This product was created as part of a joint effort between the Financial Services – Information Sharing and Analysis Center (FS-ISAC), the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), the National Health – Information Sharing and Analysis Center (NH-ISAC) and the Multi-State Information Services and Sharing Center (MS-ISAC).

Ransomware 101 Workshop Recap

The following is a brief overview of ransomware based on a series of 16 *Ransomware 101 Workshops* held across the United States. Experts from the Financial Services – Information Sharing and Analysis Center (FS-ISAC), Federal Bureau of Investigation (FBI), United States Secret Service (USSS), National Health – Information Sharing and Analysis Center (NH-ISAC), Multi-State Information Services and Sharing Center (MS-ISAC), Palo Alto Networks and Symantec organized these roadshows which presented to more than 3,200 attendees.

The workshop presentations included details on ransomware; its many variants, how ransomware operates, mitigation for ransomware, use cases and scenarios/exercises were also covered. Also, an introduction to what ISACs (Information Sharing and Analysis Centers) are and an overview of what they offer was provided.

Attendees were asked key questions, such as:

- What are your initial steps? Who do you call?
- Who should be on your crisis management team?
- What are the options for recovery?
- Do you pay the ransom now?

Ransomware Overview

Ransomware is a malware posing an increasing threat to both the business sector and individuals. Ransomware encrypts files essentially blocking access to the file(s). Due to its effectiveness, ransomware is becoming the dominate form of modern crime ware. The only way to access the encrypted contents is via the decryption key and/or through data back-ups. Depending on the ransomware, specific files types may be encrypted. Ransom notes differ but essentially, they include a ransom amount, usually in bitcoin currency, a timeframe for which payment must be made, along with instructions on how to make the payment.

Ransomware Delivery

Different variants of ransomware may try to encrypt as many files as possible, however, many encrypt specific formats of files (MS Office Files, images). Ransomware can be delivered via many forms, such as exploit kits, spear phishing emails, malicious links and drive-by downloads. One example includes an email which appears to be from an upper-level manager asking for the recipient to do something with the attachment that appears legitimate, but may be infected with malicious code or include malicious links. The recipient clicks on a link that appears genuine and suddenly realizes that files may become encrypted and are unavailable. The actor, or perpetrator, then demands a ransom payment and gives the targets a way to regain their data. The ransom amount is generally not large, averaging less than $1,000 US, but the number of incidents has risen sharply in 2016, posting record growth in the first and second quarters.

© 2016 FS-ISAC, Inc. | All rights reserved. | TLP Green

The Ransom Payment

The FBI does not recommend paying the ransom. A payment of ransom does not guarantee that the actor will allow access or send decryption details. Some organizations that paid the ransom demands never received the decryption keys afterward. There are others that believe that the value of the data that may be potentially lost outweighs the comparably minimal cost of the ransom. These organizations will pay the ransom after evaluating all options, realizing that they have an inability to function. There is no guarantee, however, that these organizations will receive the decryption keys after payment.

Preparation Beats Mitigation

It is easier to prevent an infection or an attack than it is to clean one up. Best practice is to focus on defense and utilize several layers of security including:

- Operating systems and antivirus software should be kept up to date
- Employee education
- Files should be backed up and available to reload if necessary – backups should be stored in the cloud or on drives separate from the network
- Manage the use of privileged accounts – administrator level access should be minimized
- Have a plan and exercise it

Attack Mitigation

Being prepared is essential to reduce the effects of a ransomware attack. Here are tips on how to address ransomware post-attack:

- Isolate the infected system from your network.
- Restore files by using files from regularly maintained backups.
- Report the infection to the FBI. www.fbi.gov/contact-us/field
- Report home infections to the Internet Crime Complaint Center (IC3). www.ic3.gov
- Participate and share in an information sharing organization, such as your industry ISAC.

Recommendations

Be aware of how your network is configured and what software you use on a regular basis. By knowing what your system looks like and how it works, you will be able to identify problems when they occur. Here are some key recommended steps:

- Perform regular backups of all systems
- Know what is connected to and running on your network
- Use antivirus and anti-spam solutions
- Disable macro scripts in Office
- Restrict internet access
- Participate in cybersecurity information sharing organizations
- Create a solid business continuity plan

Conclusion

Ransomware infects computer systems throughout the world in ever increasing numbers. Outbreaks that use to be perpetrated by individuals are now being organized by criminal gangs. The future of ransomware seems to be bright and profitable. As it continues to spread through western countries, it will continue amassing money for its agents. Ransomware will continue to challenge authorities as it continues to mature, and distribution methods evolve. Law enforcement will need to double-down to continue to fight against this illegal money-raising scheme. As software developers continue working to fight the ransomware scam; hackers will be working to develop new and inventive ways to hook unsuspecting victims.

© 2016 FS-ISAC, Inc. | All rights reserved.