RANSOMWARE: WHAT YOU NEED TO KNOW NOW!

Tips and Best Practices to Avoid Being Held Hostage

Tom DeSot
Digital Defense, Inc. Chief Information Officer
Housekeeping

- Webinar will be recorded
- Attendees are in “Listen Only” mode
- Submit questions via the Questions Panel
- Live Q&A at the end of the presentation
AGENDA

1. My Background
2. Evolution of Ransomware
3. How the Bad Guys are Getting to the Goods
4. Best Practices to Mitigate Risks
5. Questions
As the Chief Information Officer of Digital Defense, Tom DeSot is charged with developing and maintaining relationships with key industry and market regulators; functioning as the “face of DDI” through public speaking initiatives, identifying key integration and service partnerships, and serving as the prime regulatory compliance resource for external and internal contacts. Tom also serves as the company’s internal auditor on security-related matters.
WHAT IS RANSOMWARE?

- Ransomware is a type of malicious software that carries out the cryptoviral extortion attack from cryptoviology that blocks access to data until a ransom is paid and displays a message requesting payment to unlock it.
- Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse.
- More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.
- The ransomware may also encrypt the computer's Master File Table or the entire hard drive. Thus, ransomware is a denial-of-access attack that prevents computer users from accessing files since it is intractable to decrypt the files without the decryption key.
“EVERY 40 SECONDS, A COMPANY GETS HIT WITH RANSOMWARE”

- Kaspersky Labs
Don’t Be Held Hostage

HOW THE BAD GUYS ARE GETTING TO THE GOODS?

Most ransomware attack vectors exploit human weaknesses and take advantage of poorly patched systems.

PHISHING
Fake emails designed to trick people.

VISHING
Spoofed phone numbers with messages that appear to be from legitimate sources.

SOCIAL MEDIA
Hosting images or active content that has ransomware downloaders embedded into it.

SYSTEM VULNERABILITIES
Network weaknesses that are exploited to break in and install ransomware.
TOP VULNERABILITIES EXPLOITED

Microsoft Vulnerabilities
MS17-010

FLASH FLAWS

MICROSOFT SILVERLIGHT
CVE-2016-0034
4 STEPS TO TAKE IF YOU BECOME A VICTIM

1. **Immediately Disconnect**
   Disconnect the infected system from the wired or wireless network that it is attached to. While not foolproof, this lessens the chance that the worm will have an opportunity to spread to other computers that reside on the same network that you do.

2. **Restore your Computer**
   Restore your computer(s) from a known good backup. It is strongly suggested that this not be a backup from the day of the infection as the machine(s) may become infected all over again.

3. **Update your Computer**
   Once the system is restored, update it! Make sure that you get the patch for the MS17-010 vulnerability. Also make sure that your antivirus software is up-to-date.

4. **Look for Others**
   Look for other systems on your network(s) that may need to be updated and patch those as well.
Don’t Be Held Hostage

BEST PRACTICES TO MITIGATE RISK

**PATCH YOUR SYSTEMS**
Ensure that the Microsoft patch for MS17-010 has been installed on your computer systems. This patches the attack vector used by malware.

**UPDATE YOUR ANTIVIRUS SOFTWARE**
Ensure that your antivirus has the latest signature set so that it can detect the malware.

**USER EDUCATION**
Users need to be educated about the risks associated with ransomware and understand what they can do to help the company avoid infections.

**BE CAREFUL WITH USB DRIVES**
Use caution when sharing USB drives with other users or USB drives from conferences and trade shows.

**DISABLE REMOTE DESKTOP PROTOCOL**
Many of the ransomware programs look for Remote Desktop Protocol (RDP) services to be running on a computer as a means of propagating the malware to other computers on the same network.

**BACK UP DATA**
Companies should complete full backups at least weekly and then do incremental / differential backups on a daily basis to ensure that any files that are created or modified on the system are backed up.
WHAT IF I DON’T HAVE A BACKUP?

If You Do Not Have a Backup You Have **Two Options:**

1. **Destroy the Drive Contents**
   Reformat the hard drive and re-install the operating system and applications. In this scenario, all information that is currently on the drive will be lost with no way of recovery.

2. **Pay the Ransom.**
   Follow the instructions on the FAQ provided by the malware to pay the ransom.
3 REASONS NOT TO PAY THE RANSOM

01 BITCOIN
Note that the payment will have to be made in BITCOIN, not regular currency.

02 ASSOCIATING WITH CRIMINALS
You will be forced to reach out to the ransomware authors for assistance in decrypting your files (it is unlikely you will get a response).

03 SUCCESS IS NOT GUARANTEED
There is a high likelihood that you will not be able to decrypt your files even after paying the ransom.
Don’t Be Held Hostage

PROACTIVE SECURITY SOLUTIONS TO MITIGATE AN ATTACK

Security Awareness Training

Consistent Vulnerability Scanning

Remote Social Engineering
Don’t Be Held Hostage

BE SURE TO ASK ABOUT…

Digital Defense, is offering to webinar participants special pricing on solutions to help defend against ransomware. To learn more contact us at www.DigitalDefense.com/ContactUs
HAVE QUESTIONS?

Tom DeSot

DigitalDefense.com

888.273.1312

Tom.DeSot@DigitalDefense.com