Cyber Ransomware Attacks:

Change your cyber security perspective to reduce your risk

troywebconsulting

Learning Objectives:

- Understand Ransomware and the risk it poses to manufacturing operations.
- Use a cyber attackers perspective and learn about the “Cyber Security Kill Chain”
- Learn how cyber criminals leverage social engineering to deliver ransomware into your environment.
- Learn simple steps and best practices to reduce your exposure to a cyber security incident.

troywebconsulting

About: Me

Rick Stegmann
rick.stegmann@troyweb.com

- Worked in the Information Technology industry for 35 years
- Managed IT supporting the development of over 35 Video Game Development Projects with Activision
- Former Chief Information Officer
- Worked extensively with DHS supporting SLTT Government entities with cyber security
- Work with small and medium size organizations and local governments on cyber security best practices and Social Engineering Awareness

About: troywebconsulting

- Troy Web Consulting is the custom software development partner of choice for companies that want to optimize their business processes and customer experiences with efficient, secure and reliable software application solutions.

- Design
- Development
- Testing
- Deployment / Cloud / Integrating
- Automation

www.troyweb.com

Agenda

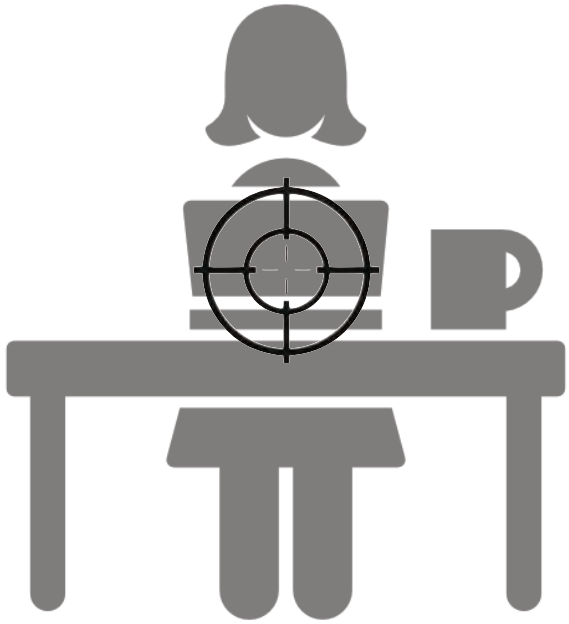
- The anatomy of ransomware and the tactics used in an attack.
- Define Social Engineering and how Phishing is used to distribute ransomware.
- What is the “Cyber Security Kill Chain”
- Take a Cyber Selfie, to better focus your cyber security activities
- Best Practices you can use to reduce your exposure to a cyber security incident.
- Summary & Recommendations
- Closing Thoughts and Video, Kim Loyd

troywebconsulting

Understanding Ransomware

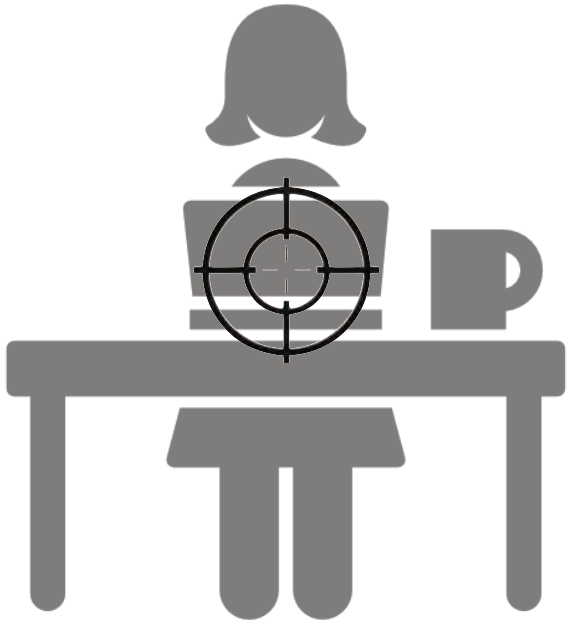
Ransomware Statistics

- In 2017, 80% of Victims who paid ransom got their files back.
- According to a Symantec ransomware report, in 2019, only 47% of people who pay the ransom get their files back
- 60% of all malware payloads contain some form of ransomware
- Every major OS has been targeted, Windows, Mac OSx, Linux, Android, even smart TVs



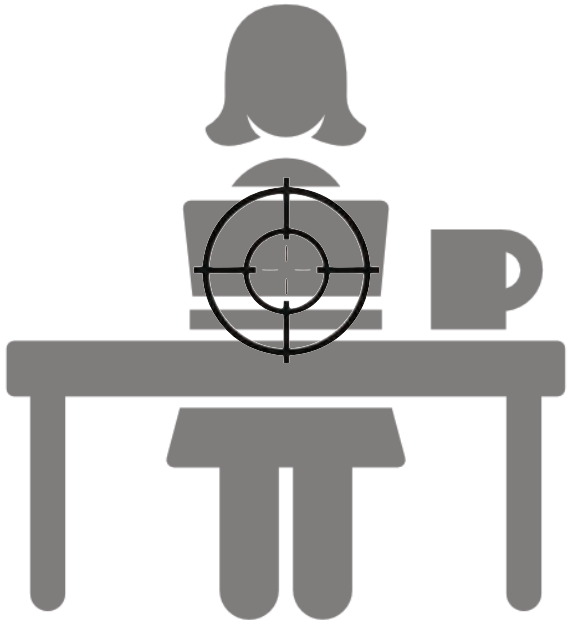
About: Ransomware

- There have been over 500 Ransomware “Families” identified.
- Popular ransomware names include WannaCry, SamSam, Crypto-Locker, Crypto-Wall
- WannaCry is both ransomware and a worm, which allowed it to spread to other systems without any further intervention



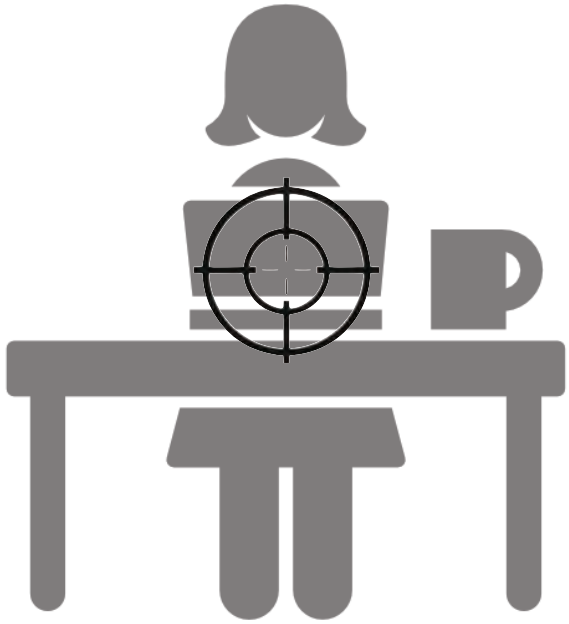
About: Ransomware

- Ransomware code is easily obtainable on the Internet via GitHub or PasteBin
- There are even actors who run RaaS, Ransomware as a service, and will take a percentage of the ransom collected
  - They provide all the tools, even a GUI to manage attacks. Makes it more approachable for less technical attackers



About: Ransomware

- Almost all ransomware attackers rely on some sort of secure payment systems such as bitcoin, Monero, Lightcoin, which makes tracing payments impossible.
- There are also crypto currency laundering services.
- iTunes and other gift cards are also often popular payment methods, especially with opportunistic attacks
- Actors will use TOR (The Onion Router) to route encrypted communications with the victim, and hide the destination and location of the attacker



Why Are Manufacturers Targets?

- They may manufacture components for the defense industry and hold “Confidential Unclassified Information” or CUI
- They may manufacture components for unreleased products and hold detailed specifications or other proprietary information
- The components or techniques used in manufacturing may be proprietary
- Many are well financed organizations, Large payrolls, and receivables
- Many are dependent on 7x24 operations, Delivery Deadlines and complex supply chains

Ransomware Categories

Ransomware typically will fall into one of three categories:

- **An Encryptor**, Encrypt files to deny access until ransom is paid
- **A File Locker**, Sometimes less sophisticated, Locks computer or device, May take a desktop screenshot and display it with ransom message, disable access to file system
- **A File Wiper**, Still encrypts, but erases files is ransom not paid. Does full erase to ensure no recovery possible, Some erase a number of files every hour until you pay ransom. Some variants will erase everything if you don't pay in a limited time period

Ransomware Attack Modes

Two common attack modes:

Ransomware Attack Modes

- Spray n Pray Mindset, the more infections, the more potential revenue can be generated.
  - By sending high volume of phishing messages, even a 1% infection rate will deliver a good financial return.
- Ransom amounts typically smaller, $100-$300 ransoms not uncommon, Might be as high as $1000.00

Ransomware Attack Modes

- Targeted attacks, ransom generally much higher, amount is based on target organization
- Any organization with reliance on 7x24 uptime, high public visibility of outage are targets.

Ransomware Attack Modes

- Strategic attack targets sometimes are identified by opportunistic attacks.
- These types of attacks are often result of a detailed business analysis and extensive reconnoissance by the attackers

Ransomware Tactics

- Some ransomware packages will use complex encryption algorithms, while other variants will only encrypt the first bytes in a file.
- May try to disable system Anti-Virus
- Able to determine if it is running in a virtual environment

Ransomware Tactics

- Able to look for common malware analysis or detection tools like Wireshark
- Patch itself by downloading any needed updates
- Drop decoy code to impede forensics and analysis
- Hide in the system registry, File-less Attack

Ransomware Tactics

- Enable encrypted communication with command and control.
- Some malicious payloads carrying ransomware will first install other tools to harvest credentials and email addresses prior to encrypting the data, to maximize revenue potential.
- Many ransomware infections can also install backdoors and other malware, permitting reinfection or other malicious activity.
- Ransomware can look for hundreds of common file types, .docx, .txt .xls etc, including common backup files as targets to encrypt.

Ransomware Delivery

- Social Engineering tools like Phishing and Spear Phishing are common methods of ransomware delivery, especially with strategic mode attacks
- Other methods exploit unpatched vulnerabilities in software and operating systems gain access

Ransomware Delivery

- Eternal Blu exploit affects SMB “server message block” protocol, common in Windows environments
  - MS17-010, CVE2017-0147, patches vulnerability for eternal blue
  - Move to SMB v2 or v3 if possible, or don’t use SMB at all if possible
- Earlier versions of WannaCry and NotPetya ransomware, leveraged vulnerabilities in JBOSS
- Dharma and Sam-Sam Ransomware exploit RDP Protocol

Ransomware Delivery

- By exploiting vulnerabilities in software and operating systems, attacks can be automated, and require less human interaction than when using phishing.
  - These methods also help attackers move laterally in a network, by finding more vulnerable or unpatched systems

Conclusions

- Remember, Ransomware is a business, with attackers constantly evolving and seeking to improve their revenue potential.

Social Engineering, Phishing, and Ransomware

Social Engineering Defined

What is Social Engineering?

- Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information.
(Wikipedia)

troywebconsulting

Why Is Awareness of Social Engineering So Important?

- Comments Made by Notorious Hacker Kevin Mitnick
  - *"The weakest link in the security chain is the human element"*
  - *"You can spend a fortune on purchasing technology and services and you will still be vulnerable to old fashioned manipulation"*

Social Engineering: Phishing

- Phishing Scams are a common method of delivering Ransomware and Malware into your environment.
- Phishing: Sending legitimate looking emails that are crafted and designed to fool the recipient into following false links, providing credentials, or opening a malicious attachment
- The overall goal is to install software on the recipients' computer or gain sensitive information including credentials

Social Engineering: Phishing

- Types of Phishing Attacks:
  - Opportunistic Phishing
  - Spear Phishing
  - Whaling

➡ Number of Targets
➡ Message:
➡ Thousands
➡ Targeted, Specific
➡ Focused, Customized

troywebconsulting

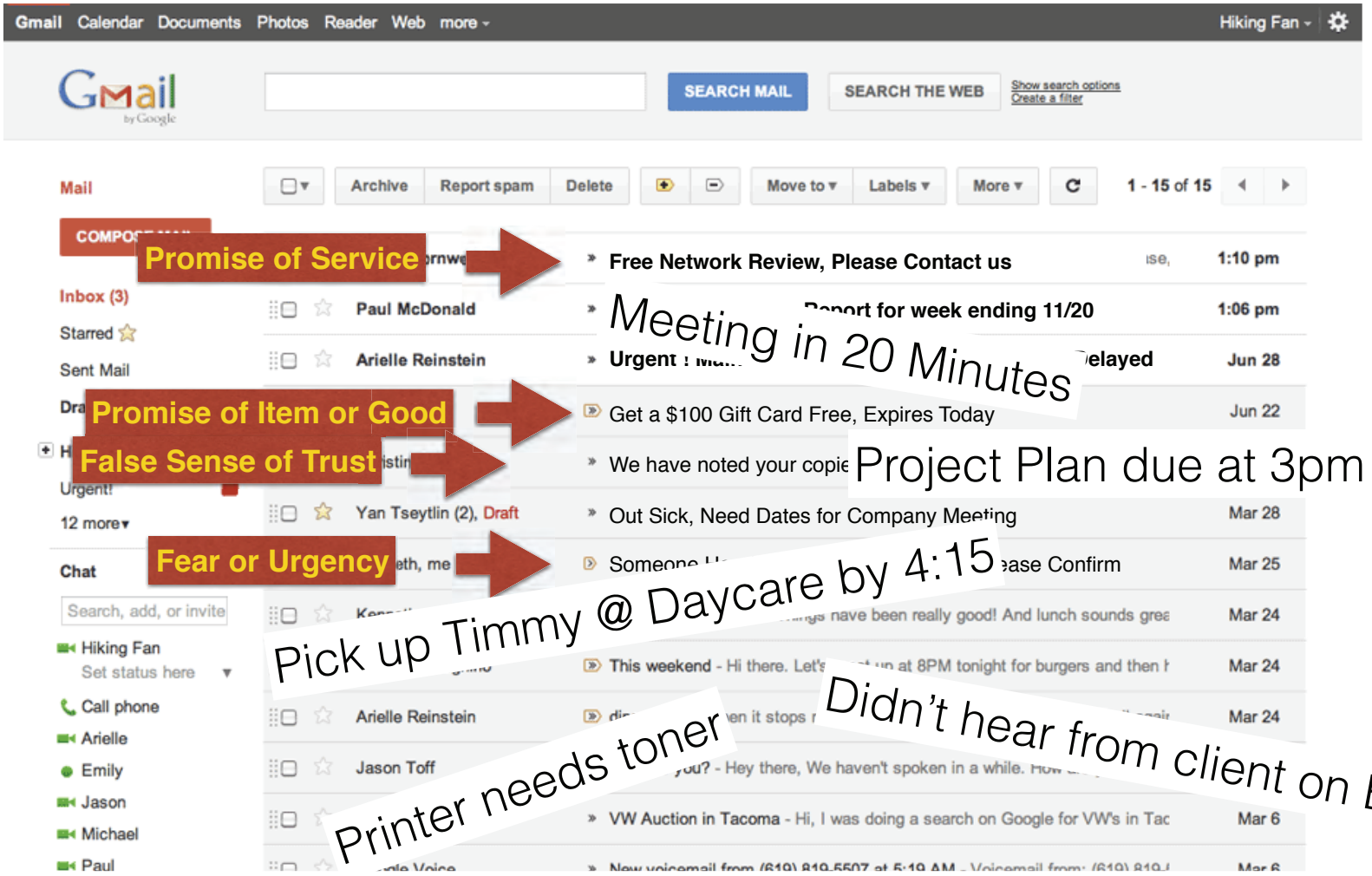
Social Engineering Tactics Used In Phishing Attacks

Use Fear or Urgency

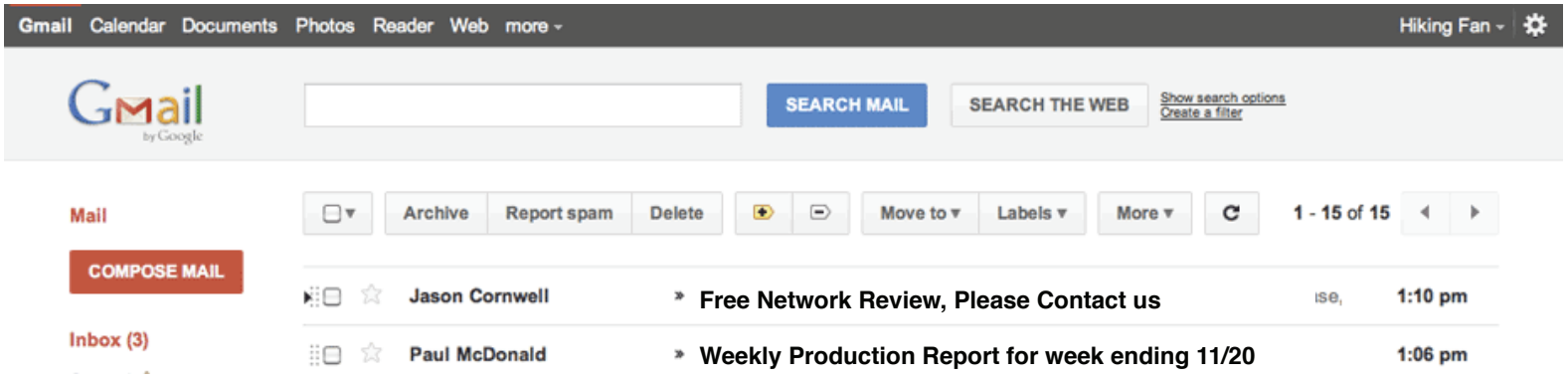
Build False Sense of Trust

Promise of an item or good

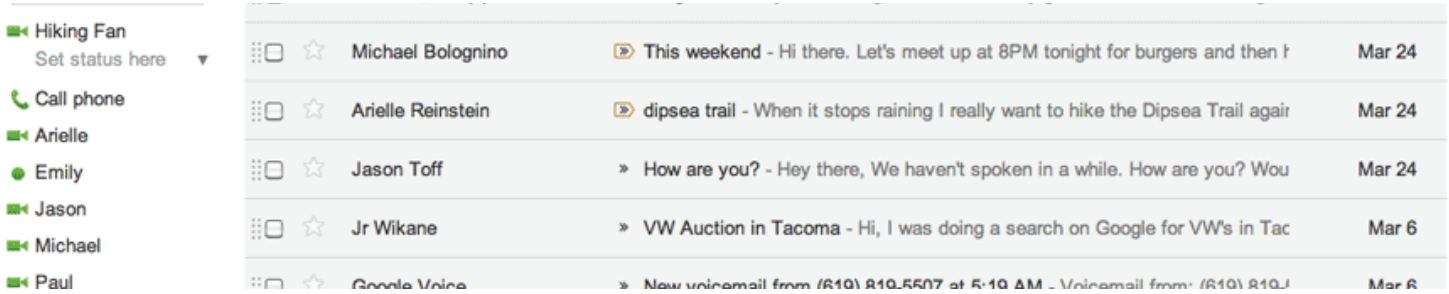
Offer of benefit or service



troywebconsulting



Employees and Managers need to be trained and conditioned to consider all of the common tactics of social engineering for each and every message <u>BEFORE</u> taking any action



Steps for Awareness of Social Engineering

- Conduct regular cyber security awareness training during the on-boarding process, and periodically thereafter.
- Institute a “Cyber Amnesty Program”
- Have well thought out policies and procedures as well as an Acceptable Use Policy for technology

Steps for Awareness of Social Engineering

- *Make cyber security part of your organizational culture*
- *Doing so will convert your staff from a cyber security liability into an asset.*

Turning the Cyber Security Lens Around

troywebconsulting

An attacker only needs to take one successful action to achieve their “win.”

Outward Facing Security Perspective

Common Detection Model

Organization's commonly invest their cyber security resources from an inside, facing out perspective

The typical detection program is designed to monitor as many of the organization's assets as possible, and to trigger alerts when things like malware is detected or cyberthreat indicators are identified.

What If We Look From The Outside In ?

What if we viewed our organization's attack surface from the attacker's perspective so we can focus resources on addressing the vectors and vulnerabilities that the attacker may see or detect.

Cyber Security Kill Chain

Attacks by seasoned hackers are broken into seven phases commonly called The:

“Cyber Security Kill Chain”

Cyber Security Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions and Objectives

Cyber Security Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions and Objectives

Cyber Security Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions and Objectives

Cyber Security Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions and Objectives

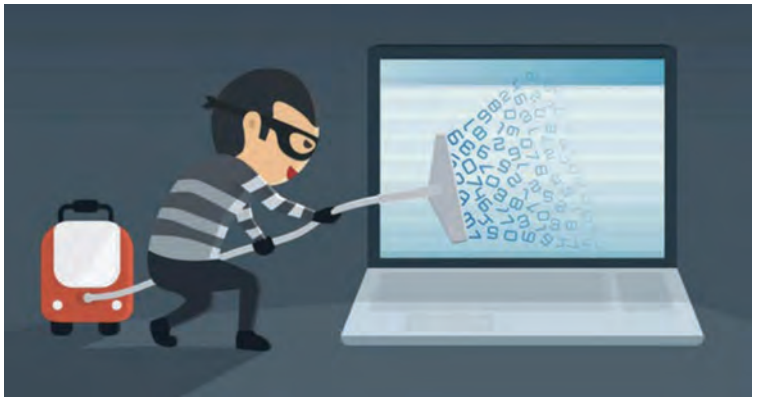
Cyber Security Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions and Objectives

Cyber Security Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions and Objectives

Cyber Security Kill Chain



- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions and Objectives

Cyber Security Kill Chain

Reconnaissance: Closer Look

Reconnaissance

Cyber Reconnaissance

- Seasoned attackers spend considerable time doing detailed research on their targets.

- This is considered the most important and time consuming phase, as it can take weeks or months. No detail is too small. Email addresses, names, phone numbers can all be important to the attacker.

Reconnaissance

Two Modes of Reconnaissance

Perspectives On Reconnaissance

Organizations Perspective

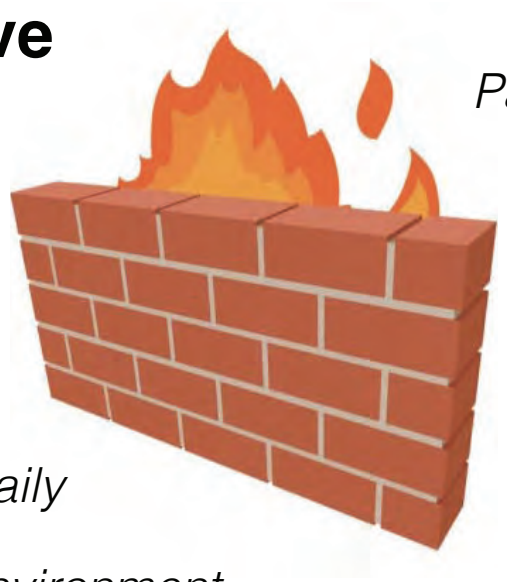
Be aware of your online footprint

Know your network, technologies, and vulnerabilities

Review your logs, Daily

Penetration Test Your Environment

Training and Team Awareness



Attackers Perspective

Analysis of Target

Passive: Open Source Information
Social Media Posts
Email Lists

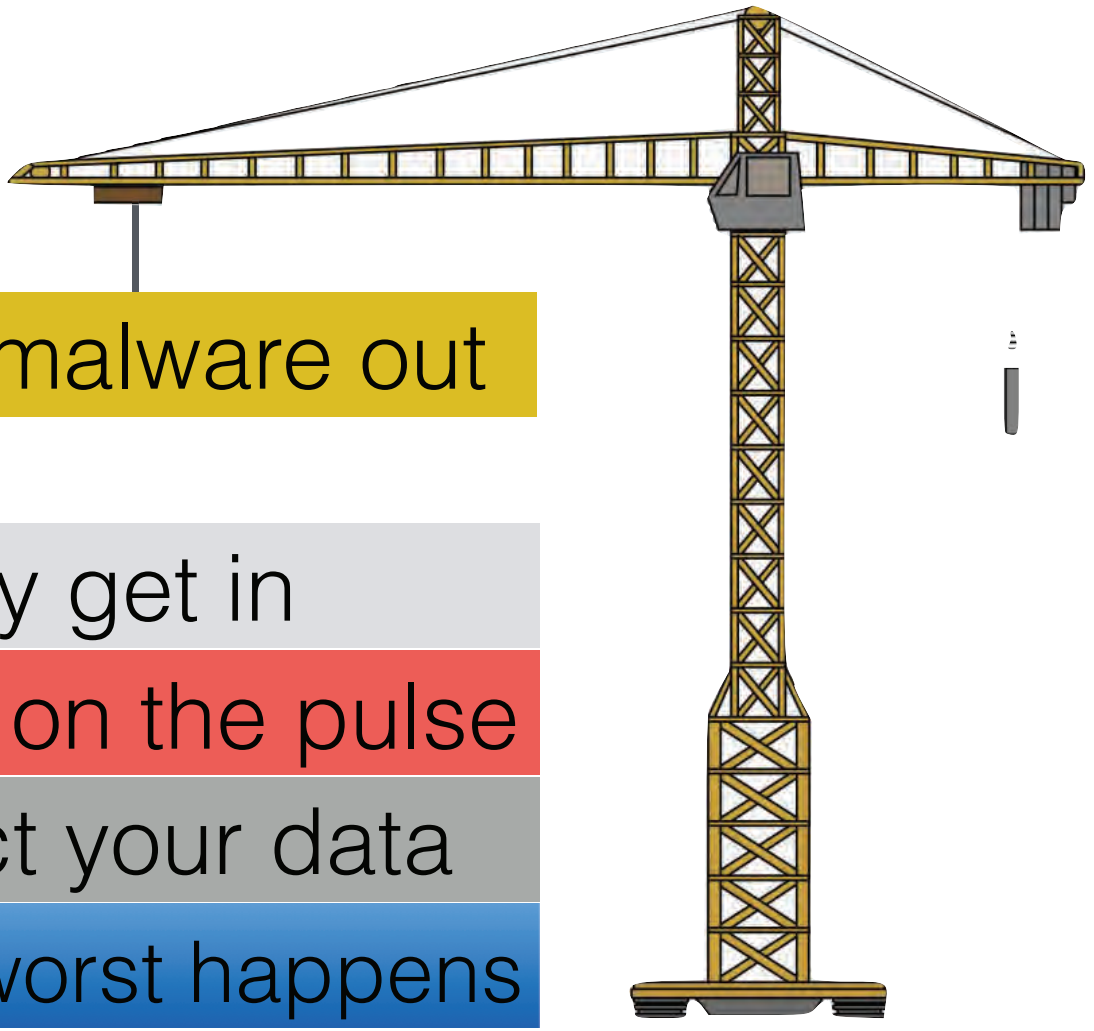
Active: Portscans,
Login Attempts
Brut Force Methods

Know the target network better than the people who run and maintain it

Best Practices For Cyber Security and Ransomware Risk Mitigation

troywebconsulting

5 Building Blocks For Cyber Security Success



Keep dangerous malware out

Stop threats if they get in

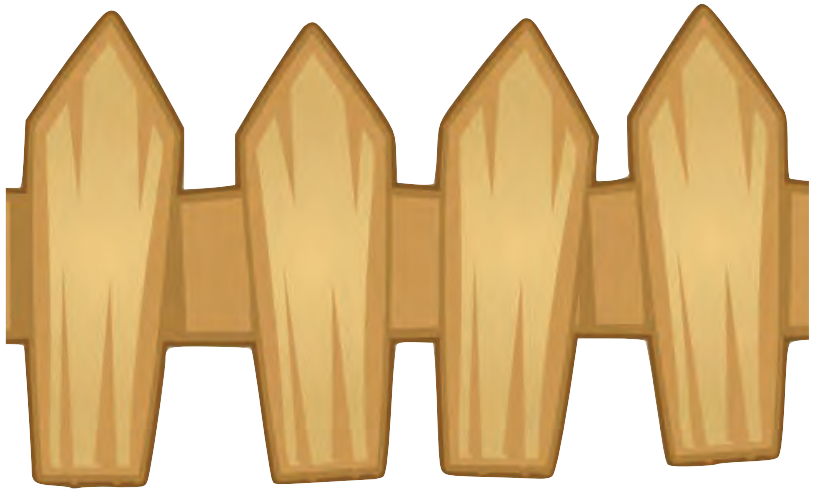
Keep your thumb on the pulse

Proactively protect your data

Have a plan if the worst happens

Keep Dangerous Malware Out

- Use DEMARC - SPF, DKIM
  - (Domain-based Message Authentication, Reporting & Conformance)
- Use an External Mail Filtering service, scan all inbound and outbound emails
- Pass Web Traffic Through a Web Proxy
  - White List of acceptable sites
- DNS Black Listing Service



Stop Threats if they Get In

- Have Comprehensive Patching Program, OS and all Applications
  - Only install software, updates, and patches from known good sources
- Avoid “Flavor of the day” applications. Standardize
- Be cautious with open source tools
- Institute a change control process

Stop Threats if they Get In

- Leverage centrally managed anti-virus tools
- Never allow users to run as Admin when doing common tasks, email, browsing Restrict who has the ability to install software in your environment.
- Use Browser plugins to block ads and popups
- Enforce a complex and unique password policy or better yet use Two Factor Authentication

Keep Your Thumb On The Pulse

- Know your environment better than your advisories
- Maintain a complete inventory of ALL hardware and software. You need to know what you have to know if and when it is vulnerable and needs patching
- Control and Protect Mobile Devices that hold your data
  - Prohibit rooted mobile devices

Keep Your Thumb On The Pulse

- Expect cyber security excellence from your vendors and partners whose systems and data you share.
- Verify by doing your due diligence.
- Target breach is a prime example of a vendor induced breach

Keep Your Thumb On The Pulse

- Establish Metrics that are both meaningful and measurable.
- Examples of useful metrics
  - How long it takes to apply a patch for a critical vulnerability across your enterprise.
  - Number of days to deactivate former employee account”
  - Number of accounts with administrative privileges
- Example of a less useful metric is the number of virus alert related trouble tickets received in a week. Lots of potential variables in this example

Keep Your Thumb On The Pulse

- Deploy consistent software images on your systems, document any non standard configurations
- Segment systems that handle CUI on a separate network segment
- Log as much activity as possible and Review your logs daily
- Nothing is bulletproof, Best Practices can be your friend by helping remove low hanging fruit from the table

Proactively Protect Your Data

- Know what data you hold, and where it is stored, AND backed up, especially CUI and proprietary data
- Implement a “Need to know policy” if you have not, Understand who can access what data and how they can manipulate, copy or delete data.
- Follow the 321 backup rule, Minimum 3 full backup copies at all times, 2 copies on different media types, 1 copy stored offsite
- Securely store backup media, ensure backup devices are physically secure. Encrypt your data backups

Proactively Protect Your Data

- Do you have comprehensive, well documented Business Continuity, Disaster Recovery, and Incident Response Plans?
  - Consider both external and insider threats
  - Have you exercised your plans?
  - It is critical that incident response plans are tested across the whole operation, not just in the IT department.
  - Is your organization prepared to work with government regulators and or cyber incident responders?
    - Do you have complete and up to date documentation for your environment?

Proactively Protect Your Data

- Encrypt your data both at rest and in transit
- Have well thought out acceptable use policies and ensure staff is trained in them and that they are enforced
- Establish Recovery Time Objective, Recovery Point Objective (RTO/RPO) that aligns with your business requirements, what could you afford to loose, how long can you be down?

Proactively Protect Your Data

- Are you protected from the “Speeding Bus Syndrome”? Are all critical skills needed for a cyber incident held with one individual, or do you have a team who can handle IT, incident management, and apply cyber security as an institutional practice
  - Create a repeatable process and cross-train employees to conduct risk and incident management as an institutional practice. Too often, there is only a single employee with subject matter expertise in key areas.

Proactively Protect Your Data

- Implement industry standards and best practices rather than relying solely on compliance standards or certifications.
- Follow best practices from organizations like NIST or The Center for Internet Security.
- Tailor best practices to ensure they are relevant for their specific use cases.

Have a Plan if the Worst Happens

- Follow your incident response plan
- There are tools available to you if you are attacked (your milage may vary)
  - https://nomoreransome.org
  - https://sensorstechforum.com
  - Offers hundreds of tools and information on how to defeat the ransomware and retrieve data

Have a Plan if the Worst Happens

- While clearly a business decision driven by individual situations, organizations should resist paying ransom as the funding perpetuates to problem.

Summary and Recommended Actions

- Assess your environment to understand your current cyber security posture
  - Leverage Available Best Practices like NIST 800-171, 800-53, CIS Critical Controls
  - Prioritize mitigation of your weaknesses. Don't try to "drink the ocean", but make regular step by step progress
- Be Proactive
  - Remove vulnerabilities by patching and updating your systems and applications, Remove/upgrade Legacy or End-of-Life Systems and applications
  - Have a well thought out data backup and recovery system, and exercise it
  - Develop your acceptable use policies, incident response plan, and BC/DR plans, and exercise them before you need them
    - Ensure your plans encompass your entire operation, not just IT, and develop detailed documentation of your environment

Summary and Recommended Actions

- Make your staff a cyber security asset
  - Train regularly on cyber security, acceptable use policies, as well as the dangers of social engineering
  - Make Cyber Security part of your organizations culture
- Do a cyber selfie and view your environment from the outside in, just like an attacker would
  - Know your environment better than the bad guys
- Expect your vendors and partners to take security as seriously as you do.
  - Set minimum requirements to share data or access systems. Do your due diligence (Trust but Verify)