STORAGE DEVELOPER CONFERENCE
SDC 21
BY Developers FOR Developers

Virtual Conference
September 28-29, 2021

A SNIA Event

Ransomware !!!

Practical Steps for Mitigation & Recovery

Presented by SNIA DPPC | DATA PROTECTION & PRIVACY COMMITTEE

Thomas Rivera, CISSP, CDPSE – Security & Privacy Technologist at VMware Carbon Black

Mounir Elmously, Consulting Services Executive at Ernst & Young

Oops, your important files are encrypted.

If you see this text, then your files are no longer accesible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We quarantee that you can recover all your files safely and easely. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $3000 worth of Bitcoin to following address :

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net . Your personal installation key:

mFSbvr- thFa7x-UkLKM7-hFsjHD-NMndbJ-9pitDG-COxnDN-1AZxjD-rLh3Th

If you already purchased your key , please enter it below.
Key:

Never-ending Storm; Constant Threat...

- Not just big organizations are being targeted
- If you are being targeted, you may have no hope
- **Paying ransom is no guarantee of recovery**
- Paying ransom may put you in jail
- Ransomware-as-a-Service (RaaS) and SDKs have made it easier for bad actors to do harm

Presenters

Thomas Rivera, CISSP, CDPSE

Thomas has over thirty years of experience in data storage architectures, with specialties in data protection and data privacy. Thomas is currently at VMware Carbon Black, working on advancing Cybersecurity & Data Privacy standards. Thomas co-chairs the SNIA Data Protection and Privacy Committee (DPPC), and is an active member of SNIA's Security Technical Working Group. Thomas also serves as the secretary for the Cybersecurity & Privacy Standards Committee within IEEE, as well as the secretary for INCITS Cybersecurity & Privacy Technical Committee (CS1).

Mounir Elmously

Mounir has over thirty years of industry experience in information technology with an emphasis around infrastructure technology architecture solutions and business continuity strategies. Prior to E&Y, Mounir held several leadership positions with both well known IT vendors and IT professional services firms. He focuses on leading practices for enterprise technology architecture, data center and disaster recovery strategy services (build, consolidation and migration), telecommunication infrastructure, and business continuity / disaster recovery services, IT cost optimization, emerging technology transformation.

Abstract

- Contrary to the general perception that ransomware is just about extorting money, now it includes reputational and regulatory damage, with severe consequences
- Additionally, attacks are not only aiming at data, now the bad actors have set their eyes on the infrastructure, undermining public confidence and the fabric of society
- This session will cover leading practices, preventive measures, as well as optional recovery measures
- Other SDC sessions explore how storage developers can help when designing products and solutions

Agenda

- Ransomware: What Is It, Why Do We Care
- Victim Landscape
- Preventative Measures
- Recovery Measures
- Recommended Recovery Steps Following the Inevitable
- Summary

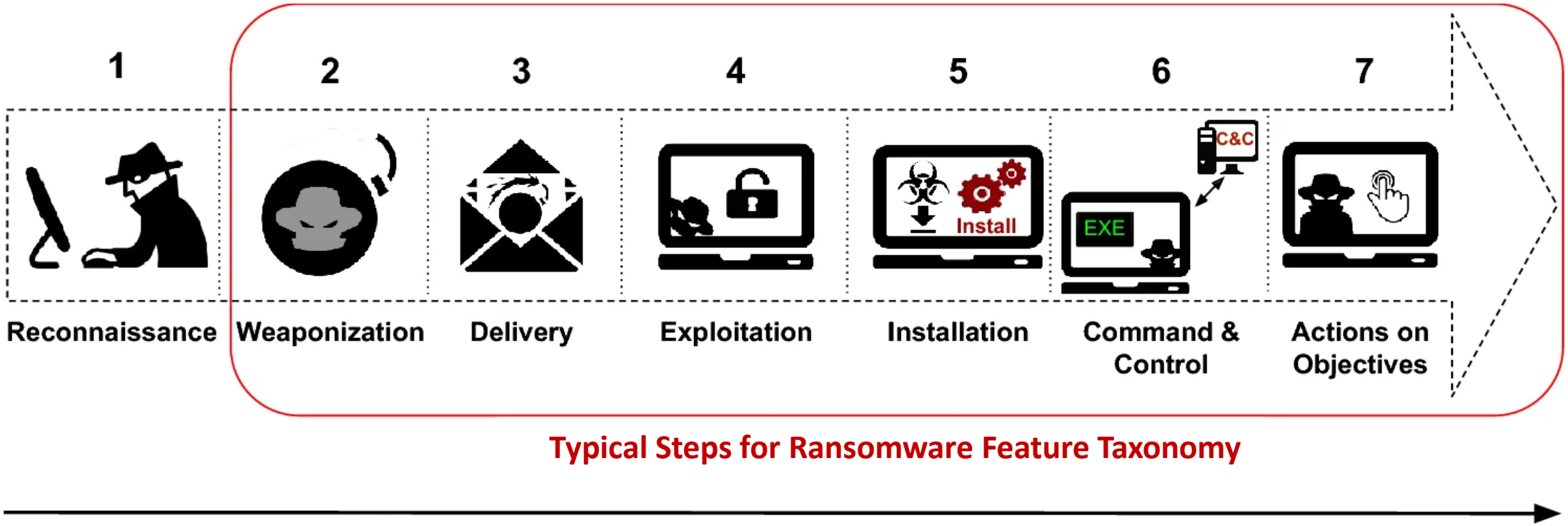
Ransomware: What is it and Why do We Care?

What is Ransomware and Why Should We Care?

- Ransomware is:
  - Software that uses encryption to disable a target's access to its data until a ransom is paid; there is no guarantee that payment will result in the necessary decryption key or that the decryption key provided will function properly

- Why should we care:
  - Do not assume that there is safe haven from ransomware!
  - **Many recent high-profile victims assumed that they were safe after investing heavily in their security posture**

Kill Chain (Sequence of Ransomware Attack)



Typical Steps for Ransomware Feature Taxonomy

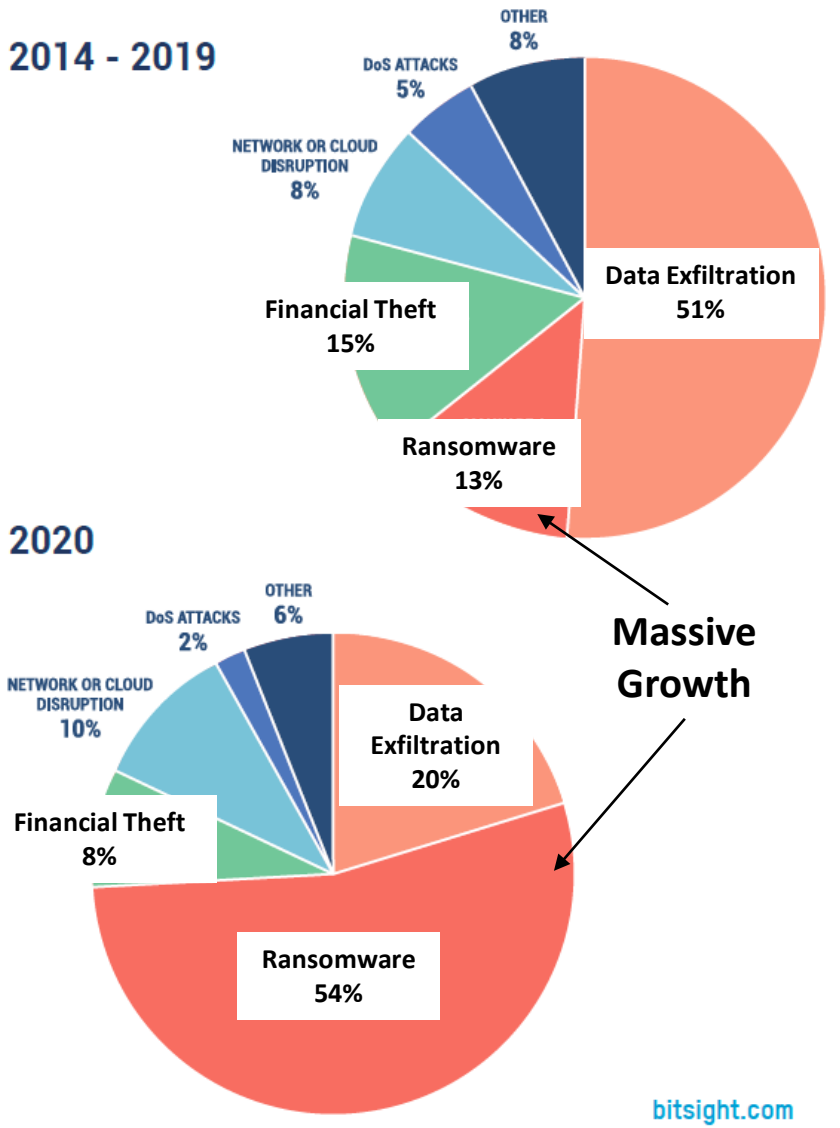
Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Victim Landscape

Ransomware Victim Landscape

- **Everyone is a potential target of ransomware**
- **2020: 84% of U.S. organizations reported phishing or ransomware incidents *[Trend Micro]***
- **2020: The average ransom payment was $312k**
  - **In the first half of 2021, the average climbed 82%, to $570k *[Palo Alto]***
- **2021: Every 11 seconds, a company is being hit with a ransomware attack *[Cloudwards.net]***
  - **It is estimated that by 2031, there will be a ransomware attack every 2 seconds *[Cybersecurity Ventures]***

Cyber Attack Types



bitsight.com

Recent High-Profile Attacks *[More on the way...]*

Healthcare

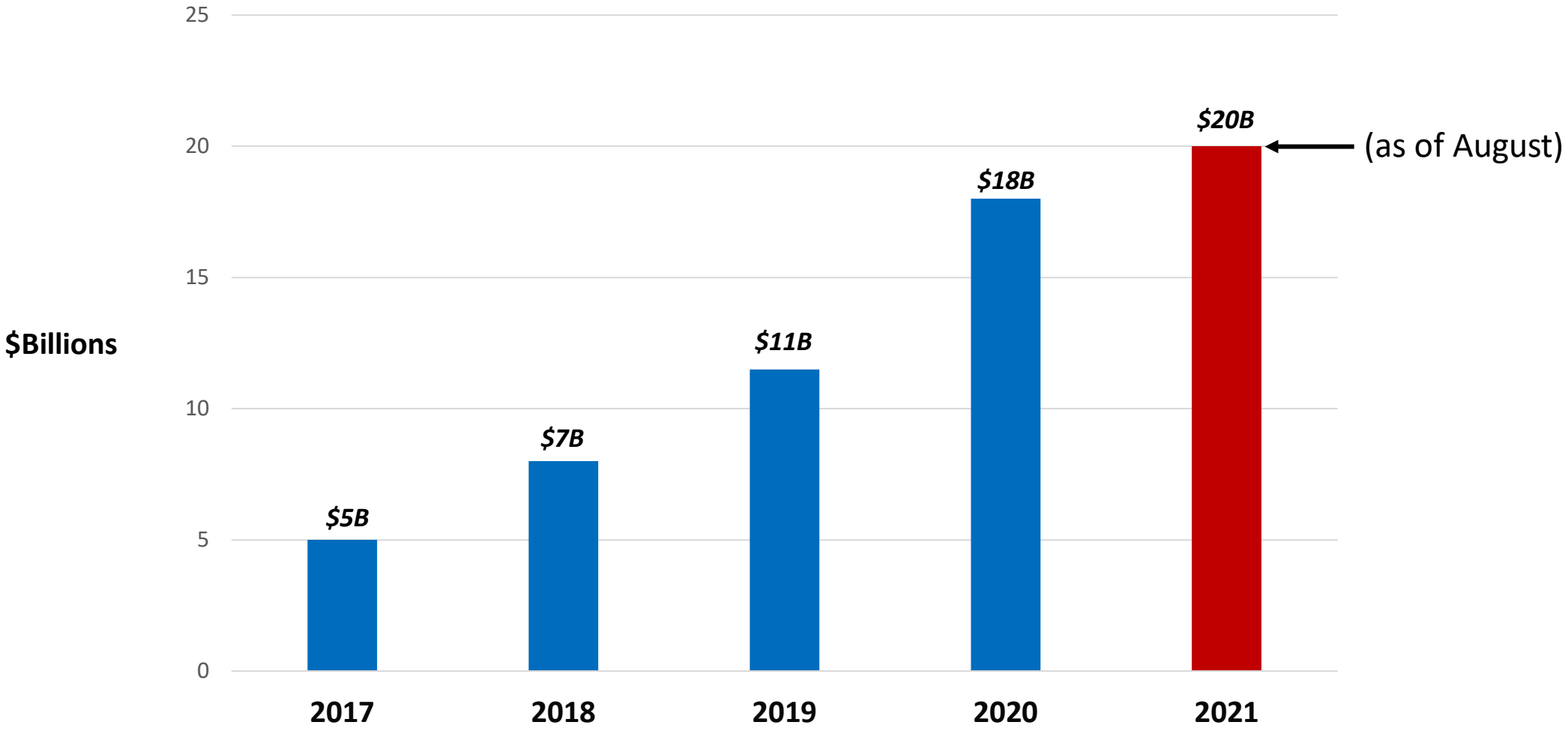
Food Supply Chain

Energy Supply

Common Motivational Criteria:

- **Traditional Ransomware Incentive:** Monetary gain
- **Fighting for a Cause**: To achieve some sort of political, social, or religious goal (Hacktivism)
- **Disruption or Instability**: Threat actors operating under the orders of their employers, governments, or groups
- **Personal Achievement**: Some hackers are simply out to boost their reputation, ego, or marketing purposes

Estimated Global Damage from Ransomware



Source: Cybersecurity Ventures

Preventative Measures

Domains of Preventative Measures*

- Education and Culture
  - Stay alert for social engineering attacks (e.g., phishing emails)
  - Stay clear of links and download attachments from untrusted/unknown sources
  - Use multi-factor authentication
- Administrative (Vulnerability Management)
  - Patch/Update OS, browsers, plugins, etc., regularly
  - Update all application software
  - Use all the necessary security tools, e.g., AV software
- Technology
  - Enforce immutable backups
  - Use micro-segmentation to limit the potential damage following an infection
  - Refrain from using un-encrypted public connections

*For an exhaustive list of actions under each of these domains, please refer to the appendix

Technology – Network Micro-Segmentation

- Micro-segmentation uses network virtualization technology to create increasingly granular secure zones in data centers and cloud deployments, which isolate each individual workload and secure it separately

- Micro-segmentation assumes that every access is malicious and reduces blast radius by adopting macro and micro-segmentation to control vertical and lateral movement

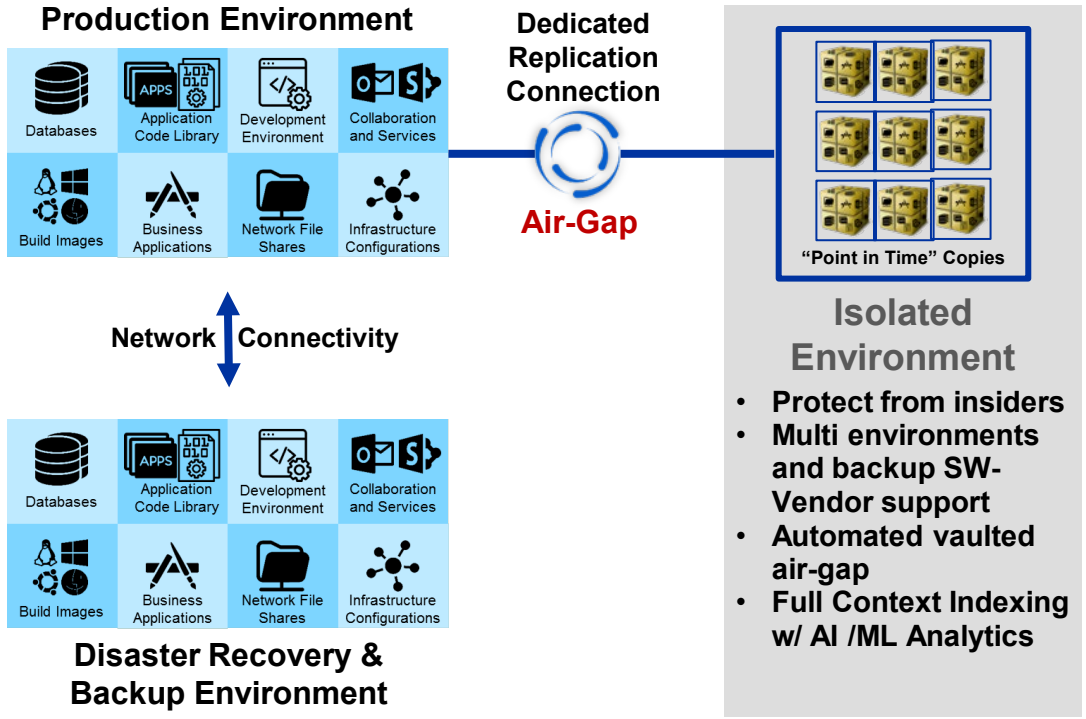
Source: https://www.vmware.com/topics/glossary/content/micro-segmentation
Additional sources are in the Appendix

Recovery Measures

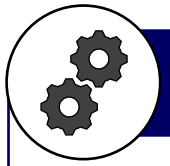
Data Protection Solutions – Air Gap Your Backup

Air Gap Backups

- A network security measure to ensure that multiple copies of critical data are stored on a secure network that is physically isolated from production and DR networks
- Caution: While air gap may help you recover from ransomware, additional measures should be in place to prevent exfiltration of data, which will be discussed in a later slide
- Utilize immutable backups



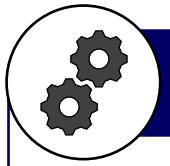
Data Protection Solutions – Snapshots



Snapshots

- Snapshots alone do not provide guaranteed ransomware recovery
- A snapshot is basically the state of a storage system captured at a given point in time
  - Snapshotting offers a quick and effective way to rewind a system to desirable points in time
  - Snapshots are dependent upon the original data set, however, if the original data set is not available, then the snapshots are of no value
- A ransomware attack is likely to prohibit users from accessing production data! A clone of your production data on immutable storage may be your path to recovery

Data Leak Protection Solutions - Encryption



Encryption

- Encryption helps guard against data exfiltration, but not a ransomware protection measure
- Implementing encryption does not prevent re-encrypting data by the bad actor, so encryption may complicate your recoverability efforts
- Key Management is the critical component, and can become the source of the data loss

Technology – Recommended Actions

- Practice good cyber hygiene (Security 101)
  - Patch/Update OS, browsers, plugins, apps, etc., regularly
  - Enforce Multi-factor Authentication
  - Keep antivirus software updated, along with signatures
  - Disable macros
  - Limit remote access to the organization's network
- Deploy "defense-in-depth" methodologies and the principle of least privilege
- Test ransomware recovery capability routinely
- Consider deploying AI IT Operations and predictive analytics
- Categorize and separate data based on organizational value
- Participate in cybersecurity information sharing programs/organizations
  - For example: MS-ISAC and InfraGard

Cyber Protection!! Reality Check

- Cyber insurance is no panacea for ransomware
  - Ransomware payments are increasingly being excluded from cyber insurance policies
  - In many situations, recovery cost is not included in cyber insurance
  - Attacks from nation states or known terrorists may be excluded from cyber insurance policies
  - Infected systems can be considered evidence that cannot be re-built, forcing the company to go through the complexity of sourcing new hardware

Security By Design

- Make ransomware protections part of the design process for emerging storage technology
- Traditional data protection technologies fall short on protecting against the increasingly sophisticated cyber attacks
  - Data protection technologies are likely to the first targets (backup servers corrupted)
- Do not assume that you will be “protected” with emerging storage technology

Recommended Recovery Steps Following the Inevitable

Commonly Employed Response Steps

Always check with your organization's policy for dealing with Incident Response activity!

- Notify the IT/Security Team
- Avoid restarting the computer

Don't Be a Hero!

If and only if you are authorized to:

- Quarantine the affected System
- Make a block-level clone of the infected drive
- Attempt disk decryption with ransomware decryption tools
- Restore infected systems from clean versions
- Restore data from clean backups
- Sanitize removable media, connected drives, etc.

Summary

Final Thoughts

- Threat landscape is changing rapidly
  - Specific regulations may prohibit you from paying a ransom
- Start with “Security 101” (prevention), and build from there
- A ransomware incident may be a reportable data breach for your organization
  - Definition of data breach varies based on geography
- Developers are a target
  - Despite the fact that there may be no revenue, bad actors may consider using the development environment as a vehicle for injecting ransomware into your supply chain
  - Attacks are moving “upstream” in the supply chain; creates an impact on product design, QA, delivery, etc.
- Ensure that you have appropriate security software installed, running, and up to date
- Enforce immutable backups

Additional Resources

- Check out the other SDC presentations from IAPP:
  - “Privacy's Increasing Role in Technology”
    - Cathleen Scerbo, VP/CIO, International Association of Privacy Professionals
  - “Designing with Privacy in Mind”
    - David Sietz, Systems / Solution Architect, International Association of Privacy Professionals
- Check out the other presentations in the following SDC tracks:
  - “Security & Privacy” track
  - “Data Protection Technologies” track
- See Appendix for Ransomware-related references/sources

Thank you for Your Time!

Please take a moment to rate this session.

Your feedback is important to us.

Appendix

Ransomware Reference Docs, definitions, previous tutorials:

- **NIST**
  - **Cyber Tips and Tactics – Preparing your organization for Ransomware Attacks**
  - ***Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*** **(NIST Special Publication [SP] 1800-25)**

- **Cybersecurity Ventures**
  - **Ransomware's Rising Tide is Threatening to Capsize Small Businesses**
  - **Global Ransomware Damage Costs Predicted to Exceed $265B By 2031**

Malware Defined

- Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability *[ISO/IEC 27033-1:2015]*

- Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system *[ISO/IEC 27032:2012]*

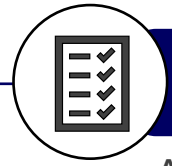
Common Malware Types Used for Ransomware

Name	Associated w/ Ransomware	Definition
Virus	Often	Piece of code that inserts itself into an app & executes when app is run
Worm	Often	Performs autonomous replication w/out embedding itself in another system
Trojan	Often	Hidden code that allows unauthorized collection, falsification, or destruction of information
Adware	Rarely	captures data associated with a user's surfing activity to build a profiles to determine which ads to serve them; tracking data can be shared or sold to advertisers without consent
Spyware	Sometimes	collects information (passwords, PINs, payment information, etc.) about users' activities without their knowledge or consent
Rootkit	Sometimes	Gives remote control of victim's computer with full admin privileges
Bot/Botnet	Sometimes	Performs automated tasks on command; used in large numbers (botnet) to launch broad remotely-controlled attacks

Common Malware Types

Name	Associated w/ Ransomware	Definition
Keylogger	sometimes	Monitors user activity and can be used to steal password data, banking information and other sensitive information
Fileless	Sometimes	Code that runs in memory (no installation) that makes changes to files that are native to the operating system; not caught by AV software
Cyptojacking	Rarely	Uses a victim's computing power to mine cryptocurrency
Ransomware	Always	Uses encryption to disable target's access to its data until a ransom is paid; there is no guarantee that payment will result in the necessary decryption key or that the decryption key provided will function properly
Blended	Often	Executes multiple type of malware as part of an attack

Preventative Measures



Education and Culture (Individuals)

A. Stay alert for social engineering attacks (phishing emails)
B. Never click on links or download attachments coming from untrusted on unknown sources
C. Practice safe browsing
D. Have strong passwords, change passwords periodically
E. Refrain from using un-encrypted public connections
F. Restrict personally owned devices on work networks
G. Use standard user accounts versus accounts with administrative privileges whenever possible
H. Apply the principles of least privilege and network segmentation.
I. Avoid using personal apps—like email, chat, and social media—from work computers
J. Have an incident response plan that includes what to do during a ransomware event
K. Use antivirus and anti-spam solutions.
L. Enable regular system and network scans with antivirus programs enabled to automatically update signatures
M. Implement an anti-spam solution to stop phishing emails from reaching the network. Consider adding a warning banner to all emails from external sources that reminds users of the dangers of clicking on links and opening attachments. Invest in staff training to increase awareness of what to look for

Preventative Measures (Continued)

Administrative

1. Separation of duties
   A. Use different credentials for Backup versus primary storage
   B. Administrators to have update (write) access segregated between the backup and primary storage environment
2. Diligent and periodic Elevated access reviews
   A. To ensure appropriate personnel have the correct access to perform their jobs
   B. Minimum of quarterly access reviews
3. System and application Backups
   A. Take Storage snapshots on backup storage if possible
   B. Air gap infrastructure to capture backups
   C. Offline storage should be implemented for backups
4. Enhance monitoring of cyber security with increased analytics to prevent or quickly identify risk situations

Preventative Measures (Continued)

Administrative

1. Have visibility into suspicious behavior
2. Perform penetration exercises to identify gaps and exposures
3. Review and exercise your incident response plan.
4. In light of the growing trend of ransomware attacks and to keep ransomware from potentially attacking your backup data first, we've modified the Backup Best Practice to the 3-2-1-1-0 rule:
5. Maintain at least 3 copies of business data
6. Store critical business data on at least 2 different types of storage media
7. Keep at least 1 copy of the backups in an off-site location
8. In the ransomware era, it's a good idea to add another 1 to the rule where one of the media is offline
9. Ensure all recoverability solutions have 0 errors

Preventative Measures (Continued)

Technology

A. Patch/Update OS, browsers, plugins, etc. regularly
B. Update all application software regularly
C. Use all the necessary security tools (antivirus software)
D. Layer your security starting with basic measures like firewall and antivirus
E. Consider micro-segmentation of the network to limit the spread of bad code and limit bad actors from accessing most resources on the network
F. Disable macros scripts. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications
G. Backups are critical. Use a backup system that allows multiple iterations of the backups to be saved, in case a copy of the backups includes encrypted or infected files. Routinely test backups for data integrity and to ensure it is operational.

Preventative Measures (Continued)

Technology

A. Restrict Internet access. Use a proxy server for Internet access and consider ad-blocking software. Restrict access to common ransomware entry points, such as personal email accounts and social networking websites. Configure operating systems or use third-party software to allow only authorized applications on computers.
B. Categorize and separate data based on organizational value and where possible, implement virtual environments and the physical and logical separation of networks and data. Apply the principle of least privilege.
C. Vet and monitor third parties that have remote access to the organization's network and/or your connections to third parties, to ensure they are diligent with cybersecurity best practices.
D. Participate in cybersecurity information sharing programs and organizations, such as MS-ISAC and InfraGard.

