Slides from Presentation on Spoof Emails, and Ransomware

prepared by Gary Patrick

December 14, 2016 (amended 12/20/16)

Lexington Computer & Technology Group

Material about Spoof Email – slides #10 - 17
Material about Ransomware – slide #2 - 9
Methods to encrypt email content – slide #18
Sources of Information – slide #19

What is RansomWare?

Ransomware is a type of malware on a computer or server that encrypts the files, making them inaccessible to the owner until a specified ransom is paid.

Ransomware typically gets installed when a user clicks on a malicious link, opens a file in an e-mail that installs the malware, or suffers a drive-by download (which does not require user-initiation) from a compromised Web site.

The FBI does not support paying a ransom to the adversary.

- doing so does not guarantee the victim will regain access to their data;
- some individuals or organizations are never provided with decryption keys after paying a ransom.

Paying a ransom emboldens the adversary to target other victims for profit, and could provide incentive for other criminals to engage in similar illicit activities for financial gain.

New ransomware variants are emerging regularly.

Recent variants have targeted and compromised vulnerable business servers (rather than individual users) to identify and target hosts,

- thereby multiplying the number of potential infected servers and devices on a network.
- some are also charging ransoms based on the number of hosts (or servers) infected.
- some recent victims have not been provided the decryption keys for all their files after paying the ransom, and
- some have been extorted for even more money after payment.

This evolution illustrates it is more profitable for the perpetrators to target small businesses rather than individuals.

The FBI is urging ransomware victims to report incidents regardless of the outcome. Victim reporting provides law enforcement with a greater understanding of the threat, provides justification for ransomware investigations, and contributes relevant information to prosecute ongoing ransomware cases. Knowing more about victims and their experiences with ransomware will help the FBI to determine who is behind the attacks and how they are identifying or targeting victims.

If you are a victim of ransomware, either -

- reach out to your local FBI office and/or
- file a complaint with the Internet Crime Complaint Center, at www.IC3.gov, with the ransomware infection details (as listed on the next slide):

What to Report to Law Enforcement: (list from FBI)

- Date of Infection
- Ransomware Variant (identified on the ransom page or by the encrypted file extension)
- Victim Company Information (industry type, business size, etc.)
- How the Infection Occurred (link in e-mail, browsing the Internet, etc.)
- Requested Ransom Amount
- Actor’s Bitcoin Wallet Address (may be listed on the ransom page)
- Ransom Amount Paid (if any)
- Overall Losses Associated with a Ransomware Infection (including the ransom amount)
- Victim Impact Statement.

Defenses against Ransomware (as summarized and recommended by the FBI):

- Regularly back up data and verify the integrity of those backups. Backups are critical in ransomware incidents; if you are infected, backups may be the best way to recover your critical data.
  (The FBI recommends against paying the ransom demanded)
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might include securing backups in the cloud or physically storing them offline. It should be noted, some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real-time, also known as persistent synchronization.

- Scrutinize links contained in e-mails you receive.
  do not open attachments included in unsolicited e-mails.
- Download software only from sites you know and trust. – especially if free software.

  When possible, verify the integrity of the software through a digital signature prior to execution.
- Ensure application patches for the operating system, software, and firmware are up to date, including Adobe Flash, Java, Web browsers, etc.
- Ensure anti-virus and anti-malware solutions are set to update automatically, and regular scans are conducted.
- Disable macro scripts from files transmitted via e-mail.

- Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office Suite applications.
- Implement software restrictions or other controls to prevent the execution of programs in common ransomware locations, such as:
  - temporary folders supporting popular Internet browsers, or
  - compression/decompression programs, including those located in the AppData/LocalAppData folder.

(Further measures are recommended for computers and servers in business settings)

Reference, FBI site:
https://www.ic3.gov/media/2016/160915.aspx

Places you can send a suspicious file or email to be checked out:

upload any suspect email attachment to:

www.virustotal.com, (free analysis of suspicious files or URLs), or

www.reverse.it. (free, malware analysis service).

Send spam to spam@knujon.net - they collect spam and go after the spammer to try to shut them down.

(knujon is "no junk" spelled backwards). based in Boston. or just forward spam to KNUJON@COLDRAIN.NET.

Spoof Email – What is It?

The term refers to an email where the sender is pretending to be someone else, identifying himself by using someone else's email address, not his own, as the sender.

(Use of some email diagnostic tools, however, can usually reveal the true source - to a internet domain address, at least).

The sender's motive for this deception may be to send spam (and keep the source unknown), but increasingly it is used to snare the recipient into a scam or action that enables malware, or spreads malware further.

A spoof email may contain a malicious file, or a link to a malicious website, hence the attempt at deceiving the recipient.

Spoof email comes in three flavors:

1) You receive an email from someone who knows your email address (or a business that knows your email address), but it's not really from this person or business.

A corollary is that someone on your contact list receives an email from you that is spurious; (is case #1 flipped end-for-end).

(sometimes the Subject field will tip you off it's not genuine, such as “Hey, look at this.”)

2) You receive an email sourced with your own email address as the sender! Whoa! I didn't send that!

3) You receive one or more alerts from an email server administrator (often called the “mailer-daemon” or “postmaster”) saying an email you sent could not be delivered because the email system could not find the recipient's email address, for an email you never composed.

(these non-delivery alerts are a hint the sender may have been shotgunning a large and probably outdated email contact list).

Someone else is using my email address to send email or spam! How does this happen?

1) because web email providers allow one to use an “alias” to send email, it's easy for any email user to pick an alternate identity.

2) there’s nothing in email protocol that requires or checks that what appears on the From: line of a message actually has anything to do with the message’s true origin.

3) the source of the spoof email is very likely an automated process by either:

- a botnet (rogue program on some server on the internet), or
- a virus that has infected someone's computer where your email address can be picked up, likely from an internal contacts list.

4) botnets can gather lengthy lists of lists of email addresses from other botnets, or from lists of addresses for sale:

- some companies may sell a list of the email addresses of their customers (check the privacy policies of sites you use)
- some companies have been hacked, and lists of email addresses (and worse, passwords) have been stolen.
- the contact list from a friend's email account may have been stolen or has spread to less controlled recipients.

For a more in-depth explanation, with a touch of humor, refer to these “Ask Leo” web pages:

- https://askleo.com/someones-sendin/
- https://askleo.com/why_am_i_getting_spam_from_myself/

It's actually less likely that your own email account has been “hacked,” but it does happen.

Evidence your email account has been breached:

1) you find messages in your “sent” folder that you did not send, an indication your email account is the actual source.

2) you are unable to log in to your email account (someone has changed your password).
You may have to contact your email provider and/or use secret question answers to get access.

Recommended action, responding to (1) or (2),
as soon as you can get access to your email account:
change your password.

Smart moves to defend your email account:

- A long, complex password.
- Don't leave yourself logged in to your email account if there's some risk your computer might be stolen, or someone might gain unauthorized access to operate your computer for a time.

  (Remember that Windows Account passwords are easily bypassed by a tech-savvy person)
- Don't use your email address as your user name on web forums or the like (although many online accounts don't give you a choice).
- Set up a second email address (an alias, and maybe even more than one alias), and

  use that alias for the more public exposures of “your” email address, where you are asked or required to supply a “return” email address (such as for online purchase receipts).

Defensive moves, continued:

- set up devious answers to security questions, especially If one avenue to changing your password is simply to answer one or more security questions. (Brian Krebs suggests gibberish or a totally unrelated answer to security questions).
- It takes only one chain email to harvest thousands of related email addresses; never reply to chain letters.
- when you need to email to a distribution list, use :bcc to isolate all those contacts from one another – i.e. doing the recipients a privacy favor.

What can you do to stop Spoof Emails?

Answer:

- unfortunately, not much;
- flag it as “spam” (“junk”) by whatever filtering capability your email provider gives you.

If spoof email becomes a severe problem, contact your email service provider.

examples:

for Google gmail,

https://support.google.com/mail/answer/50270?hl=en

for Microsoft Outlook,

https://support.office.com/en-gb/article/Get-help-with-Outlook-com-40676AD0-C831-45AC-A023-5BE633BE798D?ui=en-US&rs=en-GB&ad=GB

How to add message-encryption to your email - examples of two services:

1) ProtonMail: An encrypted-email service provided by Proton Technologies, A.G. that has its own servers in Switzerland. about: https://en.wikipedia.org/wiki/ProtonMail. basic service free, 1 million users. Can send plain-text or encrypted email. Non-subscriber recipients can still receive encrypted email from you by a password arrangement, using a separate web interface. www.protomail.com

2) GnuPG: You need to use Thunderbird (for Windows) with web based email, and install an add-on that implements GnuPG as the encryption/decryption tool. Further, you set up public and private keys that work as a pair to give you access to encryption/decryption. The recipient(s) for your emails need to do the same.

References – Spoof email and Spam:

- Windows Secrets Newletter Users' Forum, June 13, 2013 and ongoing comments:

http://windowssecrets.com/forums/showthread.php/178403-Is-having-my-email-address-spoofed-a-problem?highlight=spoof+email

and:

http://windowssecrets.com/forums/showthread.php/154855-Follow-on-to-hacked-email-thread?highlight=spoof+email

References – Articles about Ransomware:

- U.S. FBI bulletin: https://www.ic3.gov/media/2016/160915.aspx;
- KrebsOnSecurity: https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/