Panel

- Timothy M. Lott, Director of Operations – SEARCH
- Paul Weatherhead, CISSP – Digital Boundary Group
- Chief Terry Sult – City of Hampton, VA

Types of Attacks

- Denial of Services (DoS)
- Phishing
- Ransomware
- Malware
- Virus
- Worms
- Trojan Horse
- Social Media Attacks
- Social Engineering
- Theft

Cyber Attack Examples: Ransomware

- **History of ransomware**
  - —Emerged in Eastern Europe 2009
  - —Cyber criminals started using malicious code to lock up unsuspecting user machines
  - —Demand approximately 100 euros for user to regain access to their machine
  - —Over last decade multiple cyber criminal outfits as well as nation states have expanded these tactics
    - o Targeting networks over individual machines

Cyber Attack Examples: Ransomware

- **How ransomware works**
  - —Commonly begins when a single person opens malware disguised as a recognizable email attachment from a known user
  - —Once the attachment is opened the malware will begin to freeze data block by block until all the data is locked
  - —Often a countdown clock will appear with a ransom demand
  - —Some of the ransom notes contain directions on how to purchase bitcoin

Cyber Attack Examples: Ransomware

- **How ransomware works**
  - —Not always delivered through email attachments
    - o 3rd party access to network
  - —Evolving from holding hostage to destruction
  - —Loitering ransomware

Cyber Attack Examples: Ransomware

- **Attempted attacks worldwide**
  - o 2014 3.2 million
  - o 2015 3.8 million
  - o 2016 638 million
  - o 2017 2.4 billion
- **Bythe end of 2019 ransomware estimated to attack a business every 14 seconds by the end of 2019**
- **Why interested in my agency?**

—automation

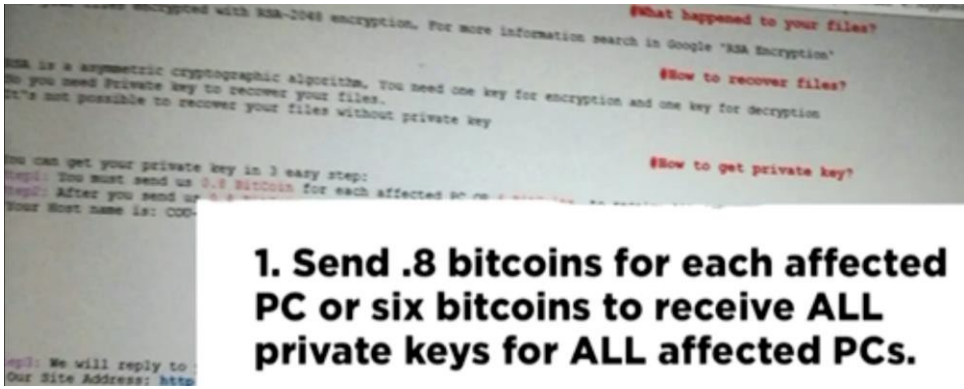
Source: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

Cyber Attack Examples: Ransomware

- **Scope of Damages in US Dollars**
  - —2015 325 million
  - —2016 1 billion
  - —2017 5 billion*
    - o Estimation due to underreporting

Atlanta Ransomware Attack

- March 22nd 2018
- City of Atlanta Information Management Team learned of a computer outage
- Estimated cost to recover from attack 17 million

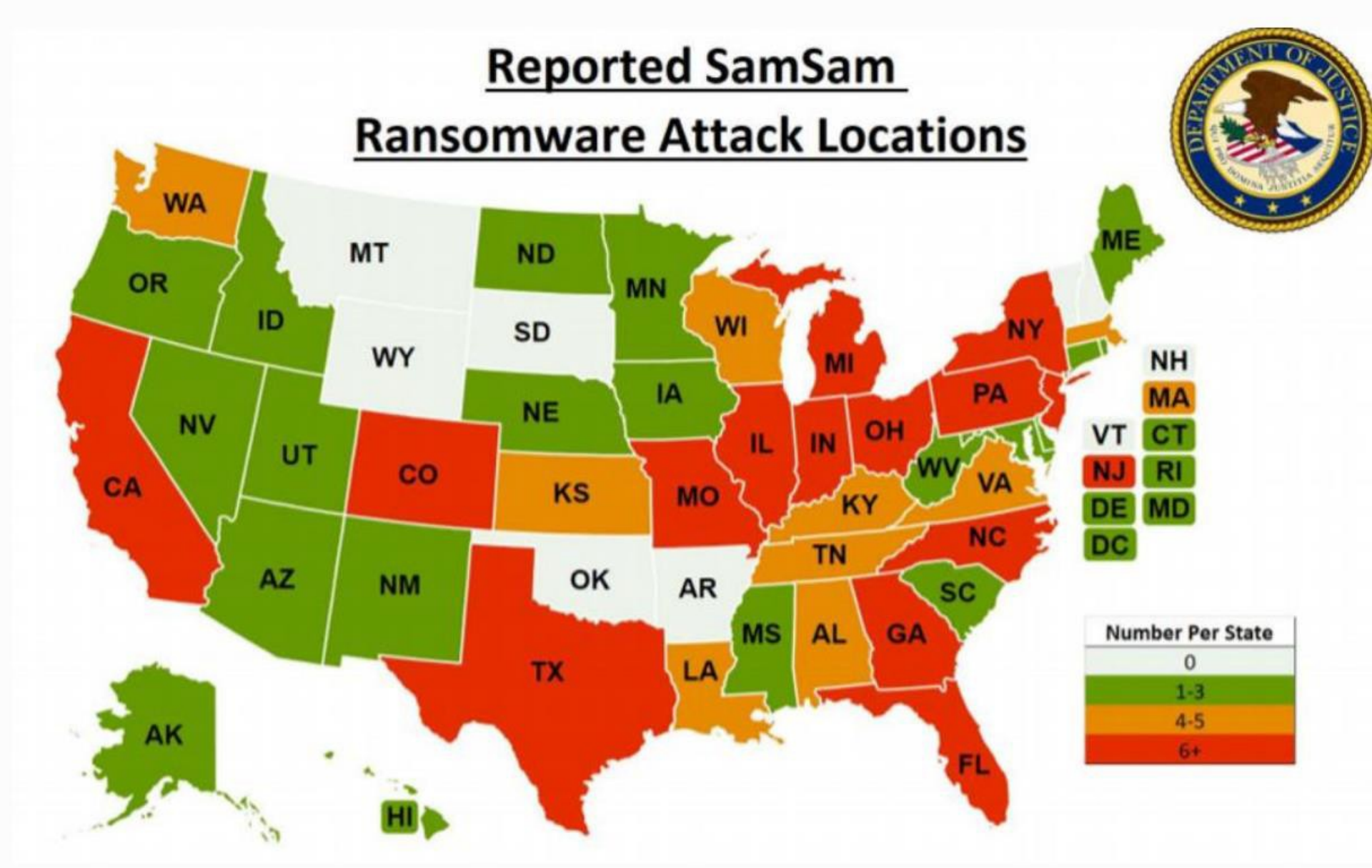


Atlanta Ransomware Attack

- **Police had to write incident reports by hand**
- **Lost access to nearly all archived in-vehicle video**
- **Affected processing of cases in Municipal Court**
  - —Unable to validate warrants
- **Payment for tickets, water bills and business licenses were also affected**
- **Stopped taking employment applications**
- **Shutdown WiFi at Hartsfield-Jackson Airport**

Atlanta Ransomware Attack

- **Two months after initial attack 141 our of 424 software programs remained offline or partially inoperable**
  - —30 percent of those were deemed mission critical by the city



A map of SamSam ransomware infections across America. DEPARTMENT OF JUSTICE

City of Baltimore Attack

- May 7th city services hit with Ransomware attack called RobbinHood
- Hackers demanded $75,000 to unlock the system
- FBI advised the City not to pay
- Total could reach 18 million dollars

An Unlikely Attack Vector?

Sports Arena (could be yours…)

City Hall (IT Partner)

Police Station (rather obvious…)

Pelladon at en.wikipedia

By Thomas1313 - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=22767785

Police Departments: Ransomware Victims

- **Collinsville, Alabama**
  - Refused to pay
    - Lost access to files
- **Dixon County, Tennessee**
  - Paid 622 dollars in bitcoin
- **Lincoln County, Maine**
  - Impacted four other police departments
- **Dallas, TX**
  - Hackers were able to set off tornado warning sirens in middle of the night

SEARCH 2019

Real World Information Security

Presented by:
Paul Weatherhead, CISSP
Senior Security Specialist

Digital Boundary Group

- Vulnerability Assessments
- System Security Auditing
- Building Robust Security

- Full assessment should be performed every 12 – 18 months
- Vulnerability scans should be performed on a monthly basis or after any significant change
- Interpreting vulnerability scan results can be difficult, sometimes several low risk vulnerabilities can be combined to create high risk vulnerabilities
- Perform your own scans? Outsource? Maybe both?

- Which vulnerabilities do I remediate first?
  - Remediate critical systems first
  - Hosts exposed to the Internet should be the highest priority
  - Vulnerabilities that require no user interaction or authentication to exploit are often weaponized to deliver ransomware and other malware. These vulnerabilities are critical to remediate.

Hosts 1940 | **Vulnerabilities** 343 | Remediations 12

Filter | Search Vulnerabilities | **343** Vulnerabilities

Sev	Name	Family	Count
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (401...	Windows	130
CRITICAL	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	129
CRITICAL	AXIS Multiple Vulnerabilities (ACV-128401)	Misc.	43
CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Code Exec...	Windows	16
CRITICAL	Unsupported Windows OS	Windows	11
CRITICAL	Microsoft Windows XP Unsupported Installation Detection	Windows	8
CRITICAL	SNMP Agent Default Community Names	SNMP	7
CRITICAL	IBM Baseboard Management Controller Default Credentials	Misc.	6

- Can reveal evidence of a current or past incident
- Is useful for comparing system settings to best practices
- Tends to focus on policies, procedures, and documentation
- Is an important component of system hardening

- Multiple layers of security is the best approach
- System hardening
- Vulnerability scanning and penetration testing
- Policies, Procedures, and Documentation
- End-User training
- Advanced endpoint protection to help defend against known and unknown malware
- Monitoring, alerting, and Honeypots

Questions