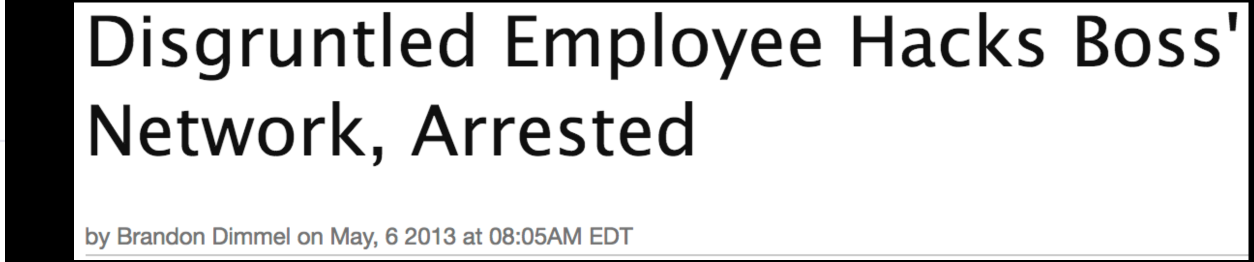


Terminated Employee Hacks His Way Back In

The disgruntled hacker compromises 1,000 servers

Jan 15, 2009 10:48 GMT · By Lucian Constantin · Share:

David Ernest Everett Jr., from Blaine, Minnesota, has pleaded guilty to computer hacking charges in a federal court. He faces 10 years in prison for installing malware on 1,000 computer servers administered by his former employer and crashing several of them.

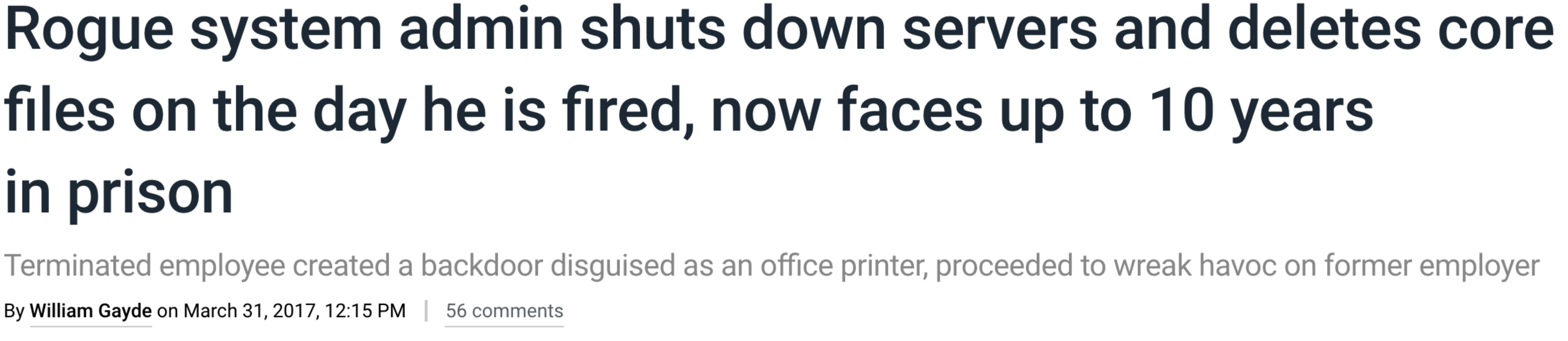


Disgruntled Employee Hacks Boss' Network, Arrested

by Brandon Dimmel on May, 6 2013 at 08:05AM EDT

https://www.techspot.com/news/68753-rogue-system-administrator-shuts-down-servers-deletes-core.html
https://news.softpedia.com/news/Terminated-Employee-Hacked-His-Way-Back-In-102053.shtml
https://www.infopackets.com/news/8404/disgruntled-employee-hacks-boss-network-arrested

In the News!



Rogue system admin shuts down servers and deletes core files on the day he is fired, now faces up to 10 years in prison

Terminated employee created a backdoor disguised as an office printer, proceeded to wreak havoc on former employer

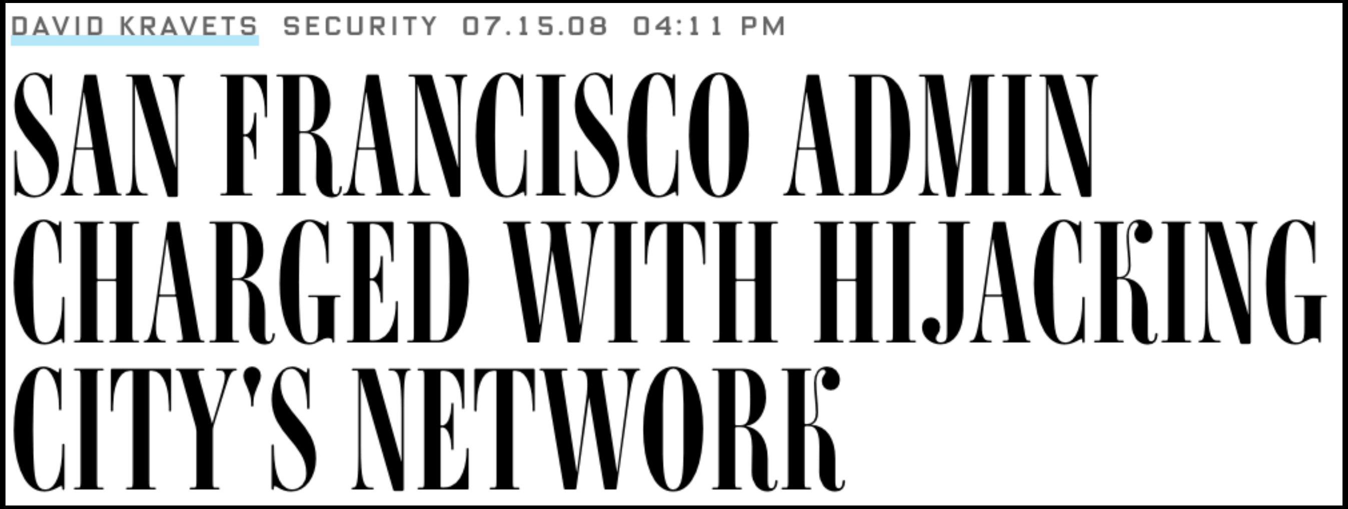
By **William Gayde** on March 31, 2017, 12:15 PM | 56 comments

Story from outside the cubical...

A LONG TIME AGO IN A NETWORK

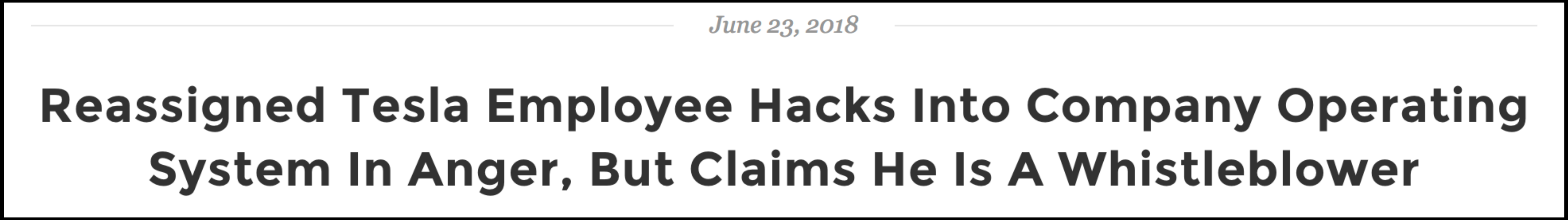
FAR, FAR AWAY

In the News!



DAVID KRAVETS SECURITY 07.15.08 04:11 PM

SAN FRANCISCO ADMIN CHARGED WITH HIJACKING CITY'S NETWORK

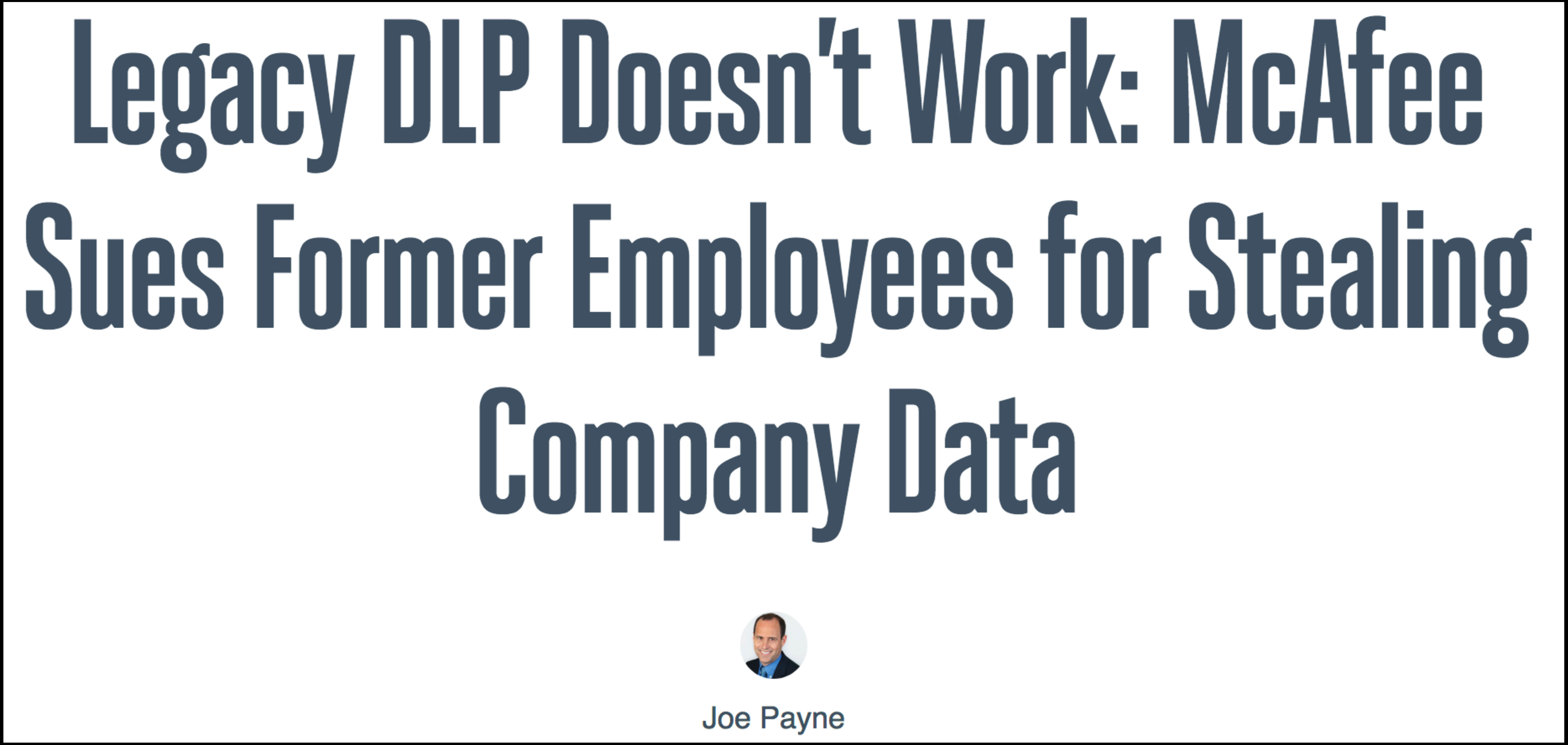


June 23, 2018

Reassigned Tesla Employee Hacks Into Company Operating System In Anger, But Claims He Is A Whistleblower

https://www.inquisitr.com/4954984/reassigned-tesla-employee-hacks-into-company-operating-system-in-anger-but-claims-he-is-a-whistleblower/

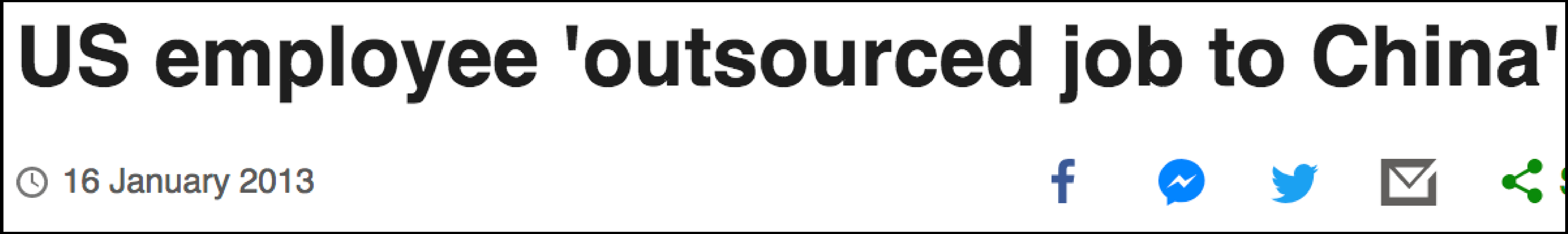
Good News!



Legacy DLP Doesn't Work: McAfee Sues Former Employees for Stealing Company Data

Joe Payne

Honorable Mention insider threat!



US employee 'outsourced job to China'

16 January 2013

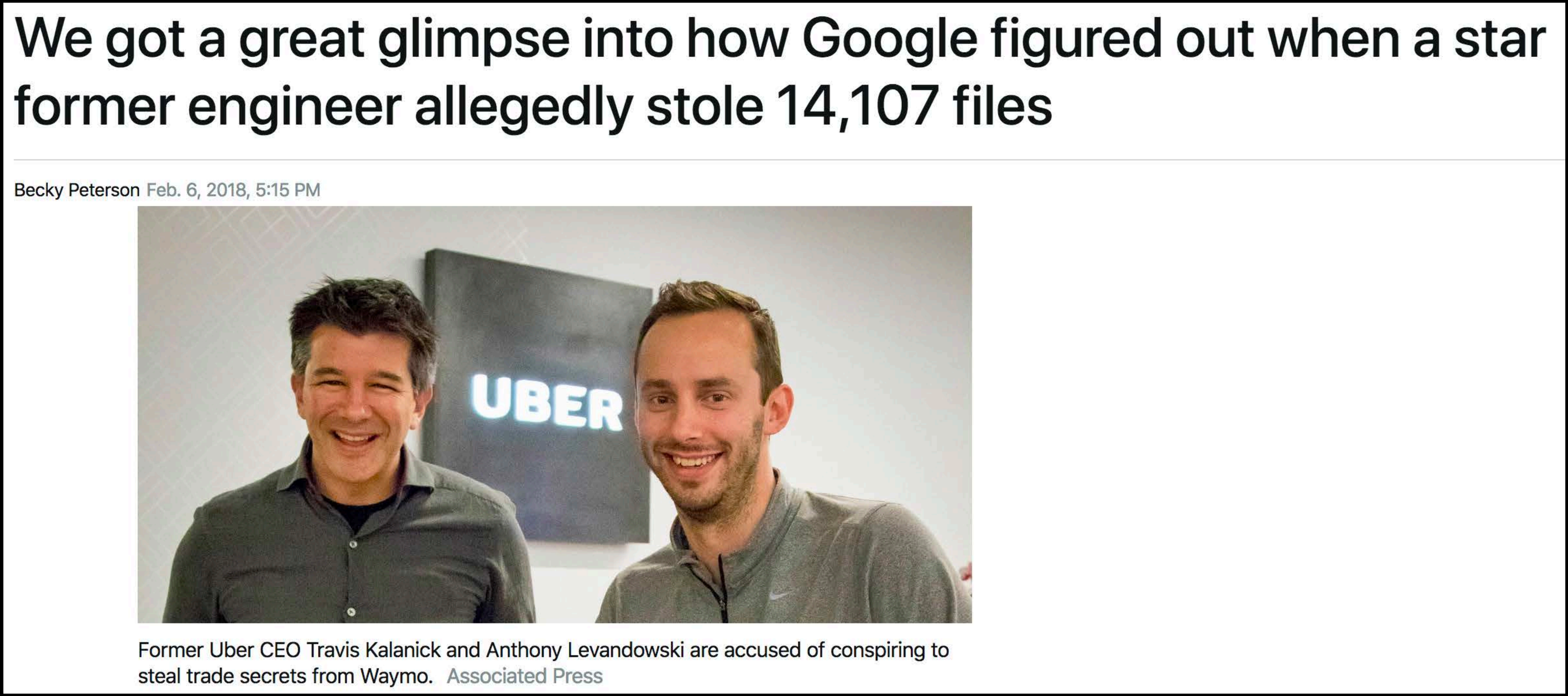
A security check on a US company has reportedly revealed one of its staff was outsourcing his work to China. The software developer, in his 40s, is thought to have spent his workdays surfing the web, watching cat videos on YouTube and browsing Reddit and eBay. He reportedly paid just a fifth of his six-figure salary to a company based in Shenyang to do his job.

"Authentication was no problem. He physically FedExed his RSA [security] token to China so that the third-party contractor could log-in under his credentials during the workday. It would appear that he was working an average nine-to-five work day," he added.

"Evidence even suggested he had the same scam going across multiple companies in the area. All told, it looked like he earned several hundred thousand dollars a year, and only had to pay the Chinese consulting firm about $50,000 (£31,270) annually."

https://www.bbc.com/news/technology-21043693

WTF!



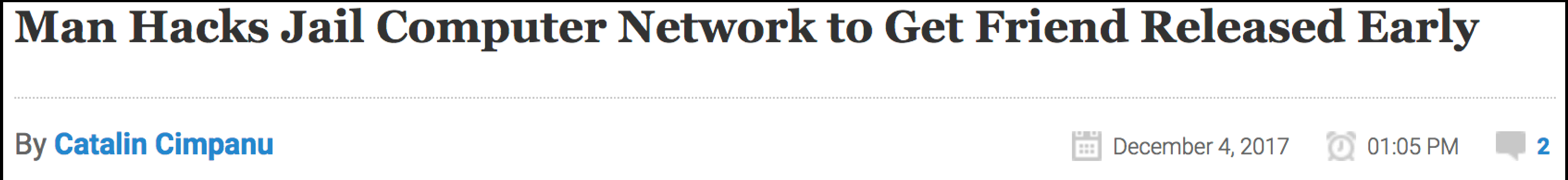
We got a great glimpse into how Google figured out when a star former engineer allegedly stole 14,107 files

Becky Peterson Feb. 6, 2018, 5:15 PM

Former Uber CEO Travis Kalanick and Anthony Levandowski are accused of conspiring to steal trade secrets from Waymo. Associated Press

https://www.businessinsider.com/uber-vs-waymo-how-google-figured-out-secrets-2018-2

The best insider threat!



Man Hacks Jail Computer Network to Get Friend Released Early

By Catalin Cimpanu December 4, 2017 01:05 PM 2

Stats...

Insider threats pose the biggest security risk

By Ian Barker | Published 5 days ago

According to a new study 91% of IT and security professionals feel vulnerable to insider threats, and 75% believe the biggest risks lie in cloud applications like popular file storage and email solutions including Google Drive, Gmail and Dropbox.

The report from SaaS operations management specialist BetterCloud also shows 62 percent of respondents believe the biggest security threat comes from the well-meaning but negligent end user.

https://betanews.com/2019/03/20/insider-threats-biggest-risk/

Stats...

Code42 2019 Global Data Exposure Report Finds 69% of Security Leaders Say Data Loss Prevention Cannot Stop Insider Threat

Over two-thirds (69%) of organizations say they were breached due to an insider threat and confirm they had a prevention solution in place at the time of the breach.

Over three-quarters (78%) of information security leaders – including those with traditional data loss prevention (DLP) – believe that prevention strategies and solutions are not enough to stop insider threat.

https://www.darkreading.com/attacks-breaches/code42-2019-global-data-exposure-report-finds-69--of-security-leaders-say-data-loss-prevention-cannot-stop-insider-threat/d/d-id/1335994

What are we missing?

Insufficient data protection strategies and solutions

Increasing number of devices with access to sensitive data

Proliferation of sensitive data moving outside the firewall on mobile devices

More employees, contractors, partners accessing the network

Greater complexity of technology

Increasing use of cloud apps and infrastructure

http://haystax.com/wp-content/uploads/2017/03/Insider_Threat_Report_2017_Haystax_FINAL.pdf

ITRC IDENTITY THEFT
RESOURCE CENTER
888.400.5530

For 2018 the ITRC reported 1,244 breaches

As of Oct 10, 2019 there have been 1,152 reported breaches

https://www.idtheftcenter.org/wp-content/uploads/2019/10/2019-September-Data-Breach-Package-1.pdf

Dave's

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

Dave's

5. Log everything / Have Unfiltered data

4. Train your Security staff

3. Security awareness for everyone

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

1. Ryan Reynolds was not available

NOT SURE IF THEY'RE CLAPPING FOR MY PRESENTATION
OR BECAUSE ITS FINISHED

Thank You

Please email any questions to dbalcar@vmware.com