CRITICAL INFORMATICS

Our stuff keeps your stuff from becoming their stuff

UW Tech Connect
March 13, 2018

Trends In Information Security

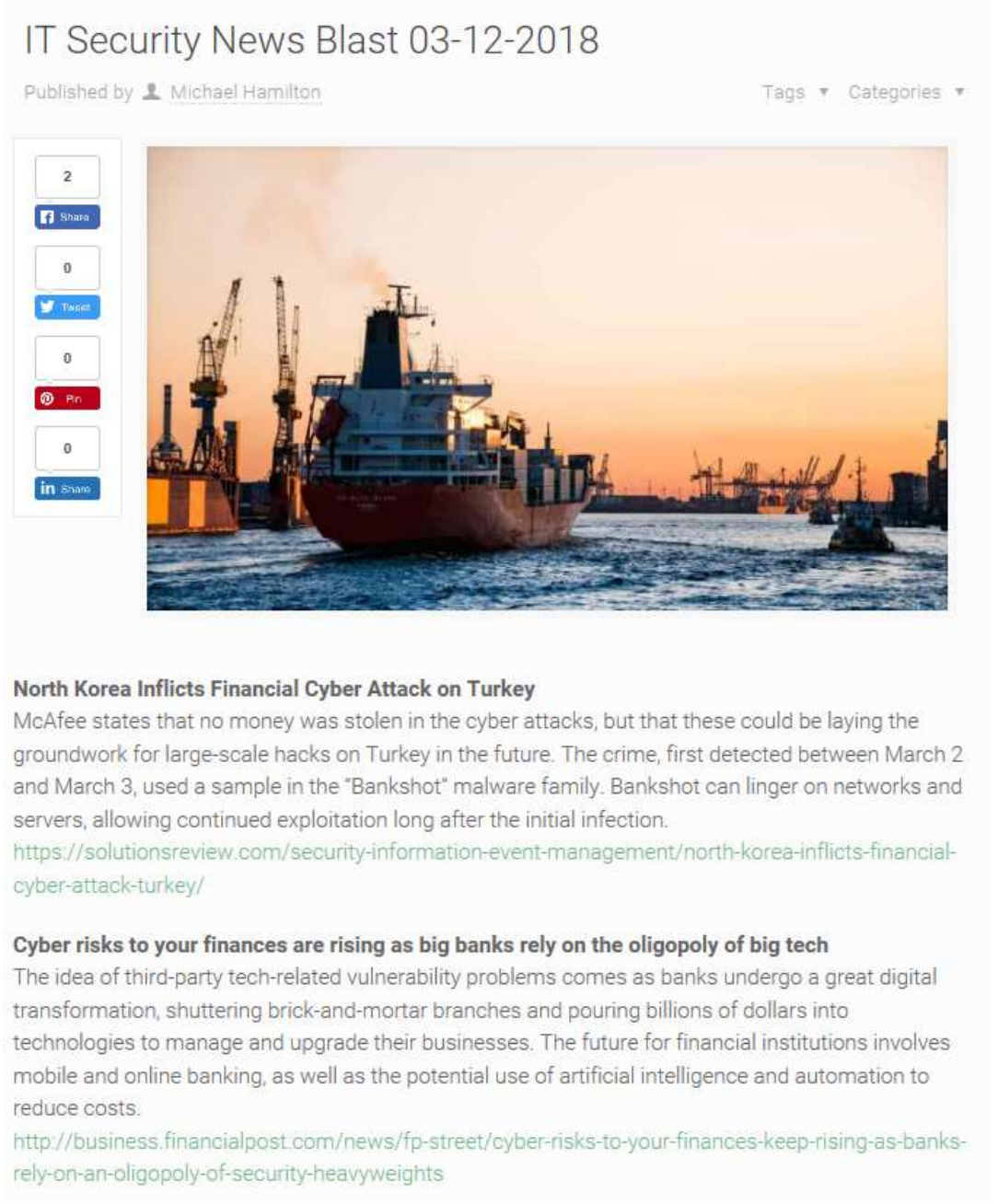
Preparing for an animated future

Outcomes to Avoid

- Records Breach: ~$150/record
- Theft: $75K-$1.2M in our region, multiple millions elsewhere
- Disruption: Loss of business continuity or operating capacity, loss of life for critical services

Leaning Into OSINT

Trends emerge, which lend themselves to prediction, or at least noticing which way the wind is starting to blow



IT Security News Blast 03-12-2018

Published by Michael Hamilton Tags Categories

2 Share 0 Tweet 0 Pin 0 Share

North Korea Inflicts Financial Cyber Attack on Turkey

McAfee states that no money was stolen in the cyber attacks, but that these could be laying the groundwork for large-scale hacks on Turkey in the future. The crime, first detected between March 2 and March 3, used a sample in the "Bankshot" malware family. Bankshot can linger on networks and servers, allowing continued exploitation long after the initial infection.

https://solutionsreview.com/security-information-event-management/north-korea-inflicts-financial-cyber-attack-turkey/

Cyber risks to your finances are rising as big banks rely on the oligopoly of big tech

The idea of third-party tech-related vulnerability problems comes as banks undergo a great digital transformation, shuttering brick-and-mortar branches and pouring billions of dollars into technologies to manage and upgrade their businesses. The future for financial institutions involves mobile and online banking, as well as the potential use of artificial intelligence and automation to reduce costs.

http://business.financialpost.com/news/fp-street/cyber-risks-to-your-finances-keep-rising-as-banks-rely-on-an-oligopoly-of-security-heavyweights

Recent Public Sector Events

Montgomery County Public Schools Says It Was Target of Cyberattack

Electronic disruption lasted three days, district spokesman says

Man Behind 911 Call System 2016 Cyberattack Sentenced to Probation

Meetkumar Desai pleaded guilty in August to felony count of solicitation to commit computer tampering

Cyber-criminals attack Atlanta, Fulton, and Clayton school districts, paychecks stolen

Posted: Oct 03, 2017 9:54 PM PST
Updated: Oct 04, 2017 8:04 PM PST

October 05, 2017

City of Englewood, Colo. hit with ransomware

The attack left the city's civic center unable to process credit cards and the city's library unable to place items on hold or accept late fines, according to an Oct. 4 press release.

Ransomware

Ransomware for robots is the next big security nightmare

Researchers found they were able to infect robots with ransomware; in the real world, such attacks could be highly damaging to businesses if robotic security isn't addressed.

By Danny Palmer | March 9, 2018 -- 15:47 GMT (07:47 PST) | Topic: Security

5 ransomware as a service (RaaS) kits

Connected Cars are vulnerable to Ransomware Attacks

MAY 17, 2017 @ 09:00 AM 24,215

The Little Black Book of Billionaire Secrets

Medical Devices Hit By Ransomware For The First Time In US Hospitals

Cryptocurrency Mining

Low-Risk for organized crime
Uses existing botnets
Becoming legitimized
Operational Continuity Threat
Better than ransomware

IoT Weaponization

- Not secured when deployed
- If exposed to the Internet, immediate takeover
- Mirai, Reaper, DoubleDoor
- Used for DDOS, and TBD

What's Going Wrong Here?

- *Manufacturers* – do not produce products that are certified as free of known security defect
- *Procurement* – does not require any attestation of product security as a requirement for purchase
- *Integrators* – do not install products with security controls
- *Operations* – does not address roles and responsibilities delineation for security

Lawsuits

Class-action cyber attack lawsuit against Banner Health may be the first of many

Aug 10, 2016, 10:49am MST **Updated** Aug 10, 2016, 4:29pm MST

http://www.bizjournals.com/phoenix/blog/health-care-daily/2016/08/class-action-cyber-attack-lawsuit-against-banner.html

August 16, 2016

Yahoo sued for gross negligence over cyber-attack that exposed 500 million accounts

REUTERS

23 SEP 2016 AT 21:51 ET

https://www.rawstory.com/2016/09/yahoo-sued-for-gross-negligence-over-cyber-attack-that-exposed-500-million-accounts/

After the breach: Settlement expected for 50M Home Depot customers

https://www.scmagazine.com/after-the-breach-settlement-expected-for-50m-home-depot-customers/article/529135/

Threats of Litigation After Data Breaches at Major Law Firms

March 30, 2016

https://bol.bna.com/threats-of-litigation-after-data-breaches-at-major-law-firms/

Shareholders Sue Companies For Lying About Cyber Security

Another key area to focus on is litigation exposure. While this area of law is still developing, **breaches can give rise to consumer litigation, securities fraud litigation, even liability for corporate directors under Delaware law**.
[…]
The markets are becoming much more sophisticated in their understanding of the financial consequences of breaches that result in the loss of key intellectual property, and legal exposure is also expanding rapidly, especially on the consumer front. **Some courts are starting to permit consumers to bring cases based on the fear of fraud that they suffer after their data is stolen—even without being able to show that anybody has actually tried to use their data.** As we start to see share prices drop after news of previously undisclosed breaches emerges, I think we will be seeing more securities fraud suits as well.

http://www.forbes.com/sites/christopherskroupa/2016/10/27/exposing-litigation-the-hidden-risks-of-cyber-breach/#6f4f218f1988

Nation-State Collateral Damage

> "The superficial resemblance to Petya is only skin deep. Although there is significant code sharing, the real Petya was a criminal enterprise for making money. This is definitely not designed to make money. This is designed to spread fast and cause damage, with a plausibly deniable cover of 'ransomware.'"

The Third Party Microscope

Verizon & 500,000 Vehicle Tracking Accounts Exposed On Misconfigured AWS S3

TARGET

SONIC America's Drive-In

Opus & Ponemon Institute Announce Results of 2017 Third Party Data Risk Study: 56% of Companies Experienced Data Breach, Yet Only 17% are Prepared to Mitigate Risk

Deloitte.

Extreme Vetting: Evaluating The Security Posture Of Third-Party Vendors

OFFICE OF THE COMPTROLLER OF THE CURRENCY

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA

A Spyware Company Audaciously Offers 'Cyber Nukes'

"This ability enables an agency to instantly disable or destroy a target. Cyber strike capability is an 'always online weapon' that can be fired at any IP connected terminal with power to disable or destroy a target permanently," a copy of the brochure reads, referring to Aglaya's self-described 'Cyber Strike' product.

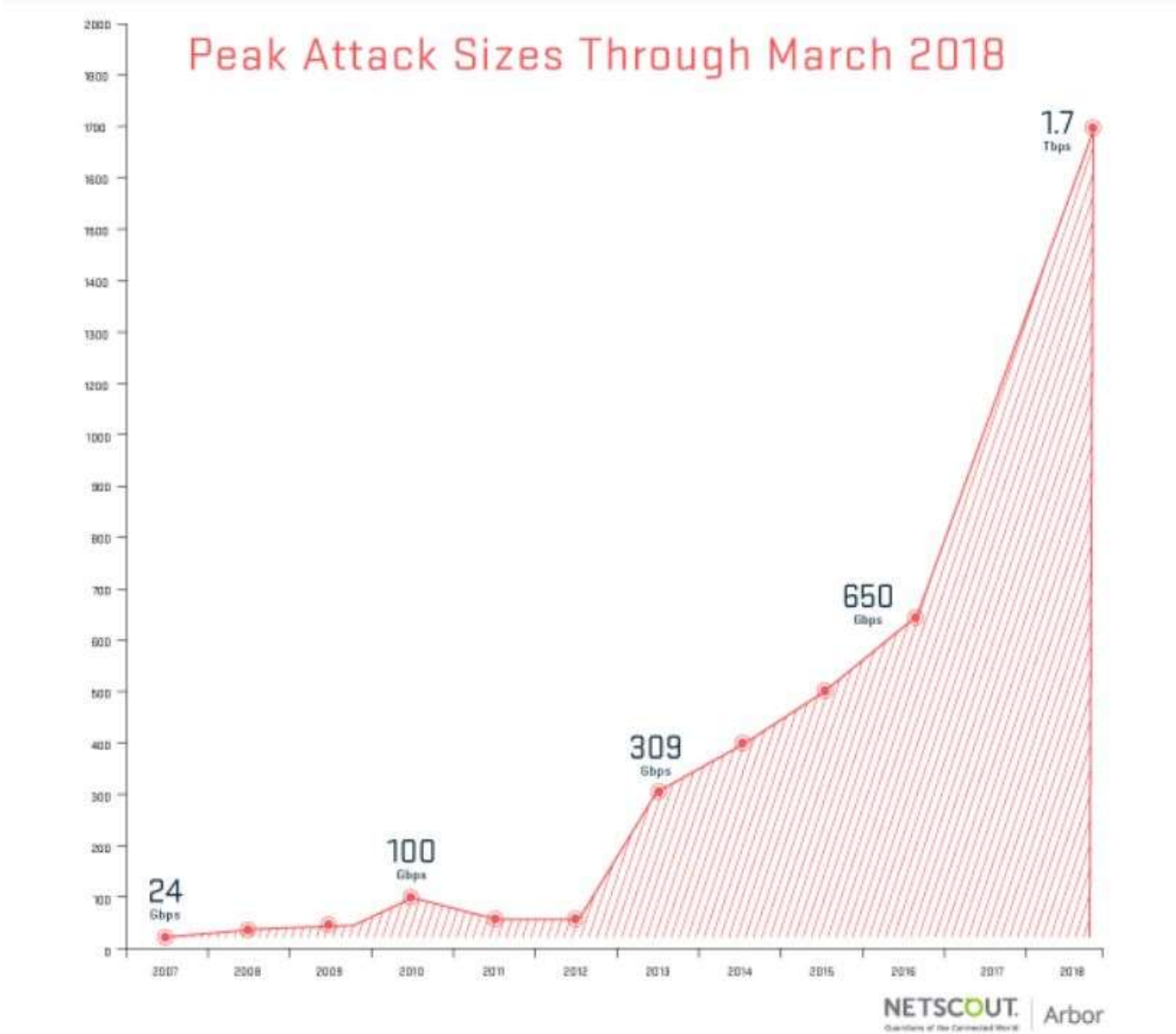
"This weapon is comparable to a Nuclear Strike that can *destroy city wide Cyber infrastructure or render a county wide IP communications ineffective*," the brochure adds.

source: https://motherboard.vice.com/en_us/article/59weqb/a-spyware-company-audaciously-offers-cyber-nukes

Gigantic DDOS

Memcached Amplification Attack Breaks New DDoS Record At 1.7 Tb/s

Arbor believes that we've entered a new era in which Tb/s DDoS attacks will be common, whether it's through memcached server vulnerabilities or through other vulnerabilities attackers may be able to find later.



Hardware Vulnerabilities

Meltdown-Spectre: Now the class action suits against Intel are starting to mount up

"One of the problems with Spectre is that it's completely silent," Evtyushkin said. "You don't see anything happening. Compared to traditional attacks, where an application usually crashes and you can see the damage, with microarchitecture attacks you won't see it or know it happened."

https://phys.org/news/2018-03-exposing-biggest-chip-vulnerability.html

Surveillance, Privacy, and Encryption

Tension between ad revenue and product companies
GDPR and the right to data removal
Disinformation, propaganda, and voter manipulation
US wants private sector cooperation w/foreign govt data requests
Role of local law enforcement

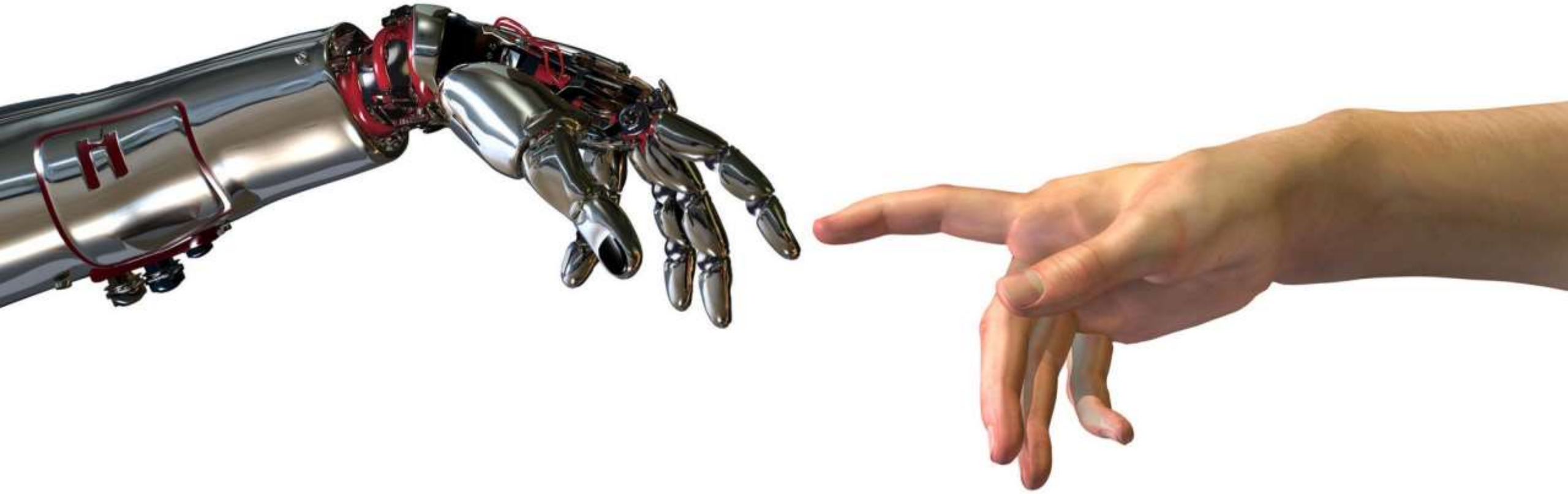
The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data

BY CAMILLE FISCHER | FEBRUARY 8, 2018

https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data

Not Everything is Bad… We Think

AI, ML, and Security Automation



Not-So-Crazy Predictions

SADLY

- DDOS will become a more prevalent (and effective) extortion tool
- Ransomware will affect transportation, manufacturing, and health sectors
- Our economy will be poked by a nation-state actor
- Government surveillance will increase
- The 2018 election will be chaos
- Extortion against a hospital will result in a death

BUT ALSO

- Boards of Directors will treat "cyber" as a business risk
- Automation with human oversight will start to help
- Security will become a competitive differentiator

THANK YOU

Mike Hamilton
Michael.Hamilton@criticalinformatics.com
@critinformatics – Company Tweets
@seattlemkh – Unvarnished Opinions

The IT Security News Blast
https://criticalinformatics.com/resources/it-security-news/

CRITICAL INFORMATICS

Our stuff keeps your stuff from becoming their stuff

info@criticalinformatics.com

Twitter
@seattlemkh
@critinformatics