CYBER READINESS INSTITUTE

CYBER HAWAII

Ransomware: What You Can Do!

March 26, 2020

Mahalo to our Community Partners!

CYBER READINESS
INSTITUTE

Presenters

Jill Tokuda, CyberHawaii

Craig Moss, Director - Content and Tools, Cyber Readiness Institute

Lisa Diercks, FBI Honolulu Cyber Squad

Cyrus Kam, FBI Honolulu Cyber Squad

Sandy Ferreira, Vice President, Atlas Insurance

Alan Ito, Information Security Officer, Hawaii Pacific Health

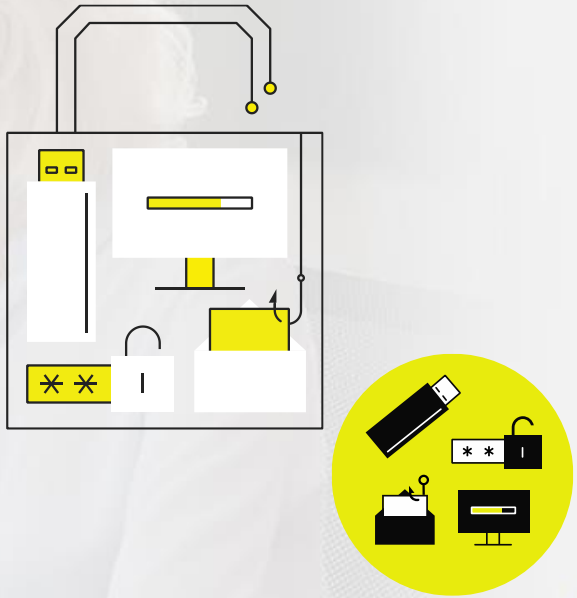
Agenda

- Basic Cyber Readiness to Prevent Ransomware Attacks
- Intelligence on Current Ransomware Attack Methods
- Cyber Insurance for SMEs to Protect Against Ransomware
- Ransomware Issues in the Health Industry
- Q & A
- Closing

The Cyber Readiness Institute

CYBER READINESS
INSTITUTE

- Non-profit
- Convenes senior leaders of global companies and value chain partners
- Shares cybersecurity best practices and resources
- Develops *free* content and tools to improve cyber readiness of small and medium-sized enterprises
- Download the Ransomware Playbook https://cyberreadinessinstitute.org/resource/ransomware-playbook/



Co-Chairs and Members:
Global business leaders – from across sectors and regions

THE CENTER FOR GLOBAL ENTERPRISE

mastercard

Microsoft

PSP PARTNERS

ExxonMobil

Principal

GM

CYBER READINESS
INSTITUTE

Preventing & Responding to Ransomware Attacks

Preparation is the Key

BeCyberReady.com

CYBER READINESS
INSTITUTE

"For health and safety reasons, we'll be transitioning to cyber crime."

CYBER READINESS
INSTITUTE

What is a Ransomware Attack?

- Conducted by a malicious actor to hold an organization’s data hostage for a ransom
- Malicious actors can gain access through various means, often phishing and unpatched software

CYBER READINESS INSTITUTE

Prevention for Small Businesses

Appoint a Cyber Leader

- Point person in Cyber Readiness Program
- Implement practical policies
- Build awareness
- Establish a culture of cyber readiness
  - Prevention
  - Incident response

Focus on Core Four Issues

- Passwords
- Software Updates
- Phishing
- Removable Media and USBs

CYBER READINESS INSTITUTE

Responding to Ransomware Attacks

Prepare

- Do back-ups
- Test the back-ups
- Patch software
- Phishing training
- Have a plan

Respond

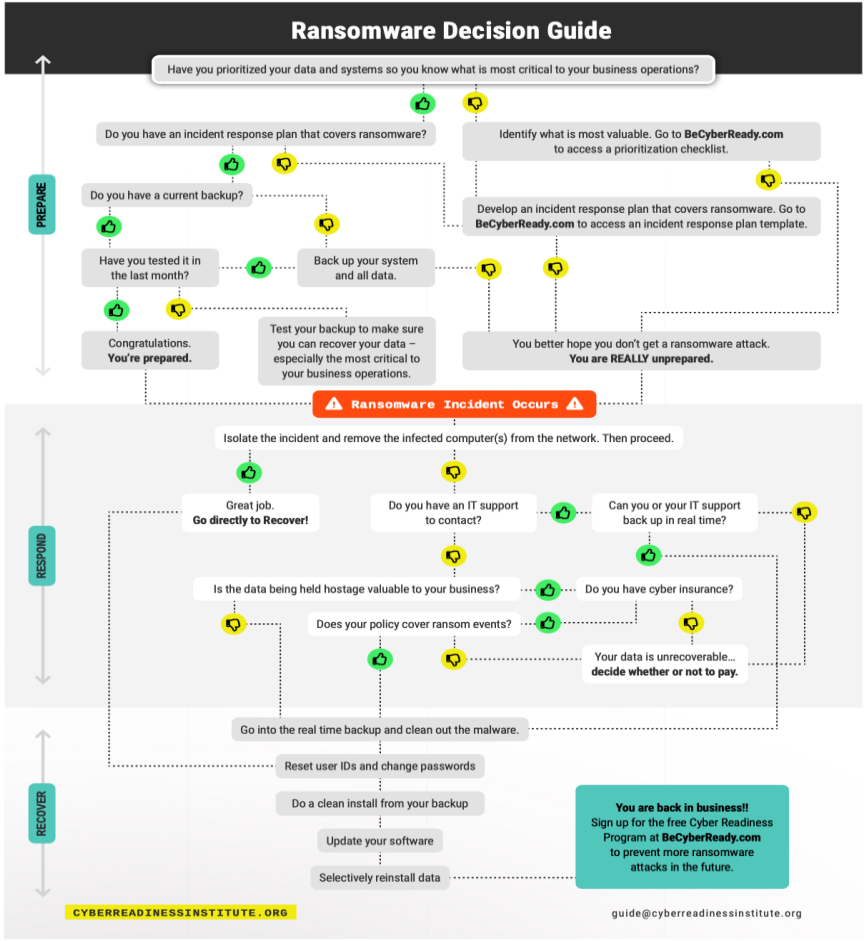
- Remove infected device(s) from network
- If tested back-ups – no problem – proceed to Recover
- Without tested back-ups:
  - Determine criticality of data
  - Try real-time back-up
  - Check insurance policy
- Contact law enforcement
- To pay or not to pay?

Recover

- Reset user IDs and change all passwords
- Do a clean install from back-ups
- Update all software
- Restore data from back-ups

Get free Ransomware Playbook with decision-tree

www.becyberready.com

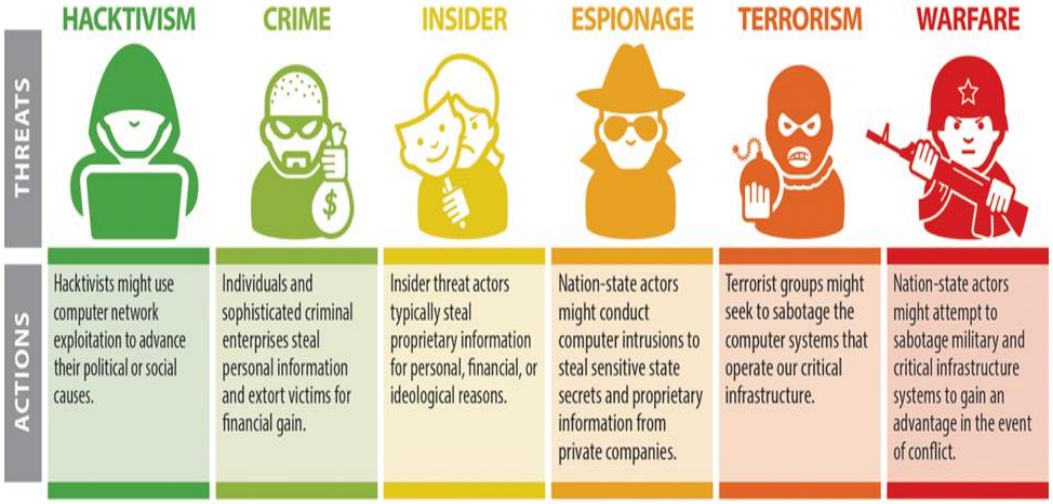


FBI Honolulu Cyber

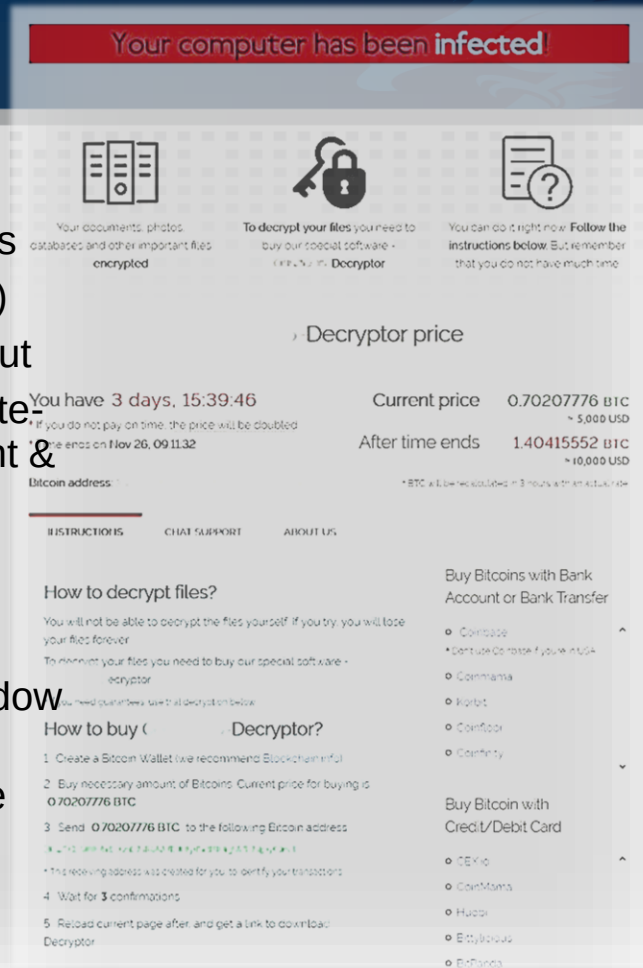
SA Cyrus Kam **CS Lisa Diercks**

March 26, 2021

(U) Who May Be Doing the Hacking?



REvil/**Sodinokibi**, aka Sodin



- April 2019 - Present
- Ransomware-as-a-Service (RaaS) – customized exploits
- Demands payment in BTC via Tor browser (30-40% cut)
- Whitelisted countries – excludes Russian keyboard layout
- Exploits software vulnerabilities (i.e. 0-day exploits), brute-force on Remote Desktop Protocol/Remote Management & Monitoring tools
- Phishing emails with malicious links and attachments, Exploit kits
- Avoids AV detection; Elevates privileges, Able to move laterally within network; Exfiltration of data; Deletes shadow copies and other backups
- Infects trusted third-party vendors and Managed Service Providers
- Threatens to release data publicly if ransom is not paid

Ransomware Investigation - Analysis

- Forensics – understand what happened
  - Ransomware note comparison
    - Bitcoin addresses
  - Identify responsible executable
  - Identify initial infection vector
- Logs
  - Persistence
  - Propagation

Ransomware Insurance Coverage

Prepared by:

Sandy Ferreira, VP

Atlas Insurance Agency, Inc.

201 Merchant Street Ste 1100, Honolulu, HI 96813

Typical Real Life Ransomware Attack

Your employee opens an invoice attached to a vendor email. It looked like other emails from the same person. That attachment releases ransomware that immediately spreads to all company machines, including your backup server. As a result, every computer in your organization is rendered **useless** and your business operations shut down immediately because you can't access any critical systems, applications or data.

This attack happened to a mid-size business on the east coast, crippling operations and resulting in at least **$18.2 million** in damages creating a combination of lost revenue and direct costs to restore its systems.

Statistics:

- 68% of ransomware attacks began with phishing links.
- Phishing attacks have increased over 600% since the start of the COVID-19 pandemic.
- By 2021, a business will fall victim to ransomware every 11 seconds.
- The average ransom demand has risen from $5k in 2018 to $100k in 2020, some as high as $1M.

Ransomware Insurance Coverage

State of the Cyber Insurance Market

- Minimum premiums for $1,000,000 policy limit are as low as $1,000 or $1,500 with cybercrime (aka Social Engineering) coverage.
- Pricing is based on loss trending and severity.
- More carriers are enforcing network security standards to reduce the number of attacks. Remote users are required to implement MFA. Other security measures which help in coverage placement include next generation anti-virus (blocking suspicious activity) and spam filtering.
- Due to increase in ransomware losses over the past year, some carriers may be reducing ransomware limits.

"The proximate cause of increased ransomware claims isn't necessarily the increasing number of bad actors, it is a lack of protection. The analogy you draw is if you leave your windows and doors open, don't be surprised if you get burgled."

Protection and Preparation in the event of an attack

Costs associated with a Ransomware attack and how a Cyber Liability policy can protect a company

- Forensic Experts $500 per hour.
- Data Breach Attorneys $500 per hour.
- Notification Costs $3 per affected individual.
- Credit Monitoring $3 per affected individual.
- Public Relations Costs $250 per hour.
- Data Rebuild Employee and 3rd party overtime costs.
- Business Interruption pays % loss of internal revenue.
- Reputational Harm pays % loss of client revenue.
- Ransomware pays the amount of cryptocurrency demanded by hacker.
- Wire Transfer Fraud Average Transaction size.
- Defense costs for 3rd party virus and privacy.

Be prepared ahead of time if an incident occurs

- Discuss claims handling with carrier and agent at the time coverage is bound.
- Internal preparation by company's incident response team and possibly board.
- Consider tabletop exercises so you can identify both internally and externally on who should be involved if an incident occurs.
- Have a reference sheet of the claims contacts so when a claim happens you don't need to scramble to figure out who to contact.
- Transparent flow of information and communication during (not after) incident.

Sources. Tokio Marine, Evolve, Advisen

CYBER READINESS
INSTITUTE

Ransomware Issues in the Health Industry

Alan Ito, Information Security Officer, Hawaii Pacific Health

'It's not a good week for healthcare': Health system IT execs react to recent ransomware attacks

Laura Dyrda (Twitter) - Updated Saturday, October 3rd, 2020 Print | Email

Major hospital system hit with cyberattack, potentially largest in U.S. history

Computer systems for Universal Health Services, which has more than 400 locations, primarily in the U.S., began to fail over the weekend.

Cyber Attack Suspected in German Woman's Death

Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.

Impact to Health Care

- Universal Health Services' (UHS) 400 US sites down for 2.5 weeks (9/27 – 10/13)
- Sky Lakes Medical Center, Oregon (Attacked on 10/27)
- St. Lawrence Health System, New York (3 hospitals) (Attacked on 10/27)
- Sonoma (CA) Valley Hospital shut down systems after 10/11 incident; In 10/30 update, reported it had experienced ransomware attack and has taken all electronic systems off-line

JOINT CYBERSECURITY ADVISORY

Ransomware Activity Targeting the Healthcare and Public Health Sector

AA20-302A

October 28, 2020

TOP NEWS

FBI warns ransomware assault threatens U.S. healthcare system

By Associated Press and Star-Advertiser Staff • Oct. 28, 2020

- 6 ransomware attacks against health care providers within 24 hr. period on 10/27
- Urgent call hosted by FBI and DHHS late 10/27
- Joint Cybersecurity Advisory: Ransomware Activity Targeting the Health care and Public Health Sector issued on 10/28
- NBC News, on 11/2, reported that at least 20 facilities struck so far
- Attackers are Eastern European gang known as UNC1878 or Wizard Spider

What's Known

- Attackers are Eastern European gang known as UNC1878 or Wizard Spider
- Leverages RYUK Ransomware deployed using TrickBot Malware
- Initial attack vector appears to be phishing email campaign
- Leverages Google Docs link to PDF document with link to site to download infection

What's Known (Cont'd.)

- Attackers are known to persist in network for long period of time (100+ days) doing reconnaissance, elevating privileges, moving laterally, exfiltrating data, identifying where most damage can be done
- Planning to attack 400 U.S. health care entities
- Asking for large ransoms

CYBER READINESS
INSTITUTE

Panel Discussion

Thank You!

Visit us at BeCyberReady.com

LinkedIn: @cyber-readiness-institute

Twitter: @Cyber_Readiness

Facebook: @CyberReadinessInstitute