Current Investigative Trends

ASAIC David Mills
USSS Seattle Field Office

Topics

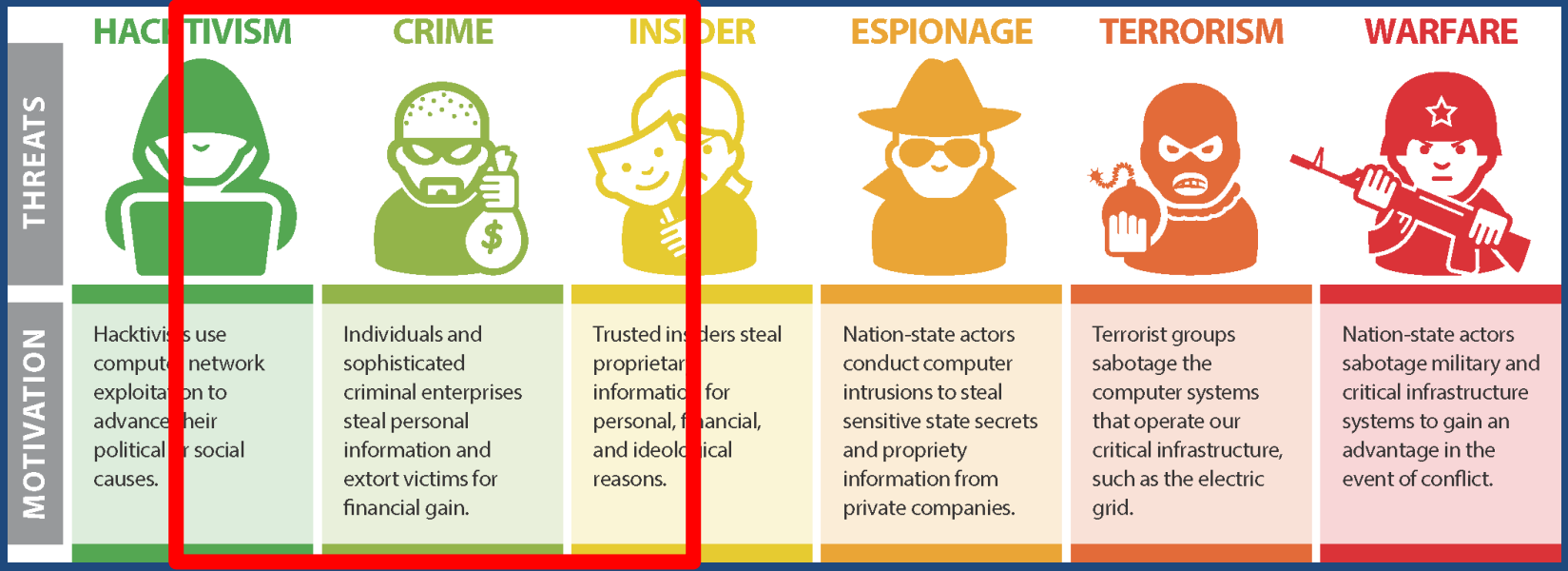
- Introduction to the USSS Investigative Mission & CFTF Model
- Current Investigative Trends and Priorities
- Questions and Follow-up

My Background

- 2000 - Started with the USSS in the Los Angeles Field Office
- 2005 - Began working at USSS HQ as program manager for “Project Colombia.”
- 2007 - Transferred to the Vice-Presidential Protective Division.
- 2011 - Transferred to Seattle, became certified computer forensic examiner, and presently serve as the supervisor of the Seattle CFTF.

USSS Background

- Our Cyber-Protective mission includes critical infrastructure of permanent and temporary protected sites, as well as National Special Security Events (UNGA, RNC, DNC, G7/8/20, APEC Summit, NATO Summit, Papal Visits ETC).
- Our Cyber-Investigative mission primarily lies in the Financial Crime Sector. This includes crimes involving payment cards, PII ,PHI, IP, and network intrusions for profit.



USSS CFTF's

- After 9/11 the USSS was directed to form a series of CFTF's
- CFTF's are a strategic partnerships of industry, academia, and law enforcement (state, local, and federal).
- The CFTF mission is deterring, investigating, suppressing, and prosecuting technology-based crime.
- Currently there are 40 CFTF's: 38 CONUS & 2 OCONUS

Electronic Crimes Task Forces

Cyber Crime Trends

- Radical shift from POS/BOH attacks to E-Skimming via compromised e-commerce websites.
- Business Email Compromises (BEC)
- Ransomware attacks
- Crypto-mining on enterprise and cloud systems
- Incident response seems to be shifting from LE preforming forensic response and analysis, to PFI performing response and remediation under the direction of outside legal counsel.

COVID Unemployment Fraud

Washington's unemployment fraud may have hit $650 million; state recovers $333 million

June 4, 2020 at 11:07 am | *Updated June 4, 2020 at 9:50 pm*

Boarded-up businesses are a familiar sight as the coronavirus pandemic keeps thousands out of work. Shown here is the Virginia Inn Restaurant... (Ted S. Warren / The Associated Press) **More**

By Paul Roberts

Seattle Times business reporter

Two weeks after revelations of a massive fraud scheme that briefly shut down Washington's unemployment system, state officials have acknowledged that the scale of theft was probably between $550 million to $650 million, or as much as one of every $8 paid in benefits during the pandemic.

Of that vast sum, the state has recovered $333 million, the state Employment Security Department (ESD) announced Thursday.

Ransomware Attacks

- Ransomware attacks employ malware to encrypt portions of a computer or network. The Ransomware then extorts a certain financial sum, in order for the data to be unlocked.
- More and more, the perpetrators are asking that the victim make the first offer.
- The victim is then left with the choice of fighting the attack, or paying the ransom and hoping the attackers fulfill their promise.
- Usually the attack vector is via Phishing / Spear phishing.

Ransomware Attacks

Baltimore transfers $6 million to pay for ransomware attack; city considers insurance against hacks

By LUKE BROADWATER
BALTIMORE SUN | AUG 28, 2019 | 12:32 PM

A posted sign on the door of the DPW's water department office. Baltimore City residents were not ab

A posted sign

ADVERTISEMENT

LATEST POLITICS

POLITICS
Elijah Cummings' widow weighs run for congressional seat; former Rep. Kweisi Mfume to announce plans Monday
12m

BALTIMORE CITY
Ritz Carlton condo owners have been asking Baltimore for water bills since 2009, attorneys say; review of estimated $2.3 million debt underway
1h

POLITICS
Baltimore business leaders urge Hogan to increase MTA funding

Ransomware Attacks

NATIONAL

22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault

August 20, 2019 · 10:16 AM ET
Heard on Morning Edition

BOBBY ALLYN

3-Minute Listen + PLAYLIST

Texas state Capitol building in Austin. This week, state officials confirmed that 22 municipalities have been infiltrated and ransom demanded.

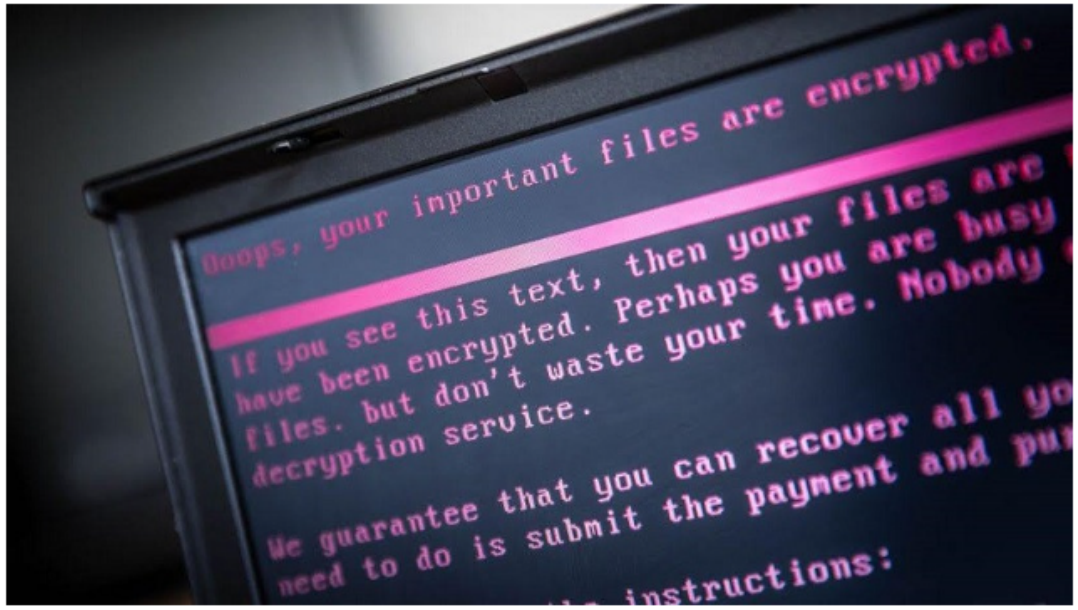
Bill Clark/CQ-Roll Call/Getty Images

Ransomware Attacks

Ransomware Attacks on Businesses Are Skyrocketing

The ransomware attacks are also largely targeting machines in the US, which accounted for 53 percent of Malwarebytes's ransomware detections. The good news is that ransomware attacks on consumers have gone down.

By Michael Kan August 8, 2019 2:41PM EST



BEC Attacks

- Business E-mail Compromise (BEC) scams usually involve spoofing a real account, or using a compromised account, in order to trick someone to send payment to an alternative location.
- For example Timothy.Hunt@Acmecorp.Com instead of Timothy.Hunt@Acnnecorp.com.
- The spoofing e-mail can either purport to be from inside of a company, or from a vendor.
- Business e-mail compromise attacks may or may not employ malware.
- Often the attacker will have compromised a legitimate e-mail account and observed traffic for sometime in order to gain intelligence to enhance the attack.

BEC Attacks – New Variation

25,068 views | Sep 3, 2019, 04:42pm

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

Jesse Damiani Contributor ⓘ
Consumer Tech
I cover the human side of VR/AR, Blockchain, AI, Startups, & Media.

Anonymous hacker programmer uses a laptop to hack the system in the dark. Creation and infection of ... [+] GETTY

It's the first noted instance of an artificial intelligence-generated voice deepfake used in a scam.

Phone scams are nothing new, but the mark usually isn't an accomplished CEO.

According to a new report in *The Wall Street Journal*, the CEO of an unnamed UK-based energy firm believed he was on the phone with his boss, the chief executive of firm's the German parent company, when he followed the orders to immediately transfer €220,000 (approx. $243,000) to the bank account of a Hungarian supplier.

Contact Us:

USSS Seattle Field Office

Cyber Fraud Task Force

Office: 206-553-1922

Cell: 206-402-7073

dmills@usss.dhs.gov

Questions?