Society of Quality Assurance

38th Annual Meeting & Quality College

3-8 April 2022 Palm Springs, CA & Online

Defending Against Ransomware

by

Bo Cheng, PhD and David Schumacher, RQAP-GLP

Alturas Analytics, Inc.

The LC-MS Experts

Session Description and Objectives

❖ Review the heightened ransomware attacks in recent years, analyze how ransomware works and the damages it can cause to the corporation.

❖ Raise awareness of ransomware for corporate leadership and ordinary employees.

❖ Planning by the corporate management and best practices for ordinary employees to mitigate the risk.

❖ Recommend actions the IT Department can take to combat the ransomware attacks.

Ransomware Surge Since 2020

Recent high profile victims in US:

- Garmin – July 2020
- CNA Financial – March 2021
- Applus Technologies – March 2021
- Quanta Computer – April 2021
- ExaGrid – May 2021
- Colonial Pipeline – May 2021
- JBS Meatpacking – May 2021
- Kaseya (Irish with US headquarters) – July 2021

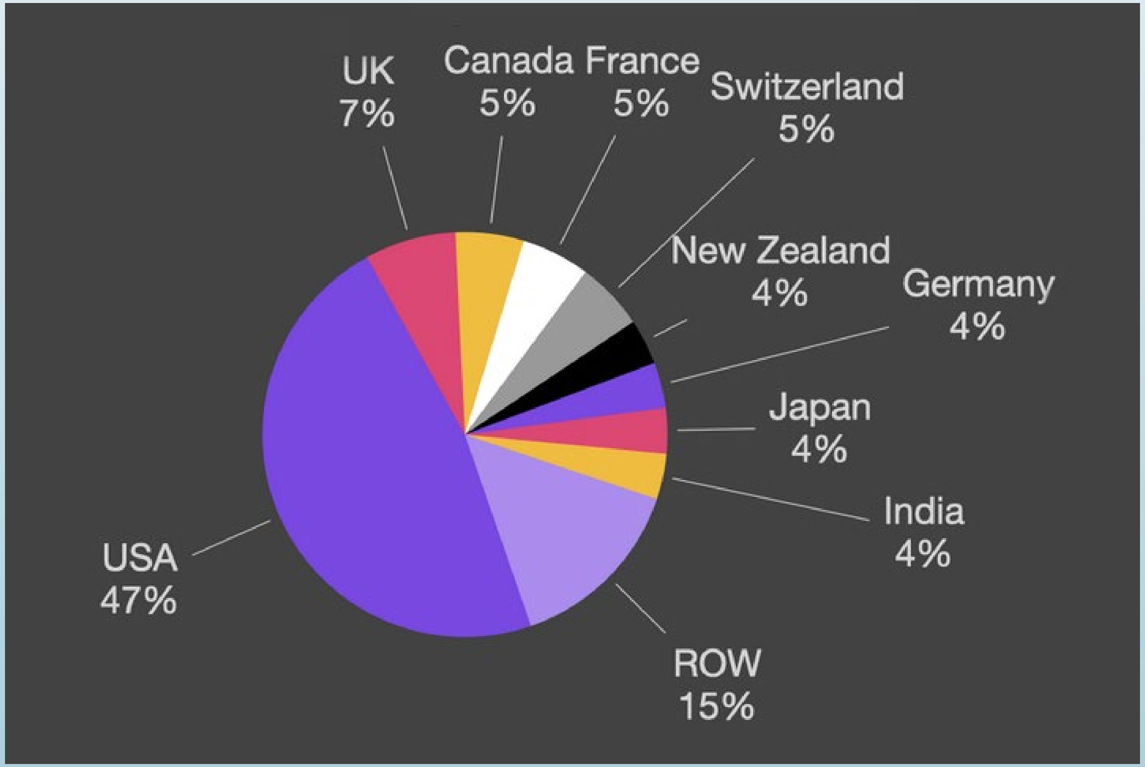
2022 starts “strong”

- Crawford County government, Arkansas
- Bernalillo County government, New Mexico
- Linn County government, Oregon
- Carthage Schools in Missouri
- Maryland Department of Health
- Griggsville-Perry School District in Illinois

Globally there are 740 named victims in Q2 2021 alone
148% increase in ransomware attacks since the pandemic (sources: Forbes)

Ransomware Surge Since 2020

Ransomware attacks by country



The surge is probably due to a confluence of factors:

- ❖ Popularity of anonymous payment (BitCoin)
- ❖ Hasty retooling of infrastructure to accommodate work from home by IT during the pandemic
- ❖ Maturing of ransomware ecosystem (ransomware for hire market)
- ❖ Recent tensions in geopolitics

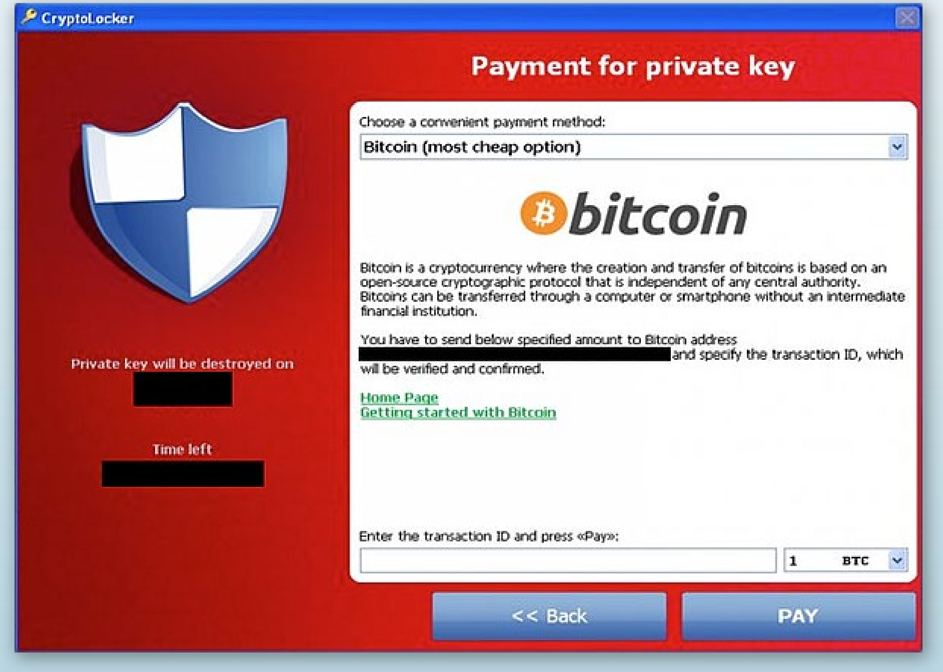
What is Ransomware?

- Infiltration of malware into corporate network.
- The malware encrypts files it can access across the entire network, including hot backups.
- Business ceases to operate due to inaccessibility of encrypted files.
- Threat actor demands payment for decrypting.
- Increasingly, in some cases, confidential information is exfiltrated. Threat actor threatens to make it for public view if not paid.

Ransomware = Malware + Cryptography

For practical purpose, the victims cannot decrypt the files without the key from the threat actor.

History



Payment for private key

Private key will be destroyed on [redacted]

Time left [redacted]

Choose a convenient payment method:

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address [redacted] and specify the transaction ID, which will be verified and confirmed.

Enter the transaction ID and press «Pay»:

1 BTC

Although internet extortion could be traced back to late 1980's, ransomware did not become popular until the arrival of anonymous payment (Bitcoin). The first notable ransomware was CryptoLocker in 2013 - it targeted individuals and asked for $300 in exchange for the key.

Today's Ransomware

- Targets businesses, asking for millions of dollars
- Has become an ecosystem on dark web
- RaaS (Ransomware as a Service) for hire, like "Killer for Hire"

The Damages

- Ransom payment: Usually several million USD, in form of Bitcoin. About 70% of victims choose to pay
- Interruption: Usually a week or more even if you pay the ransom. For most victims it took several weeks to come back to normal operation
- Cost in forensic investigation, damage assessment and control
- Legal ramifications if customer data is exfiltrated, possible restitution
- Regulatory compliance: Data breach issues - HIPAA, GDPR, CCPA and many more
- Reputation damage and loss of clients, contracts and revenue: Having the company in such news headline alone is damaging enough

Ways of Malware Infiltration

Primary Way: Through User Interactions

- ❖ Clicking links in malicious emails
- ❖ Opening attachments in malicious emails
- ❖ Visiting malicious websites
- ❖ Downloading malicious contents
- ❖ Leaking credentials (passwords) accidentally or by malicious insiders

91% Cyberattacks Start with Phishing Emails (sources: PhishMe/Cofense)

- ❖ System Vulnerability Exploitation
  - Vulnerabilities in Exchange Server (Hafnium attack) eventually turned to ransomware in March and April 2021 – many victims.
  - SMBv1 EternalBlue vulnerability and WannaCry of 2017
- ❖ Weak Information Security Policy
  - Allowing weak or shared password
  - Giving users more privileges than they need
  - Not giving users clear guidance
  - Some small businesses may not have an Information Security Policy at all
- ❖ Security Misconfigurations by IT

Counter Measures

At Corporate Leadership Level

- Get Top Management Involved
  - Cybersecurity has evolved to a business issue, no longer a simple technical issue
- Foster a Cybersecurity-aware Culture
  - Cybersecurity is the responsibility of each employee, not just the IT Department
- Give IT Department Sufficient Resources
  - Money and manpower so it can act proactively
- Consider Cybersecurity Insurance
  - Especially important for small businesses to remain financially solvent if attacked
  - Be aware of the coverage. Does it cover 3rd party (customers) IP loss?
- PR Readiness
  - When compromised if there is no corporate response or announcement, it creates confusion and worry for customers and causes further reputation damage

Counter Measures Cont.

At IT Department Level

- Periodic User Awareness Training
  - This is the #1 counter measure. No technical measure can offer 100% protection
- Conduct periodic phishing email exercise for all employees
- Tag external emails
  - Remind users such emails are potentially harmful
  - Promote zero-trust email security policy
- Prohibit personal use of work email
- Actively discover system vulnerabilities and patch timely
  - Following vendors advisories and tech news
- Establish and enforce Information Security Policy
  - Access policies based on “Need to Know” and “Least Privilege” principles
  - Robust password policies
  - Multi factor authentication
- Reduce attack surface by reducing exposure on the Internet
  - Placing servers behind firewall/VPN if possible

Counter Measures Cont.

At IT Department Level (cont.)

- ❖ Monitor security events and logs
  - SIEM (Security Information and Event Management)? SIEM can be quite “noisy”
- ❖ Establish and Maintain
  - Firewall rules allowing utilized traffic only
  - Web filter to block malicious sites
  - Anti-virus at multiple places (emails, firewall and endpoints)

- ❖ Conduct Periodic Penetration Tests
- ❖ Maintain a DMZ (Demilitarized Zone)
  - Placing high risk servers in DMZ
- ❖ Maintain Robust Cold Backups
  - Off-line backups that malware cannot reach
- ❖ Partition storage servers
  - Assign permissions per “need to know” principle to limit the damage
- ❖ Have a contingency plan and mock test it

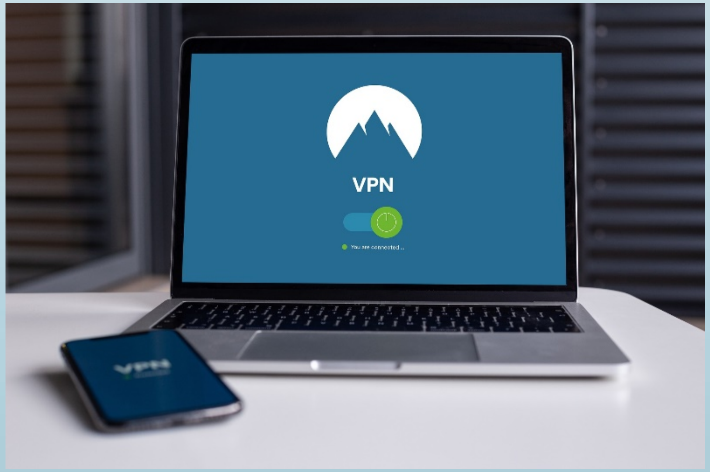
Counter Measures Cont.

At Ordinary Employee Level

- Follow Information Security Policy
- Check with IT for emails from untrusted sources you are not sure of legitimacy
- Don’t open email attachments out of curiosity
- Hover mouse to reveal the linked address in email web links before clicking
- Utilized “Preview” feature in Outlook before fully opening attachments
- Report your computer’s suspicious behaviors
- Visit work related websites only
- Never click “Clickbait”
- Safeguard your passwords

QAU Monitoring

- ❖ Ensure password security through password complexity and frequent changes; establish a PW reuse policy
- ❖ Ensure departed employees are immediately removed from any access to computer systems
- ❖ Provide regular training to all staff on email awareness
- ❖ Remove or deactivate any removable media on computer for staff that do not require it
- ❖ Require two-factor authentication for VPN or other access to company resources from Internet
- ❖ Have an internet policy limited to work related functions and website
- ❖ Ensure there are regular back-ups of server and test the restore capability
- ❖ Perform regular vulnerability (internal and external) and penetration testing from a qualified provider



Best Way to Combat Ransomware

Prevention, Prevention and Prevention!

The prevention of ransomware involves the entire company and heavily relies on ordinary employees’ daily activities at their workstations.
No technical measures taken by IT will provide 100% protection.

Questions and Contact Information

Bo Cheng, Ph.D.

Director of Information Technology
bcheng@alturasanalytics.com

David Schumacher, RQAP-GLP

Quality Assurance Director
dschumacher@alturasanalytics.com

Alturas Analytics, Inc.
The LC-MS Experts

Alturas Analytics, Inc.

1324 Alturas Dr.
Moscow, ID 83483

alturasanalytics.com