Ransomware

Prevention, Response, and Recovery

November 2, 2021

Microsoft Partner

Microsoft

Gold Application Development
Gold Collaboration and Content
Gold Cloud Productivity
Gold Messaging
Gold Datacenter

Collaborate with Confidence

Accessible content is available upon request.

Meet Your Presenters

AGENDA

- Ransomware Overview
- Ransomware Trends
- Technology, Policy, and People Best Practices
- Next Steps, Q&A, and Additional Resources

What is Ransomware?

Ransomware Fundamentals

- Ransomware is a type of malware (malicious software) used by cybercriminals.

- If a computer or network has been infected with ransomware, the ransomware blocks access to the system or it encrypts the system's data. Cybercriminals demand ransom money from their victims in exchange for releasing the data.

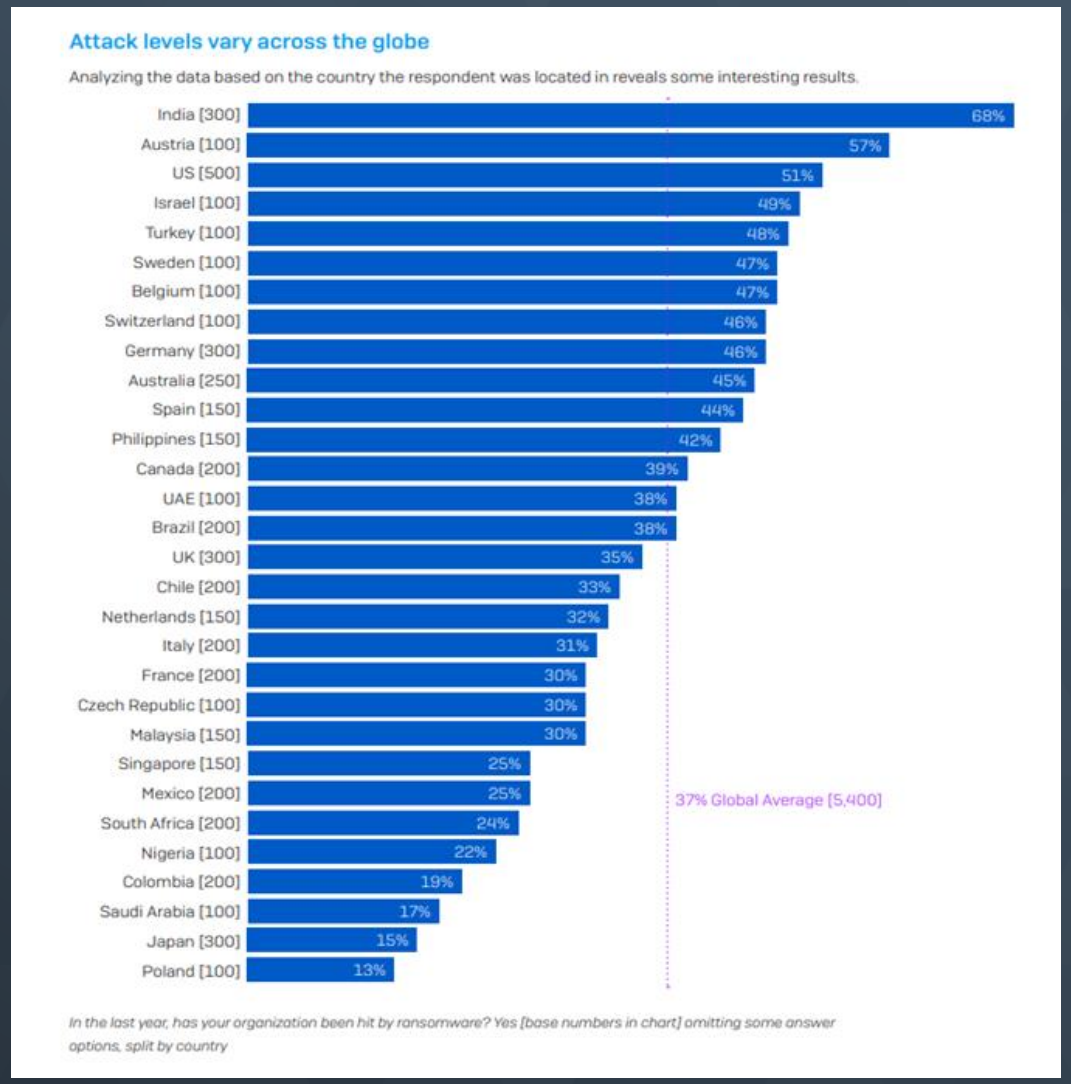
- Today, ransomware can be divided into two main types: locker ransomware and crypto-ransomware. These are commonly being paired with exfiltration and extortion techniques.

Ransomware Trends

The Rising Price of Ransomware

- Cybercrime to total an estimated $6 trillion USD in 2021. (Cybercrime Magazine, 2020)
- Average ransom fee requested has increased from $5,000 in 2018 to over $200,000 in 2020. (NSI, 2021)
- Cost to rectify the impacts of a ransomware attack up more than double in the past year to $1.85 million from just over $760,000. (Sophos, 2021)
- The volume of ransomware attacks in Q3 2021 totaled more than 190 million, nearly topping the 195 million attacks in the first three quarters of 2020. (Infosecurity Magazine, 2021)

State of Ransomware 2021



AvePoint®

Technology Best Practices

2021 Data Risk Report Financial Services

Path to Least Privilege

Companies with sensitive files open to all employees via global access

Sensitive files open to everyone	% of companies
< 1,000	35.71%
1,000-10,000	25%
>10,000	39.29%

Stale sensitive data by financial services company size

Financial Services company size	Avg. # of stale sensitive files	Avg. % of sensitive files that are stale
Large	526,606	63%
Medium	208,490	74%
Small	109,152	74%
Industry average	290,173	70%

Poor Active Directory Hygiene

Companies with passwords that don't expire

Passwords that don't expire	% of companies
< 500	41.07%
500-1,500	37.50%
> 1,500	21.43%

Companies with ghost users

Size of stale user account group	% of companies
< 1,000	35.71%
1,000-10,000	25.00%
> 10,000	39.29

Policy Best Practices

Policies & Procedures for your data

- Access Control
- Password Protection and Management
- Data Classification
- Acceptable Use
- Data Governance and Handling
- Backup, Storage and Data Retention

People Best Practices

Best Practices

People

- Training
- Awareness

Processes

- Business

Technology

- Permissions
- Isolating Devices

Next Steps and Q&A

Next Steps

- Today
  - Ensure you have a granular backup solution in place
  - Resource: Case Study - MCI Protects Against Ransomware with Cloud Backup
  - Resource: Case Study - Walls Construction Protects Critical Data From Ransomware Attack with Cloud Backup

- 30 Days From Now
  - Create a plan for visibility and classification for information
  - Resource: Try a Free Demo of Policies and Insights

- 90 Days From Now
  - Establish perimeter controls
  - Resource: Mitigating Collaboration Risk Workbook

thank you

AvePoint®

Sales@AvePoint.com | +1 800.661.6588

www.AvePoint.com