Ransomware: Practical Insights from the Trenches

Presenters:

Michael Waters, *Polsinelli PC*

Abby Bonjean, *Polsinelli PC*

February 20, 2020

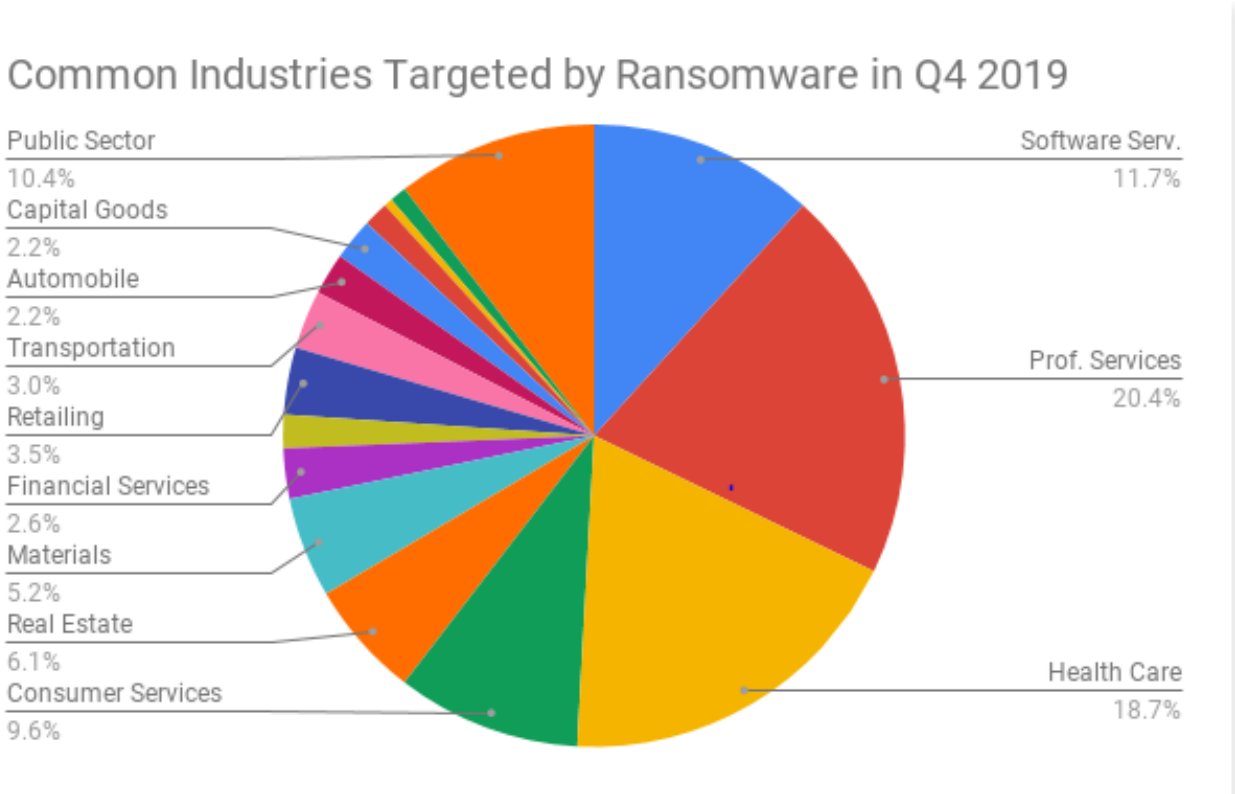
Frequency

- There has been a significant increase in ransomware incidents
- The number of incidents have more than doubled between 2018 and 2019
- The targets of ransomware attacks have changed
  - Pre-2018, individuals were often targeted
  - Now, businesses and other entities are targeted
  - It is easier for attackers to get paid by businesses than individuals who may not be as sophisticated or have access to Bitcoin

High Profile Incidents

- National Health Service – May 2017
  - WannaCry impacted hospitals and businesses across the world
  - Cost NHS approximately £92 million
- Baltimore – May 2019
  - $18.2 million
  - Impacted online payment services for water bills, property taxes and traffic citations
- New Orleans – December 2019
  - $3 million

Industries Targeted



Source: Coveware

Ransomware Variants

- There are over 200 variants of ransomware
- Most do not have publicly-available decryption keys
- Common variants include:
  - Ryuk
  - Sodinokibi
  - Bit Paymer
  - CryptoLocker
  - GandCrab
  - Dharma

Ransomware Deployment

- Ransomware can be deployed in multiple ways:
  - Email phishing campaigns;
  - Remote Desktop Protocol (RDP) vulnerabilities;
  - Software vulnerabilities, particular remote management tools; and
  - MSPs and IT vendors – Sodinokibi, for example, is often deployed in situations in which an MSP is impacted along with all of its business customers

Cyber Extortion

- Cyber Extortion occurs when someone acquires data or information and demands payment (typically in bitcoin) in exchange for a promise not to release the information.
- These scenarios increasingly occur in conjunction with ransomware events.
  - Sometimes the attacker publicizes the attack and demands payment in exchange for not releasing data - Maze Ransomware.
  - Sometimes the attacker says that they will publicize the attack unless payment is made.

Ransom Payments – FBI's Formal Position

The FBI does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data. In some cases, victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.

Paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

The FBI wants entities to report ransomware incidents.

Ransom Payments - Reality

Ransomware attacks are becoming more sophisticated. In particular, bad actors are often able to encrypt backup data. As a result, entities often have little choice but to pay the ransom demand.

This reality is demonstrated by the fact that there are now companies whose only service is serving as an intermediary between attackers and entities impacted by ransomware events.

Largest demand seen by Polsinelli: $18 million (MSP whose business customers were impacted by the incident)

Are the Attackers Caught?

- In the vast majority of situations, the answer is no. Attackers are able to disguise the source of the attack and Bitcoin allows for anonymous payments.
- In November 2018, the United States did unseal indictments against two Iranian men accused of perpetrating SamSam ransomware attacks. Those individuals have not been extradited.
- To increase the chance of catching the attackers, the FBI is asking from prompt notice of ransomware incidents (within 24 hours). Polsinelli has several contacts with the FBI who typically respond within hours.

Breach Notification

- Legal obligations related to breach response
  - Federal (Industry-Specific) Obligations
    - HIPAA
    - Gramm-Leach-Bliley
    - Department of Education
  - State Obligations
    - Breaches impacting residents of state
  - Contractual Obligations
    - Business Associate Agreements
    - Data Handling Agreements

Breach Notification – State Law

- Most common definition of breach (including Illinois): “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information”
- Connecticut, Florida, New Jersey and Puerto Rico: “unauthorized access”
- In a traditional ransomware incident, there has been no data access or acquisition
  - For this reason, ransomware incidents may be widely underreported

Breach Notification - HIPAA

- “Breach” defined as the acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of PHI
- OCR Ransomware Guidance – when PHI is encrypted as the result of a ransomware attack, a breach [is presumed to have] occurred because the ePHI encrypted by the ransomware was acquired
  - Notification required unless the entity can demonstrate no data access or acquisition through a forensic investigation
  - Where a healthcare provider did not experience the ransomware attack, but was directly impacted (e.g., EMR provider hit with ransomware that impacts healthcare provider, including patient care), healthcare provider may have notification obligations

Breach Notification - HIPAA

Who Receives Notice and When?

- **Breach involving fewer than 500 individuals**
- Notify affected individuals as soon as possible but no later than 60 days following discovery of breach
- Document breach and report breach (along with other breaches involving fewer than 500 individuals) to HHS no later than 60 days following the end of the calendar year during which the breach was discovered
- Notice provided through HHS website

- **Breach involving 500 or more individuals**
- Notify affected individuals as soon as possible but no later than 60 days following discovery of breach
- Notify HHS of the breach as soon as possible but no later than 60 days following discovery of breach
- If breach involves more than 500 residents of a particular state or jurisdiction, notify prominent media outlets serving such state/jurisdiction

Stages of the Incident Response

- *Mitigate* - Mitigate the harm caused by the incident
- *Remediate* – Recover from the incident through backups, ransom payment or otherwise
- *Investigate* – Conduct a forensic investigation to determine how the incident occurred and whether data was accessed or acquired.

Roles of Third Parties

- Insurance
- Legal Counsel
- Ransom Negotiator and Payment
- Data Forensic Firm
- Tech Vendor for Recovery
- Law Enforcement
- PR/Crisis Management
- Audit

How to Prepare

- Confirm insurance coverage
- Develop an Incident Response Plan
  - Identify key stakeholders
- Perform tabletop exercises
- Ensure data is adequately backed up
- Develop and test Disaster Recovery/Business Continuity Plan

Cybersecurity Risks in Transactions

- Many target organizations have not conducted an adequate security assessment
- Target organizations may have been subject to ransomware or other cyber-attacks
  - May not have reported
  - Inadequate identification of full scope of damage or fact that malware remains
  - Inadequate remediation

For More Information

Michael Waters **mwaters@polsinelli.com** **312-463-6212**	**Abby Bonjean** **abonjean@polsinelli.com** **312-463-6230**

RANSOMWARE: PRACTICAL INSIGHTS FROM THE TRENCHES

The process of responding to a ransomware incident can be stressful and frenetic. In light of this, you should give advance consideration to the various entities that you may need to contact in the event of an incident, which include the following:

- **Insurance** – Organizations may have cyber insurance that covers the costs associated with responding to a ransomware incident, and possibly payment of a ransom demand; however, the insurance company typically needs to be promptly notified and approve such costs.

- **Legal Counsel** – Legal counsel provide two primary functions: (i) managing the incident response and (ii) assisting the organization in identifying and carrying out any legal obligations associated with the event.

- **Digital Forensics** – Digital forensics are typically necessary to identify how the event occurred, so that the organization can make sure it does not happen again, and whether any data was accessed or acquired.

- **Ransomware Negotiation, Payment and Decryption Provider** – There are vendors who specialize in helping organizations analyze the ransomware variant, negotiate with threat actors, make bitcoin payments, and decrypt files.

- **Technical Advisory and Computer Restoration** – Organizations may need boots on the ground technical assistance and/or additional manpower to recover from backups, rebuild systems or facilitate file decryption. The digital forensic provider and ransomware negotiator often don't provide these services.

- **Federal Bureau of Investigation** – The FBI wants organizations to provide notice of ransomware events so that it can investigate. It will likely not have decryption keys, but may have helpful information about the ransomware variant and/or threat actor.

- **Audit** – Some organizations, including public companies, may need to inform auditors or other oversight entities of ransomware and other cybersecurity incidents.

- **Business Partners** - Ransomware incidents can have a significant impact on customers, business partners and other third parties, and the organization may have contractual or other obligations to provide prompt notice of events that impact those parties' data.