Cyber Threat Brief
January 2019

Ilene Klein, CISSP, CISM, CIPP/US

Arizona Cybersecurity Program Coordinator

UNCLASSIFIED / TLP:WHITE

Cybersecurity in the News

- Century Link outage – 12/28-29
  - Affected nation-wide internet connectivity and 9-1-1 functionality (due to VOIP)
  - Was a hardware / configuration issue with a network management card – ***not cybersecurity***
  - FCC is investigating
  - Shows ramifications of reliance on one carrier / technology
- Newspaper attack – 12/27-30
  - Affected newspaper publishing at Tribune Publishing, including LA Times, Wall Street Journal, the New York Times, San Diego Union Tribune, more
  - Was due to Ryuk ransomware, a form of "targeted" ransomware with indicators similar to malware from North Korea

Current Threats

- SamSam ransomware is still out there
  - A Louisiana motor oil manufacturer was recently hit with SamSam
    - They're considered critical infrastructure
  - It cost them $2M/day they were down
- Ryuk ransomware is a growing and serious threat
  - The attackers target their victims and are demanding high ransoms
  - This is the malware that hit Tribune Publishing around 12/28-30
  - Ryuk is currently hitting California businesses
  - Seattle FBI is taking the lead on investigating Ryuk incidents

More Current Threats

- There have been a lot of drone sightings around Louisiana's Mississippi corridor – specifically over ports and plants, like Exxon and Dow Chemical
  - The theory is these are being used for economic espionage
- Emotet malware is hitting agencies in NY and CA
  - Emotet is a type of banking/financial Trojan that originally stole financial account info
  - Some of the current infections involve 100s-1,000s of workstations
  - Emotet hit Arizona governments and organizations late 2018

Watch for Seasonal Scams

- It's W-2 and IRS scams season!
- Be skeptical of requests for W-2 info for all employees
- Expect all types of IRS scams
  - File your taxes ASAP (before bad guys do)
- Changing payroll info is hot still
  - Via telephone/email phish or compromising a user's account

Watch for “Grooming”

- Scammers are now grooming their victims
  - Making multiple phone calls or sending multiple emails
  - Getting to know the victim and gaining their trust
  - Then delivering their payload

- Example:
  - Accounts Payable gets a telephone call from a woman stating she’s the new clerk at a vendor’s company
  - She follows up by sending Accounts Payable an introductory email (from a spoofed email address)
  - Then she sends the request to change payment information

Madam Ilene's 2019 Predictions

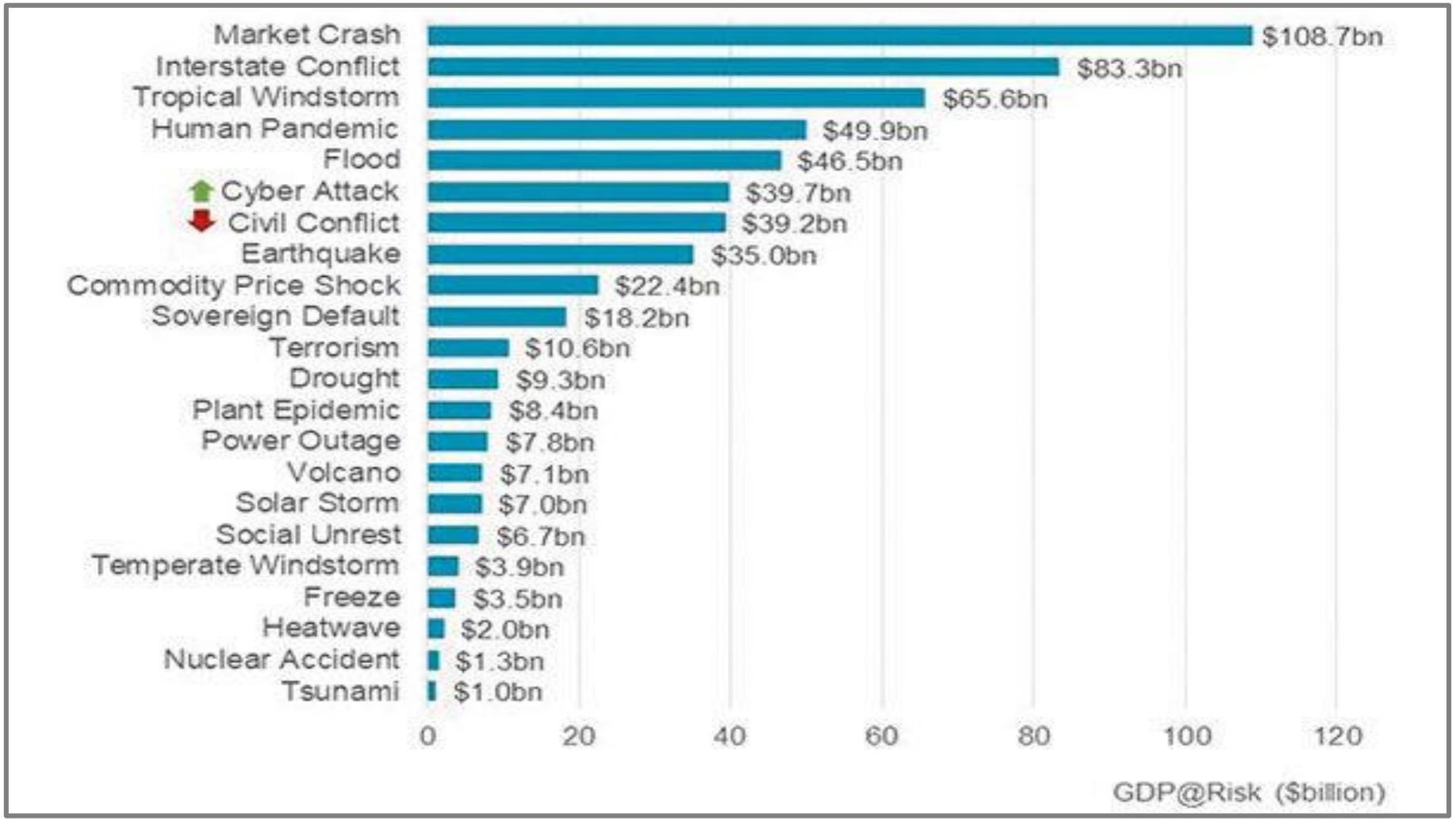
- Cryptojacking / cryptomining malware
  - It rose 4,000% in 2018
- Phishing using evasion /obfuscation techniques
  - Encrypting or obfuscating phishing emails and websites
- Money-grubbing criminal attacks
- Deepfakes and disinformation
- Denial of service attacks
  - We haven't had a good one since 2016
- Critical infrastructure attacks
  - We're overdue

FYI AND OLD STUFF FOLLOWS

2018 Q4 VISE Meeting – Key Points

- Top malicious Arizona government trends
  - Phishing spoofing other governments, Thanksgiving-themed, and Help Desk themed
  - Ransomware
    - September 2018 – an Arizona government entity suffered a ransomware attack that affected 95% of its applications servers
    - On average, one U.S. government entity is hit with ransomware each week
      - City of Atlanta, Colorado Dept of Transportation
      - Ports of Long Beach, San Diego, Barcelona
      - Baltimore's 911 emergency dispatch system
      - Farmington, NM, Mecklenburg County, NC
  - On 26 November 2018, the District of New Jersey indicted two Iranians for developing and deploying SamSam ransomware
- Note: VISE is a group of Arizona government cybersecurity leaders

Cyber Attack Impact on Global Cities Grows by 9%



Source: 2019 Global Risk Index, Centre for Risk Studies, Cambridge Judge Business School

Personnel Changes

- Todd Therrien
- City of Phoenix Acting CISO
- Randell Smith retired late November

- Owen Zorge
- State of Arizona Interim CISO
- Mike Lettman left December 31

- Note: VISE members stated personnel changes was one of their larger risks (Q4 VISE meeting)

State Cyber Disruption Exercise – December 5, 2018

- State / DEMA hosted the cyber disruption exercise
- Breakouts for
  - State agencies' tabletop
  - State functional (Security Operations Center, National Guard)
  - Local governments' tabletop (about 30 participants, including Phoenix)
- PCI breach was key scenario
  - Discussed incident response best practices
  - Encouraged more mature governments help less mature ones

Phishing is Rampant

- About 90% of all security incidents start with a phishing email
- November saw a rash of Thanksgiving-themed phish from spoofed government entities, including law enforcement, fusion centers, and federal/state agencies
  - Campaign hit across the U.S., including Arizona
- Currently seeing help-desk themed phish
  - Campaign recurs regularly
- This week we saw our first IRS/W-2-themed phishing campaign
  - Typically hits late January – early April
- Expect to see holiday and package delivery themed phish the rest of this month

Printer Hacking as a Service

- A Twitter user hacked over 50,000 printers recently to promote a YouTube channel
  - Part of a guerilla marketing campaign
- This spawned a new “Printer Advertising” service
- Website claims it can hack printers all over the world to print out messages on demand

Seattle PD Swatting Registry

- Swatting has increasingly become a part of online harassment
- Seattle Police Department created a proactive registry for residents who think they might be a target

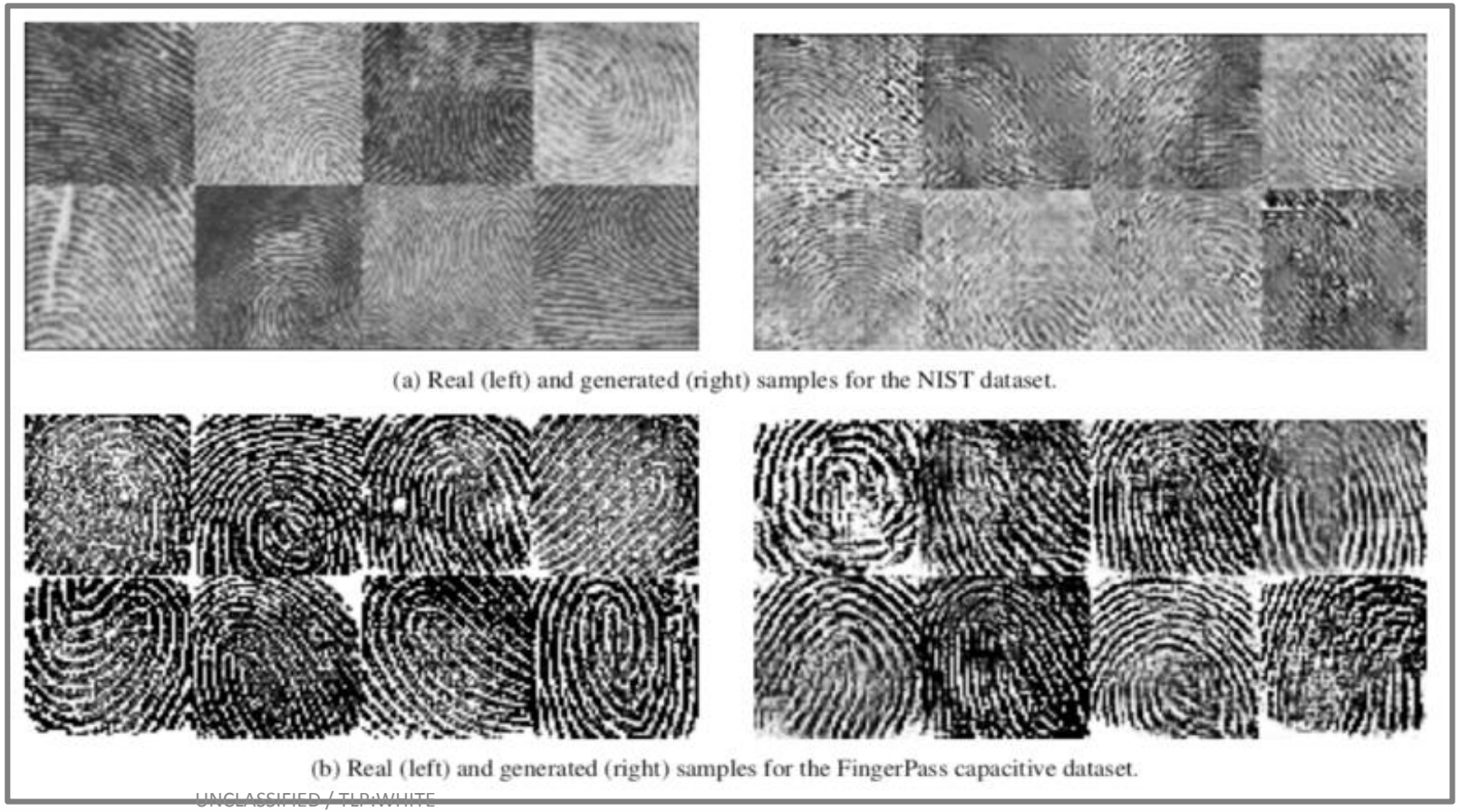
- “If a police response is requested to an address where swatting concerns have been registered, this information will be shared with first responders to inform and improve their police response to the incident.”

Emerging Trend – Deepfakes

- Increasingly realistic, but fabricated images, videos, and audio created using AI and other tools
- Can be used by malicious actors (and nation states) for
  - Disinformation campaigns in our elections
  - Efforts to exacerbate political and social divisions to weaken our nation
  - Modifying body cam footage

Fake Fingerprints Can Imitate Real Ones

- Researchers used AI to generate artificial fingerprints
- They work for biometric ID systems
- They prove fake fingerprints can be created



(a) Real (left) and generated (right) samples for the NIST dataset.

(b) Real (left) and generated (right) samples for the FingerPass capacitive dataset.

Hacker Threatens to Release 9/11 Documents

- Hacker Dark Overlord threatens to release 9/11-related documents stolen from a law firm that handled September 11-related cases
- Stolen info includes “emails, retainer agreements, non-disclosure agreements, settlements, litigation strategies, liability analysis, defense formations, collection of expert witness testimonies, testimonies, communications with government officials in countries all over the world, voice mails, dealings with the FBI, USDOJ, DOD, and more, confidential communications, and so much more[.]”
- He’s also threatening to release pictures of stars’ plastic surgeries stolen from a plastic surgeon

And In Other News…

- Kentucky man who ordered child sex dolls will not be charged with child porn
  - Judge ruled “no actual child involved”

- Houston’s City Council banned a “try-before-you-buy” sex robot brothel