LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Malspam

09/17/2020

Report #: 202009171030

Agenda

- Background
- Types of Malspam
- Threat to HPH Sector
- Detection
- Mitigation Strategies

Slides Key:

👤	Non-Technical: Managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Background

- **Spam:**
  - Generally defined as “unsolicited bulk email”
  - Name comes from a Monty Python comedy sketch referencing the canned meat “SPAM”
  - First spam email sent on May 1st, 1978 to several hundred people on ARPANET
  - The CAN_SPAM Act of 2003 attempted to address unsolicited email
- **Malspam (malicious spam):**
  - Spam sent with malicious intent

Image Source: Monty Python’s Flying Circus

Image Source: Hormel Foods

Types of Malspam

- Droppers
- Phishing
- Spear Phishing
- Whaling
- Business Email Compromise

We need to verify your credit card number.
Don't take the bait. Protect your financial information.

Types of Malspam – Droppers

- Droppers are initial malware delivered by spam messages that install, or “drop”, additional malware such as keyloggers or ransomware

- Malspam messages may have droppers as attachments, or may contain links to websites hosting the droppers

- Example (Emotet):
  (See https://us-cert.cisa.gov/ncas/alerts/TA18-201A)
  - Emails claiming to be invoices or receipts
  - Contains a malicious download link, a PDF file, or a macro-enabled Microsoft Word document
  - Once a user is infected with Emotet, it can remain persistent across reboots and spread on the internal network

Types of Malspam – Phishing

From FTC website:
(https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/phishing-scams)

Phishing is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source – an internet service provider, a bank, or a mortgage company, for example. It asks the consumer to provide personally identifying information. Then a scammer uses that information to open new accounts, or invade the consumer’s existing accounts.

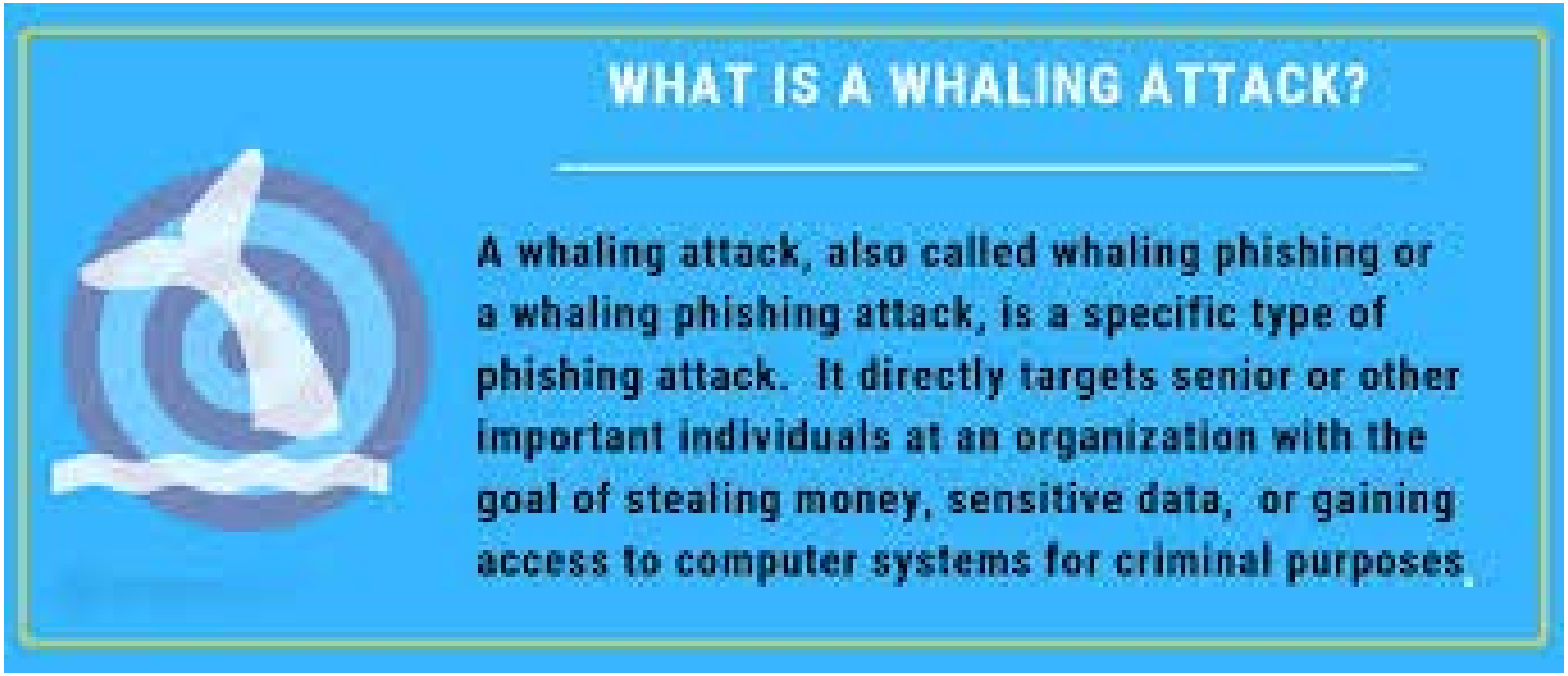
Types of Malspam – Spear Phishing & Whaling

- **Spear Phishing:**

  Sending phishing emails to a small, targeted group of recipients

- **Whaling:**

  Spear phishing that targets executives / upper management

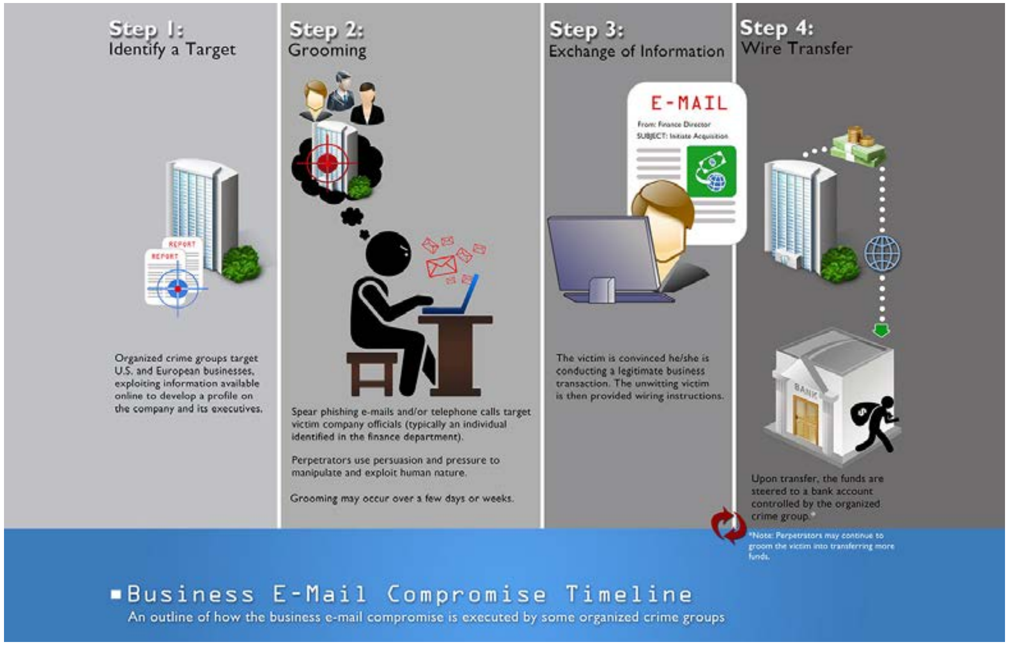


WHAT IS A WHALING ATTACK?

A whaling attack, also called whaling phishing or a whaling phishing attack, is a specific type of phishing attack. It directly targets senior or other important individuals at an organization with the goal of stealing money, sensitive data, or gaining access to computer systems for criminal purposes.

Types of Malspam – Business Email Compromise

- Targeted emails sent from spoofed or actually compromised organizations or individuals
- The recipient is familiar with the apparent sender
- The sender makes a seemingly legitimate request



Step 1: Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2: Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups

https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

Threats to HPH Sector

- Healthcare recipients were the most targeted sector for credential theft in the first half of 2020
- Ransomware attacks against healthcare increased 350% during Q4 2019, the majority of which were a result of phishing

Detection (Definitions)

- **SMTP (Simple Mail Transfer Protocol)**
  - The Internet protocol used to send email
  - *How email is sent*
  - Analogy: Postal carriers and the envelopes they carry
- **IMF (Internet Message Format)**
  - The syntax for email messages
  - *The actual message which is sent*
  - Analogy: A letter inside of an envelope

Detection (Definitions)

- **DKIM (Domain Keys Identified Mail)**
  - Email authentication that uses a digital signature
  - The sending organization can sign emails
  - Receiving organizations can verify the signature
- **SPF (Sender Policy Framework)**
  - Specifies valid SMTP servers for the sender’s domain
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**
  - Extends SPF and DKIM
  - Allows admins of sender domains to specify:
    - Which SPF and DKIM policies to use
    - How recipients can check the “From:” field in the message
    - How to handle failures
    - How to report actions performed under the policies

Detection (Example)

SMTP Mail Envelope	**HELO mail.evil_sender.local MAIL FROM: <malory.doe@evil_sender.local> RCPT TO: <victor.smith@victim.local> DATA**
IMF Headers	**Received: from mail.evil_sender.local ([192.168.0.1]) by mail.victim.local; Wed, 9 Sep 2020 17:02:15 +0000 Content-Transfer-Encoding: binary From: "Malory Doe" <malory.doe@good_sender.local> Reply-To: <malory.doe@evil_sender.local> To: "Victor Smith" <victor.smith@victim.local> Subject: Overdue Invoice Date: Wed, 9 Sep 2020 17:02:05 +0000 Message-ID: erwitufgj-4875205-8D9ds@evil_sender.local**
IMF Body	**Please reply to me with your credit card number and expiration date.**
SMTP Commands	**QUIT**

Detection (Example)

SMTP Mail Envelope	**HELO mail.evil_sender.local MAIL FROM: <malory.doe@evil_sender.local> RCPT TO: <victor.smith@victim.local> DATA**
IMF Headers	**Received: from mail.evil_sender.local ([192.168.0.1]) by mail.victim.local; Wed, 9 Sep 2020 17:02:15 +0000 Content-Transfer-Encoding: binary From: "Malory Doe" <malory.doe@good_sender.local> Reply-To: <malory.doe@evil_sender.local> To: "Victor Smith" <victor.smith@victim.local> Subject: Overdue Invoice Date: Wed, 9 Sep 2020 17:02:05 +0000 Message-ID: erwitufgj-4875205-8D9ds@evil_sender.local**
IMF Body	**Please reply to me with your credit card number and expiration date.**
SMTP Commands	**QUIT**

Should we accept email from evil_sender.local?

The IMF “From” address does not match the envelope sender address

The “Reply To” address looks suspicious

There is no DKIM signature

Is evil_sender supposed to send email for good_sender? (SPF)

Am I expecting an overdue invoice?

Mitigation Strategies

- Keyword Filtering
- Email Blacklists
- Spam Scoring
- DKIM/SPF/DMARC
- User Education

Mitigation Strategies – Keyword Filtering

- Emails can be inspected for certain strings in the subject or body
- Example: Filter all emails for “parcel deliveries failure” in the subject
- Caveats:
  - Attackers can easily change their email wording to evade the filters
  - Attackers can use different character sets with similar-looking characters
  - Be careful to not filter strings used in legitimate emails

Mitigation Strategies – Email Blacklists

- Bad sender email domains or bad sender email addresses can be used for filtering
- Blacklists can be developed internally or obtained via threat feeds
- Caveats:
  - Attackers could spoof legitimate domains
  - Attackers could compromise accounts at legitimate organizations
  - Attackers can easily change sender accounts or domains, particularly via spoofing

Mitigation Strategies – Spam Scoring

- Multiple factors are taken into account to develop a score as to the likelihood of an email being spam
- Algorithms differ by vendor and configuration
- Emails can be delivered, quarantined, or rejected based on a score threshold

Mitigation Strategies – DKIM / SPF / DMARC

- **DKIM:**

  Handle email differently if it is signed, not signed, or the signature does not match

- **SPF:**

  Handle email differently if the sending mail server is not authorized for the sender domain

- **DMARC:**

  Provides the legitimate domain of the sender granular control of authenticating email, helping to mitigate spoofing

Mitigation Strategies – User Education

- The recipient is the last line of defense
- Users need to get in a security mindset, and be aware that emails can be spoofed and email accounts can be compromised
- Organizations may implement ethical phishing campaigns to provide a realistically simulated phishing attack in order to educate users

Reference Materials

References

Background:

- https://www.wsj.com/articles/SB121003279234369267
- https://www.govinfo.gov/content/pkg/PLAW-108publ187/html/PLAW-108publ187.htm

Threats to HPH Sector:

- https://healthitsecurity.com/news/ransomware-attacks-on-healthcare-providers-rose-350-in-q4-2019
- https://healthitsecurity.com/news/credential-theft-via-spoofed-login-pages-increase-healthcare-top-target

Detection (Definitions):

- https://tools.ietf.org/html/rfc5321
- https://tools.ietf.org/html/rfc5322
- https://tools.ietf.org/html/rfc6376
- https://tools.ietf.org/html/rfc7208
- https://tools.ietf.org/html/rfc7489

Questions

Questions

Upcoming Briefs

- Netwalker Ransomware – 9/24

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday–Friday, between 9am–5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday–Friday, between 9am–5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV