RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **MASH-M06**

Ransomware: How One Company Fought Back

Raymond Umerley

Vice President, Chief Information Risk Officer
Pitney Bowes Inc.

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

The Attacks

October 2019 – Ryuk

Shipping Giant Pitney Bowes' Services Stalled by Ransomware Attack

The company, which serves over 1.5 million clients, has been able to get some services back online but is still working to address the damage.

Pitney Bowes Hit by Ransomware

The attack does not appear to have endangered customer data, but it has had an impact on orders for supplies and postage refills.

DARK Reading

Dark Reading Staff
Dark Reading

October 15, 2019

Postage Provider Pitney Bowes Hit in Apparent Ransomware Attack

Pitney Bowes is blaming the disruption on a 'malware attack that encrypted information on some systems,' which is preventing clients from stamping their packages. The same attack has also hit the company's 'presort' mail cataloging service for the US Postal Service.

May 2020 – Maze

Package delivery giant Pitney Bowes confirms second ransomware attack in 7 months

Pitney Bowes network infected with Maze ransomware, after the company got hit by the Ryuk gang in October last year.

Maze ransomware fails to encrypt Pitney Bowes, steals files

pitney bowes

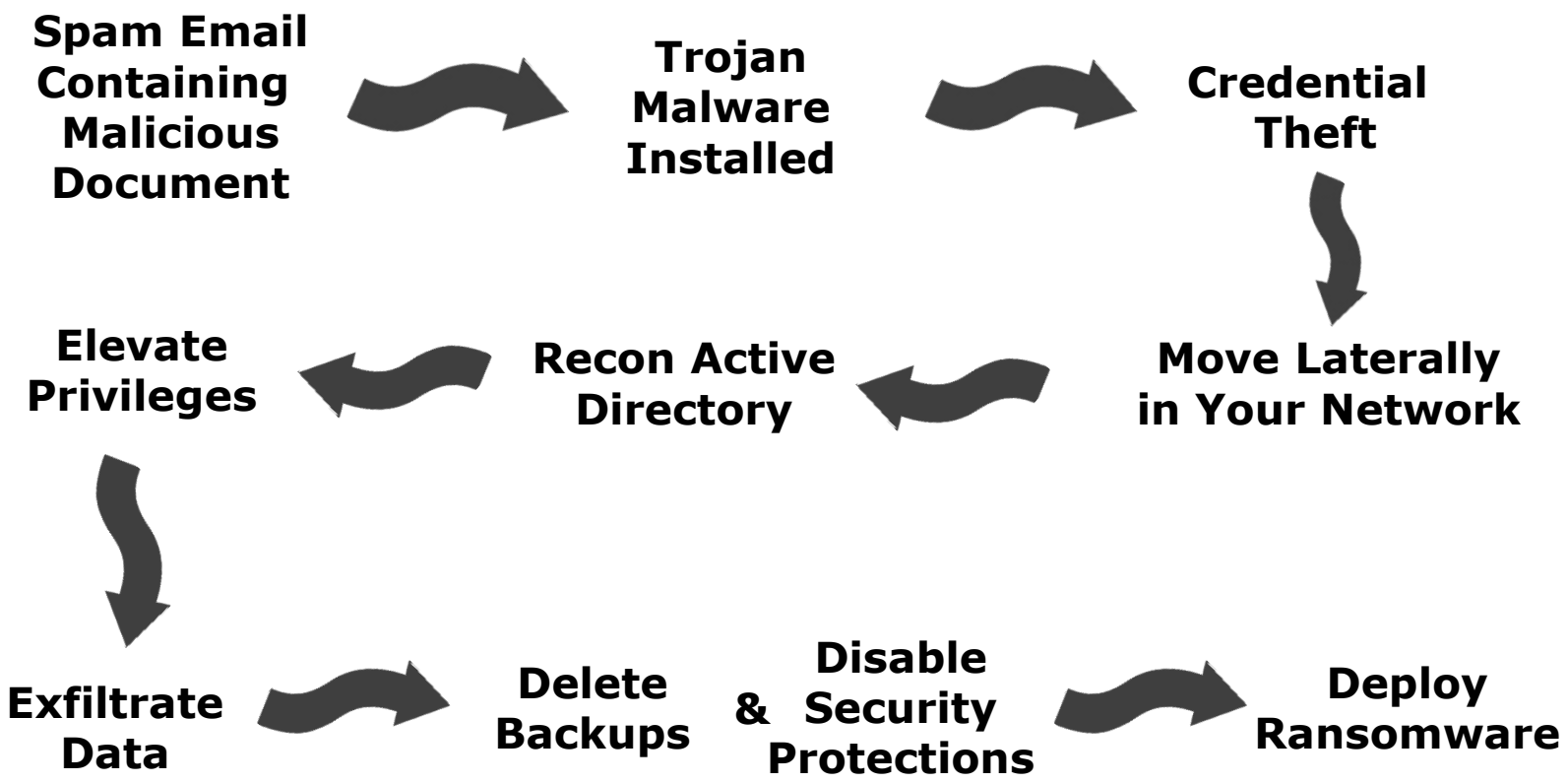
Impacts of the Attacks

- Operational Downtime
- Data Loss and Exposure
- Customer Disruption and Inquiry
- Workforce Stress and Disruption
- Legal and Regulatory Obligations
- Financial Loss
- Brand and Reputation

RSAConference2022

Anatomy of the Attacks

Anatomy of a Ransomware Attack



RSAConference2022

Internal Lessons

Lessons on Response and Recovery

Positives

- Speed of Response
- Third Party Security Expertise
- State of Backups
- Business Operations and Resilience
- Communications
- Enterprise Teaming and Ingenuity

Negatives

- Ensuring that “All equals All”
- Speed and Scale of Recovery
- Islands of Understanding
- IT Tools Immobilized
- Individuals and Teams Overwhelmed
- Partners Overwhelmed

RSAConference2022

When You Go Home…

Apply What You Have Learned Today

- **Next week you should**:
  - Evaluate your protection, detection, and response capabilities and technologies based on today's discussion
  - Identify your infrastructure crown jewels (e.g., Active Directory) and ensure they are appropriately protected (e.g., multifactor authentication, privileged access management, network segmentation, immutable backup storage)
- **In the first three months following this presentation you should**:
  - Ensure that you have an accurate asset inventory of your hardware, software, and data
  - Run scenario-based tabletop exercises involving your crown jewel assets to identify and remediate potential people and process gaps
  - Update your business continuity and disaster recovery plans to account for a cyber event, and the potential scale of digital recovery processes and technologies
- **Within six months you should:**
  - Look holistically at cybersecurity people, process, and tool harmonization (1-10-60)
  - Ensure your crisis plans include principles, positions, and processes for transparency and communication to your customers, employees, law enforcement, and regulators
  - Identify and establish relationships or retainers with the partners and suppliers that can assist you in these events, including your insurers

RSAConference2022

Questions?

raymond.umerley@pb.com