Storage Developer Conference
December 4-5, 2020
BY Developers FOR Developers

Ransomware proof storage

Nalini Kumari Nallamalli
Anindya Banerjee
Veritas Technologies LLC

Agenda

- Introduction
- Ransomware protection
- Best Practices
- Summary

Please take a moment to rate this session.

Your feedback matters to us.

Introduction

What is Ransomware?

How Do I Get Ransomware?

- Spear-phishing emails
- Remote Desktop Protocol (RDP)
- Weak passwords
- Infected software apps
- Infected external storage devices
- Compromised websites
- Remote attack on server
- Misconfigured public cloud instances

How it works?

- Once ransomware infects a computer, it will lock access to
  - The computer itself or
  - Data and files stored
- Advanced versions can encrypt files, folders on
  - Local drive
  - Attached devices
  - Can spread to other computers across network via network shares

Target Devices

OS Disk

Local Disk(s)

Connected Device(s)
(USB)
(e.g. Backup Disk)

Mapped Network Drive(s)
(e.g. NAS / File Servers)

Other Accessible Folders / Shared Local Network
(e.g. NAS / File Servers)

Dropbox

OneDrive

Who is Target?

- Individuals
- Every organization is a target, regardless of size, sector, or geography
  - Education
  - Financial
  - Governments/public sectors
  - Businesses
  - Hospitals/healthcare organizations

Ransomware Statistics and Facts

- First known malware attack in 1989, The “AIDS Trojan”
- Became more prominent in 2005
  - Started using more sophisticated RSA encryption
    - With ever-increasing key-sizes
- Starting from around 2012, the use of ransomware scams has grown
- Expected to attack a different business every 11 seconds by the end of 2021
  - 57X more than it was in 2015

Source: – **CyberSecurity Ventures,** **Global ransomware damage costs**

SEC-17a-4(f)

- **SEC Rule 17a-4** is a regulation issued by the U.S. Securities and Exchange Commission
- Outlines requirements for data retention, indexing, and accessibility for companies
- According to the rule, Records must be retained and indexed on indelible media
  - With immediate accessibility for a period of two years
  - With non-immediate access for a period of at least six years.
  - Duplicate records must also be kept within the same time frame at an off-site location.

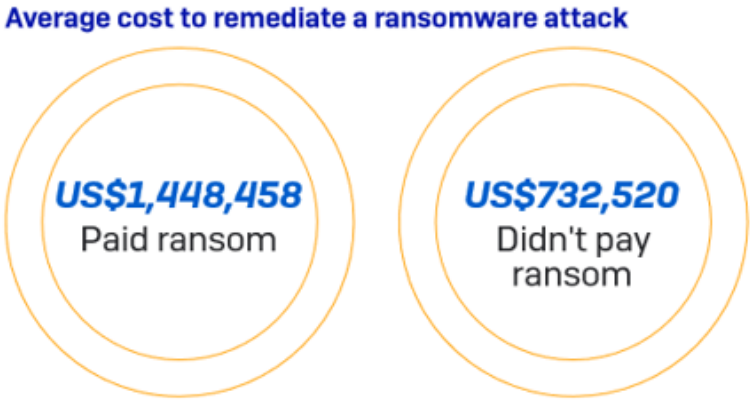
Ransomware Protection

Why Ransomware Protection?

- Downtime
- Pay to get the data unlocked
  - Fueling cyber criminal activities.
- Damage to reputation
- Legal Implications
- Loss of data
- Loss of customers

Why Ransomware Protection?

- Paying the ransom doubles the cost versus not paying and getting the data back via backups or other means



Source: Sophos The State of Ransomware 2020

Ransomware Protection

Three stages of defense against malicious activity

Prevention

Keep ransomware outside the environment

Detection

Detect malicious activity that it is can be stopped before spreading to additional systems

Recovery

Recover the data and infrastructure quickly

Prevention

- Security Tools
  - Watching for - Phishing, Malware, Downloads
- Secure Authentication
  - Multi-Factor authentication
- RBAC at granular level
  - Only specific services, ports and processes can be used by specific users
- Backup data verification
  - Validate at write and restore

Prevention

- Hardened hardware and software
  - Tightly limits data access to only those programs that need access
  - Lock down application binaries and configuration settings
- Data encryption
  - In-transit and at rest
- Having security awareness training
- Immutable storage
    - WORM(Write Once and Read Many) devices
    - Retention period

Protection – Write Once Read Many

- Immutability
  - Data, once written, cannot be deleted or altered
  - For either a pre-determined length of time or perhaps even forever (Retention Period)
- Secure clock or Compliance clock
  - WORM needs a clock to compare retention time
  - System clock can be tampered with
  - Need to have a clock that can not be manipulated

Detection

- Heuristics - Spikes in Encryption, File Rename
- Detection Tools - Anti-Virus, Intrusion Detection
- Audit logs
  - Attempts to modify or delete WORM files need to be logged
  - Log itself should be tamper proof
- Alerting
  - Backup size change alerts..
  - Alert on anonymous application or compromised account based on data usage

Detection

- Backup Environment monitoring – Ensure all data is protected
  - Validate backups regularly
- Infrastructure monitoring
- Monitoring
  - Find user anomalies and malware extensions
  - Network port monitoring
  - File size and backup duration exceptions

Recovery Readiness

- The 3-2-1 Rule to safeguard the data
  - 3. Keep 3 copies of any important data: 1 primary and 2 backups.
  - 2. Keep the data on 2 different media types to protect against different types of hazards.
  - 1. Store 1 copy offsite (e.g., outside of the business facility).
- Keep backups stored on air-gapped storage
- Disaster Recovery Orchestration
- Confirm critical systems are backed up

Recovery

- Removing the infection and Get access to the data
  - Cleaning the infected data with recovery tools
- Recover data from secondary storage / LTR
- Scans on restore
- Faster recovery
  - Able to perform automated and/or Bulk restore
  - Automated and orchestrated complete cross-system restoration
  - Automated recovery of last known good

Best Practices

Best Practices

- Start with the assumption that you will be hit
- Protect data wherever it's held
  - On premises, public or private cloud
- Backup to removable media
- Keep operating systems, software, and applications current and up to date.
- Controlled folder access

Summary

- What is Ransomware
- How it works
- SEC-17a-4(f) Regulation
- Ransomware protection
  - Prevent
  - Detect
  - Recovery
- Best Practices

References

- Wikipedia Ransomware
- Microsoft ransomware-malware
- CyberSecurity Ventures, Global ransomware damage costs
- Imperva 2020 cyberthreat defense report
- Digitalguardian history-ransomware-attacks
- Veritas risk-of-ransomware

Thank You!

nalini.nallamali@veritas.com
anindya.banerjee@veritas.com