Ransomware and Cyber-Awareness
Presented by Max Greene S.E.P.P
Ransomware Evolution
The father of modern ransomware
Your network has been penetrated.

This link and your decryption key will expire in 21 days after your systems were infected. Sharing this link or email will lead to the irreversible removal of the decryption keys.

**NO TIME remains for special price.**

All files on each host in your network have been encrypted with flawless algorithm. Backups were either encrypted or deleted and backup disks were formatted. **There is no working decryption software that may solve this.**

Do not rename the encrypted or informational text files. Do not move the encrypted or informational text files. This may lead to the impossibility of recovery of the certain files.

Also, we have gathered all your private sensitive data. So if you decide not to pay, we would share it. It may harm your business reputation.
Your files and documents have been encrypted!

What happened to my files?
Your photos, documents, and videos on this computer have been encrypted with AES-256. To get your files back you will need to purchase your encryption key within the set date, failing to pay will result in the destruction of your key.

How do I obtain my key?
The key produced for your computer is stored on our server. To obtain the unique key for your computer, which will decrypt and recover your encrypted files, you will need to pay a fee in Bitcoin/UKash/PSC prior to the key destroy date. After that your key will be destroyed and nobody will ever be able to recover your files.

Payment Method
Bitcoin (Cheapest Option)
Preparing for Ransomware
Protecting Your Data
Information Security

• The state of being protected against unauthorized use or access of information

• The practice of protecting information by mitigating information risks
The Three Tenets of Information Security

Every element of an Information Security Program should be designed to achieve one or more of these principles.
**Confidentiality:** Preventing unauthorized disclosure and use of information

**Integrity:** Preventing unauthorized creation, modification or deletion of information

**Availability:** Preventing unauthorized delay, or denial of information
Preventing Infection
Recognizing Fraud
In the last 12 months, cybercriminals launched thousands of new phishing pages every hour to harvest personal information, steal corporate data, and commit credit card fraud with no sign of slowing down.

- Phishing increased 42% in 2020, over 2019
- By mid-2020 phishing threats top 25,000/day, a 30% increase over 2019 figures
- By fall, it hit 35,000/day…
- And grew to 50,000/day by December
- Attacks continue to rise in 2021

Source: SlashNext Threat Labs
Visit the account and log in directly!

---

**Your Account Has Been Suspended**

Dear Netflix,

We are sending this email to let you know that your credit card has been expired. To update your account information, please visit [Your Account](mailto:Your Account).

-Your friends at Netflix
Be mindful of what you are clicking!

From: Bank of America <crvdg@comcast.net>
Subject: Notification: Irregular Activity
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients.
Reply-To: crvdg@comcast.net

Online Banking Alert

Dear member:

We detected unusual activity on your Bank of America debit card on 09/22/2014. For your protection, please verify this activity so you can continue making debit card transactions without interruption.

Please sign in to your account at https://www.bankofamerica.com to review and verify your account activity. After verifying your debit card transactions we will take the necessary steps to protect your account from fraud. If you do not contact us, certain limitations may be placed on your debit card.

© 2014 Bank of America Corporation. All rights reserved.
Don’t be fooled by click-bait!

From: Docusign with World Health Organization BR <contato@redem4.com.br>
Sent: Friday, March 13, 2020 10:35:50 AM
To: [Redacted]
Subject: Health Message: Important health guidelines and information about corona virus

WHO guidelines against Corona Virus, sign in to download the instructions.

Source: IANS, 2020
Think before you click!

Be aware of any attachments you receive or download via email

If malicious they can install malware or unwanted software onto your device
Recognize SMS Text Message Fraud

Your statement is ready for you to view online. Go to https://goo.gl/ak9t3k to view and manage your account.
Browsing Rule

1. Forward Slash

www.aa.airlineaamemembers.com/seat/us

2. Two Dots Back

Forward Slash, Two Dots Back
Customer Satisfaction Survey

Share your opinion - Chase will add $100 credit to your account just for taking part in our quick survey. With the information collected, we can decide to direct a number of changes to improve and expand our services.

Note: Only one survey per card is allowed. If you own multiple cards, you can run the survey again for each.
Website Fraud

- International domain names system abuse
- Hyperlink display name
- Bad sites with SSL certificates
- Using cheap website templates
Recognizing Fraud Checklist

- Do you recognize the sender?
- Have you hovered over the link?
- Do we see any red flags?
- Are we getting any high-risk requests?
- Did we initiate this?
Social Engineering
Social Engineering is the action of exploiting human nature rather than technical hacking techniques to gain access to systems, data or buildings.
The Who
The Adversaries

Insider
- Financial Gain
- Grievance
- Targeted

Hacker
- Financial Gain
- Opportunistic
- Bragging Rights

Cyber Criminal
- Financial Gain
- Opportunistic

Cyber Hacktivist
- Grievance
- Targeted

Cyber Terrorist
- Political Warfare
- Targeted
The Why
A \rightarrow B \text{ easy way}

A \rightarrow B \text{ hard way}


“Why doesn’t this feel risky?”

- **Availability Heuristic**
  "If I can’t recall specific instances of this happening, it doesn’t feel risky."

- **Optimism Bias**
  "Bad things only happen to others."

- **Level of Control**
  "This problem is too big. I have no control over what happens."

- **Risk Homeostasis**
  "I am so used to this level of risk; it will have to be raised or lowered dramatically for me to re-engage."

- **Group/Social Norms**
  "I don’t want to be ostracized by my co-workers or friends."
Responding to Infection
**Preparation** is the most important phase to incident response. It enables you to effectively respond to any incident. Planning should include the following elements: Training, Budget (your plan must be funded and in place before an incident occurs), Practice (tabletop exercises including senior management are critical in order to achieve resilience).

**Detection** is the process of determining if a breach has occurred. 49% of security alerts triggered by endpoint devices were found to be false positives. Breaches are typically discovered in one of four ways: Reviewing system logs for anomalies, third party notification, Law enforcement notification, **All files on you network area encrypted.**

**Containment** The affected devices are identified and isolated. This is when the response team is notified along with legal counsel, insurance, and law enforcement…. This is when the incident becomes real… it’s stressful…don’t panic.

**Investigation** is the phase where priorities are determined along with the size and cause of the incident. Forensics will be taking place.

**Remediation** you begin to restore business operations, legal counsel will guide you on regulatory requirements / notifications. Your organization will be judged on how you handle this phase.

**Recovery** this is the lessons learned phase. You get to be a “Monday morning quarterback” and analyze what could have been done better. Use this info to update the Incident Response Plan.
The ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events
Value of Threat Intelligence

• Being reactive instead of proactive – if you understand your adversaries, you can develop tactics to combat current attacks and plan better for future threats.
• Driving better, more informed responses to security incidents.
• Enhancing communications between the security team, management and board members.
• Using a shared language
• Driving better investment strategies and more directly connecting security priorities with business risk management priorities.
Identify Internal Vulnerabilities & Prepare

- Know the current threat landscape
- Look at the entire picture – cyber, physical, and fraud
- Use the information to create Incident Response plans
- Test employees as if it were the real deal
Questions????

Max.Greene@tylertech.com