DATA SECURITY

Current Trends and the Law Enforcement Perspective

ADRIENNE EHRHARDT, DATA SECURITY & PRIVACY PARTNER AT PERKINS COIE LLP

AMELIA GERLICHER, DATA SECURITY & PRIVACY PARTNER AT PERKINS COIE LLP

GABE GUNDERSON, FEDERAL BUREAU OF INVESTIGATIONS

SCOTT BRADFORD, U.S. ATTORNEY'S OFFICE, DISTRICT OF OREGON

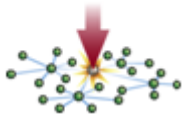
TRENDS IN CURRENT INCIDENTS

Types of Attacks

DDoS

False Tax Return Filings

Doxing



Network Destruction Attacks

Theft of IP

Ransomware and Extortion

Theft of PII, PHI

Business E-mail Compromise

Point of Sale Breaches

Website Defacements

Business Email Compromise

- **Account Compromise**
- **Bogus Invoice**
- **Executive "CEO" Fraud**
- **Data Theft**
- **Lawyer Impersonation**

PERKINSCOIE

What is Ransomware?

Ransomware is a malware that encrypts a user's files and computers, making them inaccessible until a ransom is paid.

- Victim’s computer is infected with the malware.
- Encrypts victim’s data and/or systems, making them unreadable.
  - Networked backups are encrypted or deleted
- Announces Itself unlike other malware
  - Actor demands payment to decrypt files or network.
  - Cryptocurrency (BTC)
- Constantly evolving
  - People pay
  - Enterprise attacks on the rise

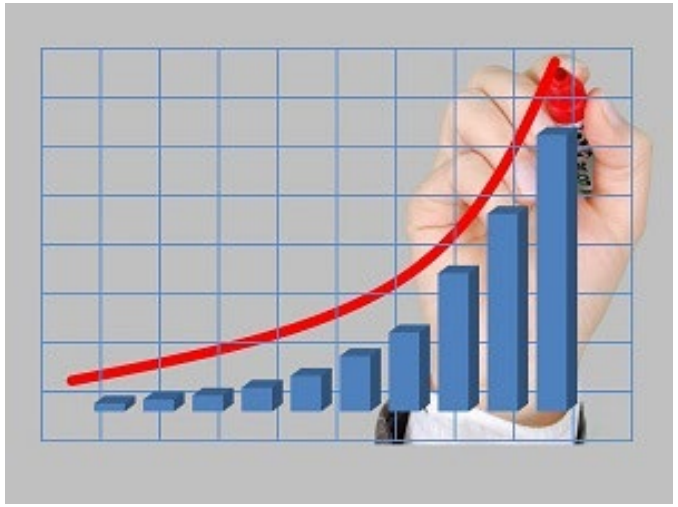
Ransomware Background

- Modern day ransomware began around 2013
  - Cryptolocker
  - Ransoms were $300 - $700
- Primary Actors Deploying Ransomware
  - Cyber-criminals
  - Financially motivated
- Difficult to investigate
  - All aspects are supported by anonymization
  - Initial intrusion
  - TOR (Darkweb)
  - Virtual Currency

PERKINSCOIE

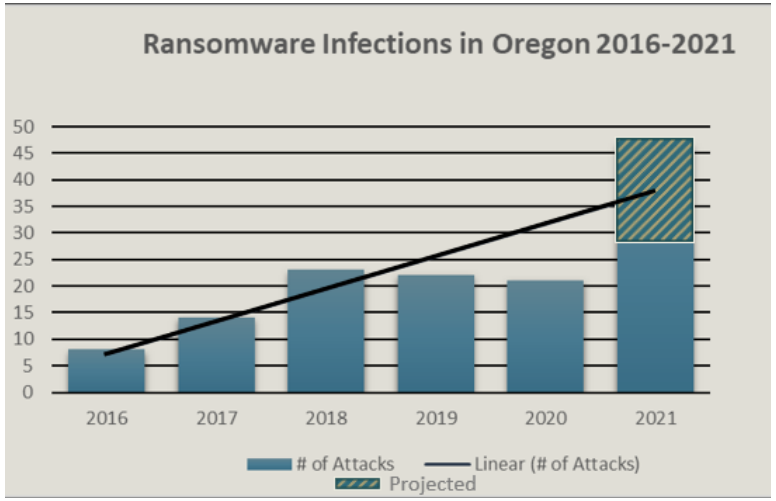
Global Impact

- Government, Health, Emergency Services, Hospitals, Police & Fire
- Loss of critical work
  - City records/planning documents, LE evidence, DNA
  - Patient Records, imaging, degradation of care
  - 911 dispatch and EMS response
- Remediation Costs
  - Can be in the millions
- Paying a ransom vs not
  - FBI recommendation



Oregon Impact

- As of mid September 2021, 2414 complaints, 32 in Oregon
- Average Ransom Demand = $36,000 (2019) -> $847,344 (2020)
- Non-Ransom Costs:
  - $900,000 Average Cost for Small Companies
    - Remediation
    - Legal Fees
    - Lost business
    - Downtime
  - Larger companies paying in multi-millions
  - Most costs must be paid even if you pay ransom!!
- Oregon attacks typically 4 per month
- Top targets: medical, government, academics, manufacturing, retail, technology



PERKINSCOIE

USG Strategy - Ransomware

- NSC Task Force
- FBI Strategy
- Treasury / OFAC
  - Civil Penalty
- Ransom Disclosure Act (draft)

Other Attack Trends and Consequences

- Credential stuffing
- Unsecured databases
- Perils of unstructured data

PERKINSCOIE

WHAT TO DO

General Best Practices

POLICIES

Security Program • Retention • Personal Information handling • Data classification • Least privilege • Incident Response

PRACTICES

Regular threat training • Data minimization • Secure coding • Updated hashing

TECHNICAL TOOLS

Rate limiting • IP whitelisting • Key management • Logging

Business Email Compromise Protection

Implement a two-step verification process for IT, financial and business procedures.

- ✓ Use out-of-band communications to confirm transactions.
- ✓ Be cautious with social media.
- ✓ Implement technical solutions to flag malicious behav
- ✓ Inspect payment details, amounts and justification.

Ransomware – Immediate Response

Backups are critical, and may be the best way to recover critical data.

- ✓ Isolate the infected computer(s).
- ✓ The No More Ransom Project (www.nomoreransom.org)
- ✓ The FBI does **not** advocate paying the ransom.
- ✓ Report to IC3 or your local FBI Field Office.

Ransomware Protection

- Offline Backups
  - Networked vs Offline
  - Backup regularly and often
  - Restore procedures

- Identify and fix the underlying problem
  - Employee Training/Awareness
  - Vulnerability Testing

LAW ENFORCEMENT REPORTS

Where to Report?

www.IC3.gov

CYWATCH@fbi.gov
(855) 292-3937

Why Work with the FBI?

- Establish trusted partnerships *prior* to a cyber event.
- Increase optics into nefarious cyber activity.
- Bilateral information exchange.
- Surge USG resources and capabilities.
- Investigative focus on actor attribution and disruption.
- Maintain consumer confidence.
- Incorporate the FBI's victim-centric approach into your response plan.
- We will determine the best approach together.

What the FBI does NOT Do…

- Take over your systems
- Repair your systems
- Share proprietary information with competitors
- Provide investigative-related information to the media or your shareholders

Working with US DOJ on Cyber Cases

DEBUNKING MYTHS

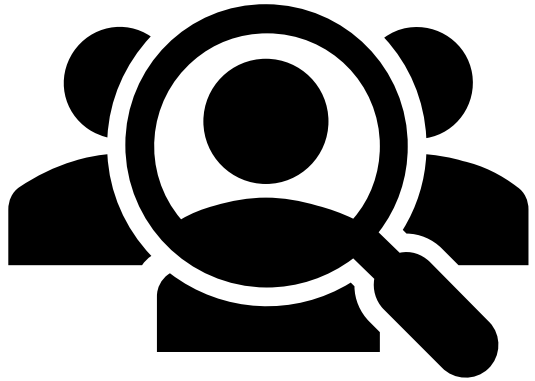
- Treatment of Victim Companies
- Interactions with Third-Party Mitigators
- Privilege Issues
- Restitution
- Crypto
- Trial

Treatment of Victim Companies

- Treated like victims of a crime
- Confidential treatment
  - Legal pleadings
  - Press releases
  - Trial
- Not reporting to regulatory authorities
- No victim blaming

Third-Party Mitigators & Privilege Issues

- Not interested in obtaining privileged information
- Not interested in victim blaming
- Basic forensics
- Communications with threat actors
- Crypto payments/wallets



Restitution & Crypto

- Restitution is a priority
- Tracing crypto
- Realities of recovery

PERKINSCOIE

Trial

- Outline of a criminal trial
- Confidentiality concerns
- Managing expectations

QUESTIONS?