LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Business Email Compromise in the Health Sector

July 9, 2020

Report #: 202007091030

Agenda

- Executive Summary
- BEC and Cybercrime Ecosystem
- BEC Statistics
- Evolution of Targets
- BEC Interdependencies in Cybercrime
- BEC Attack Phases
- BEC TTPs and Case Studies
- Recommendations and Mitigations

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Business Email Compromise

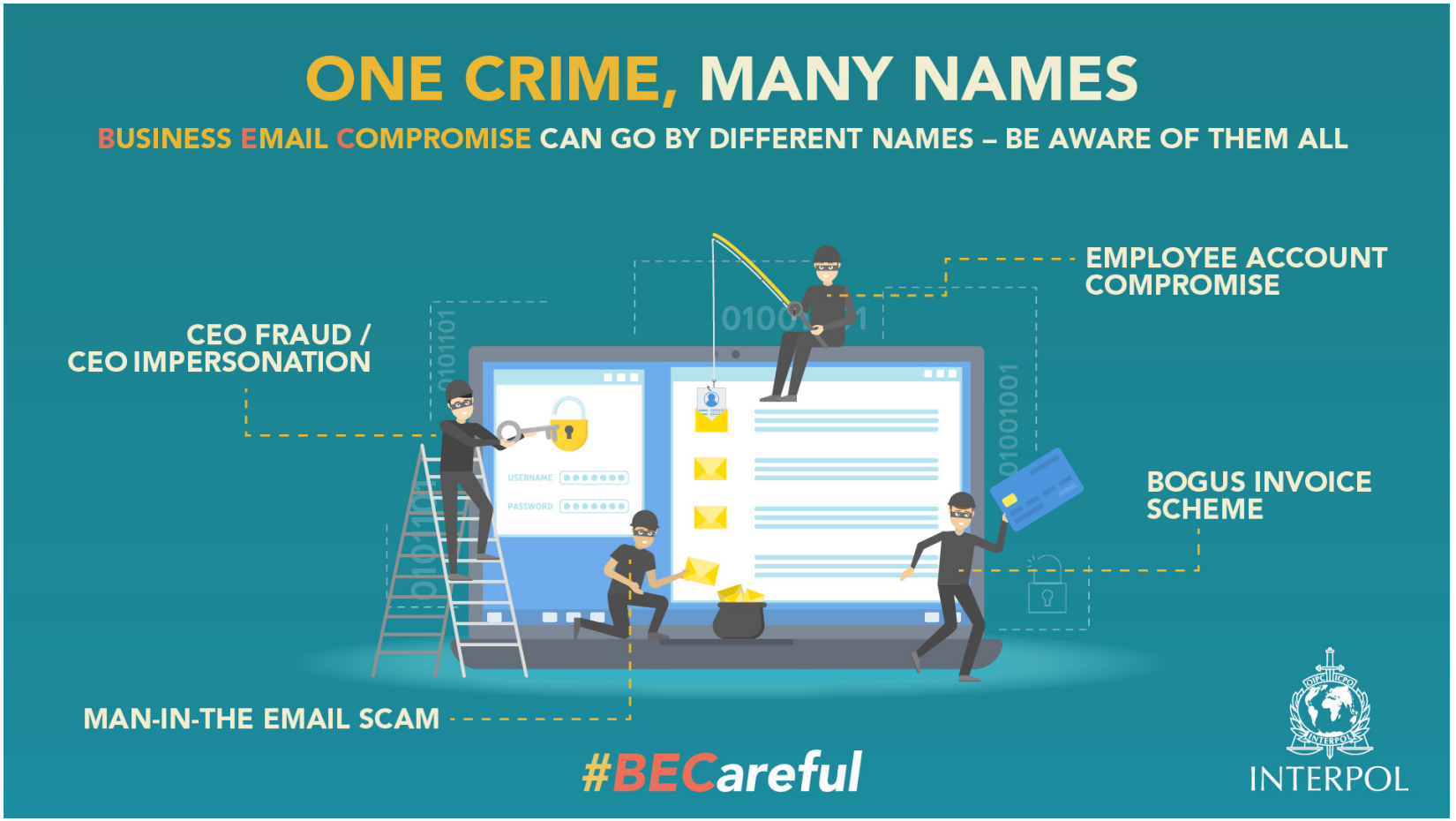
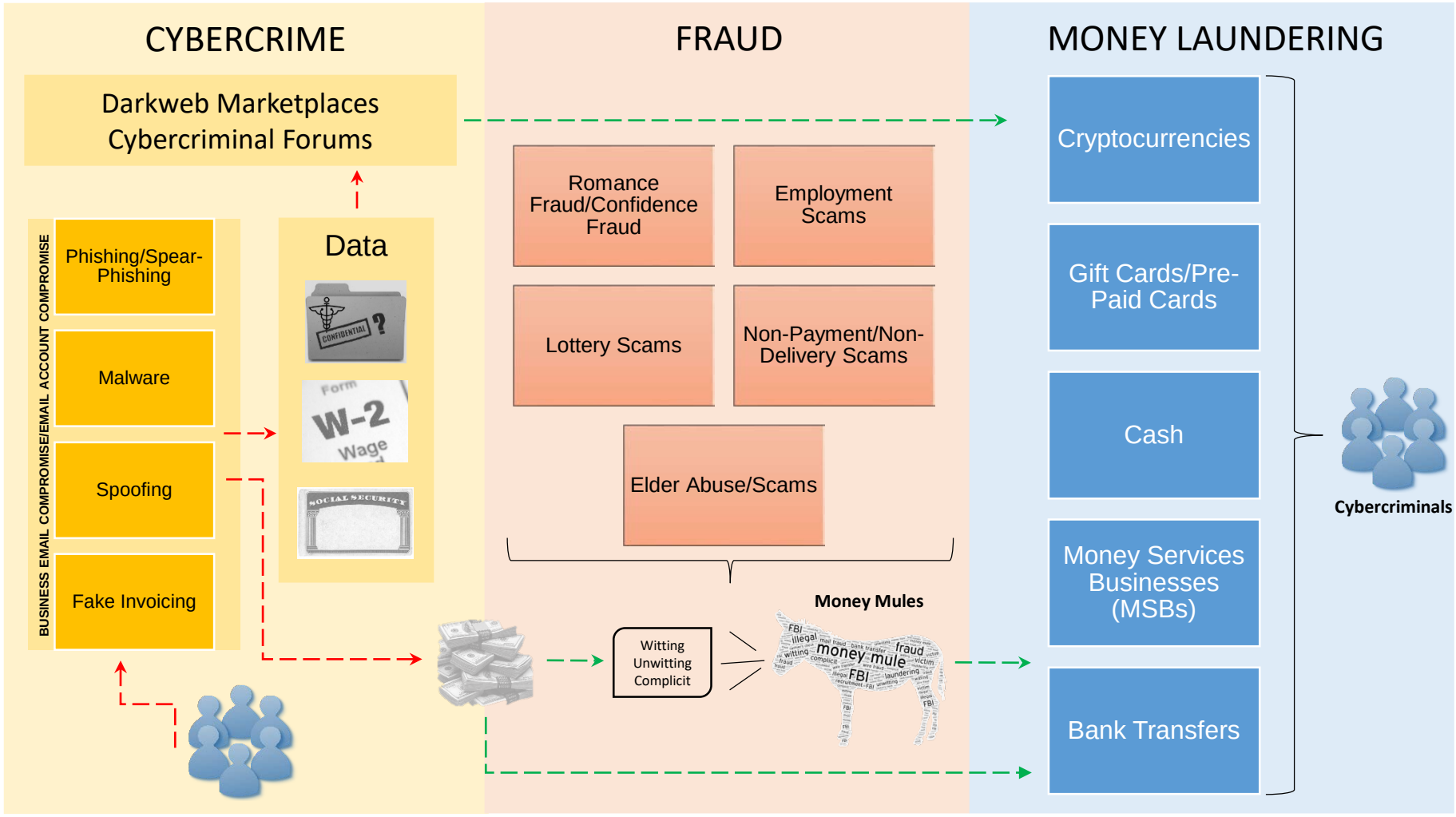


Image source: Interpol

BEC and Cybercrime Ecosystem

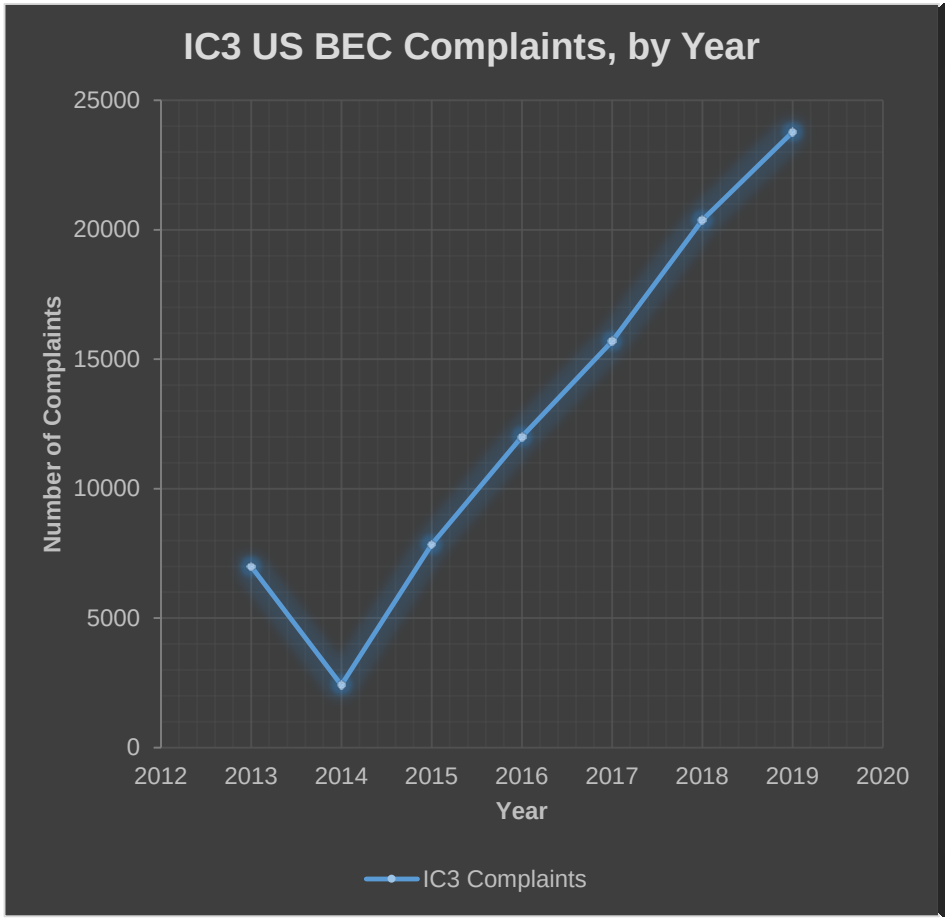


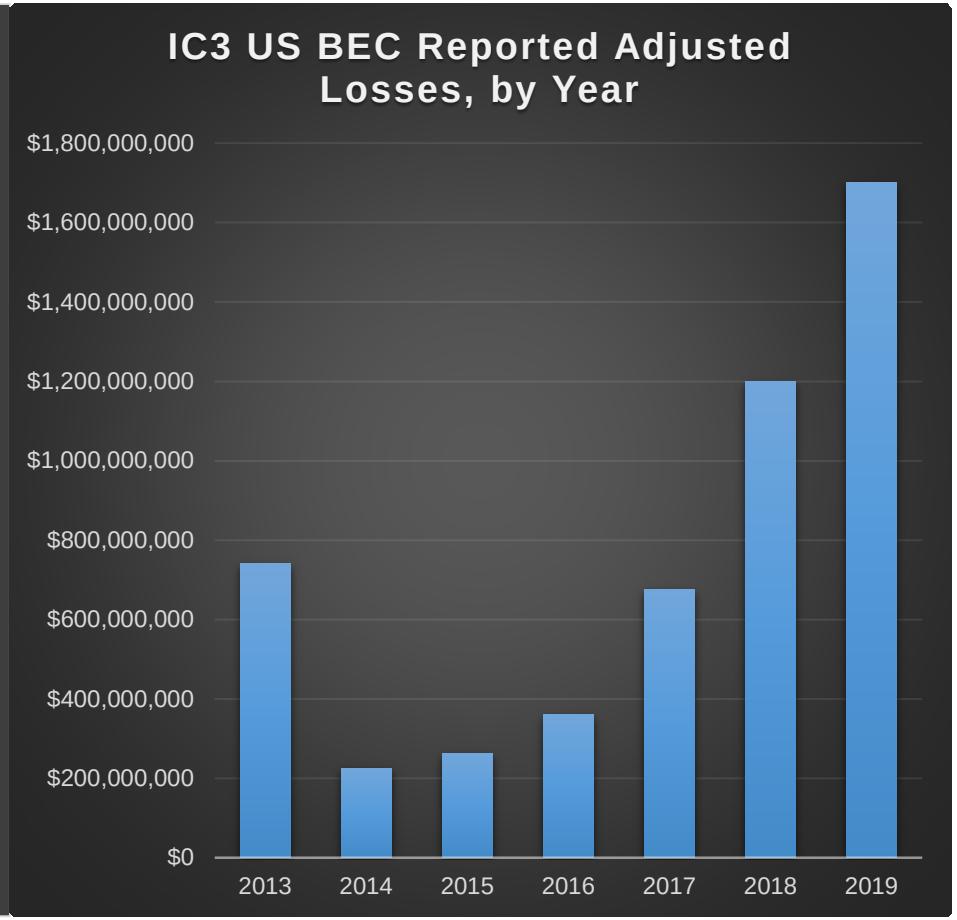
(CISA, 2009) (IC3, 2019)

Images Sources:
Creative Commons & FBI

BEC Statistics

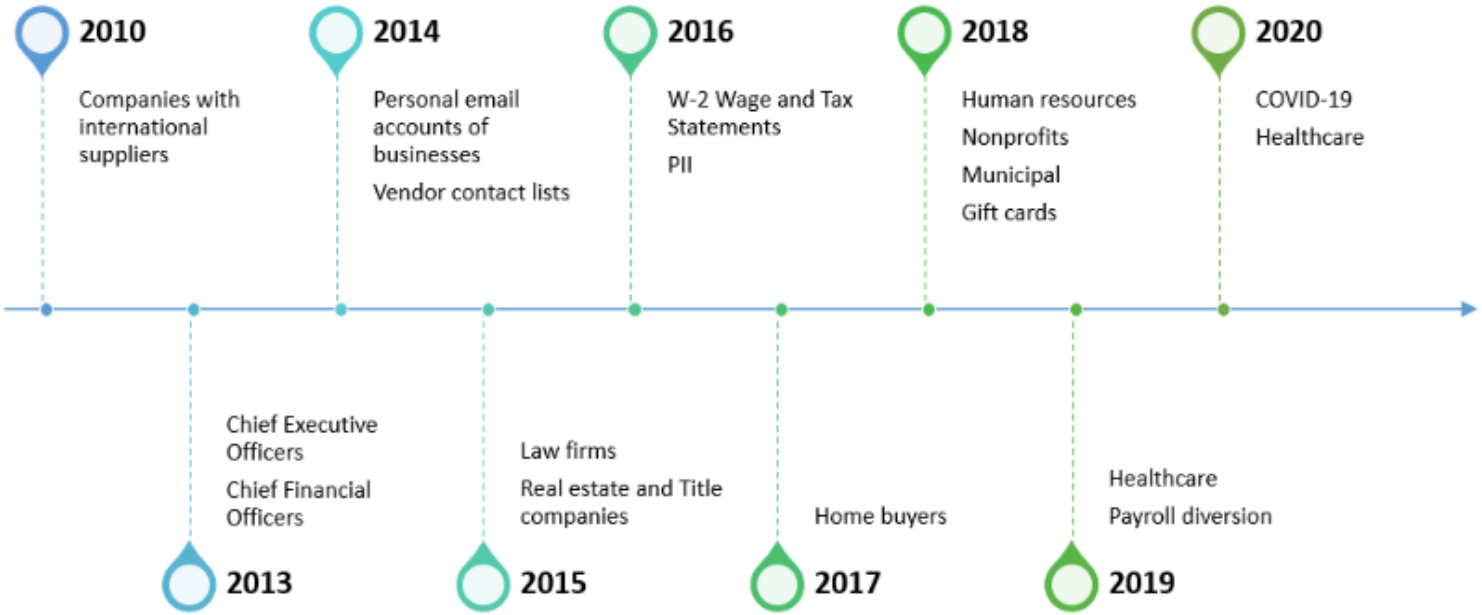
From 2016 to 2019, FBI's Internet Crime Complaint Center (IC3) reports BEC is responsible for **$26 Billion** in losses domestically and internationally.





(IC3, n.d.) (FBI, 2019)

Evolution of BEC Targets



Targeting trends evolved from companies used to sending large international wires to entities that handle money-in-motion (legal, real estate, title) and those with data rich environments (healthcare, human resources, payroll)

(IC3, n.d.)

BEC Attack Phases

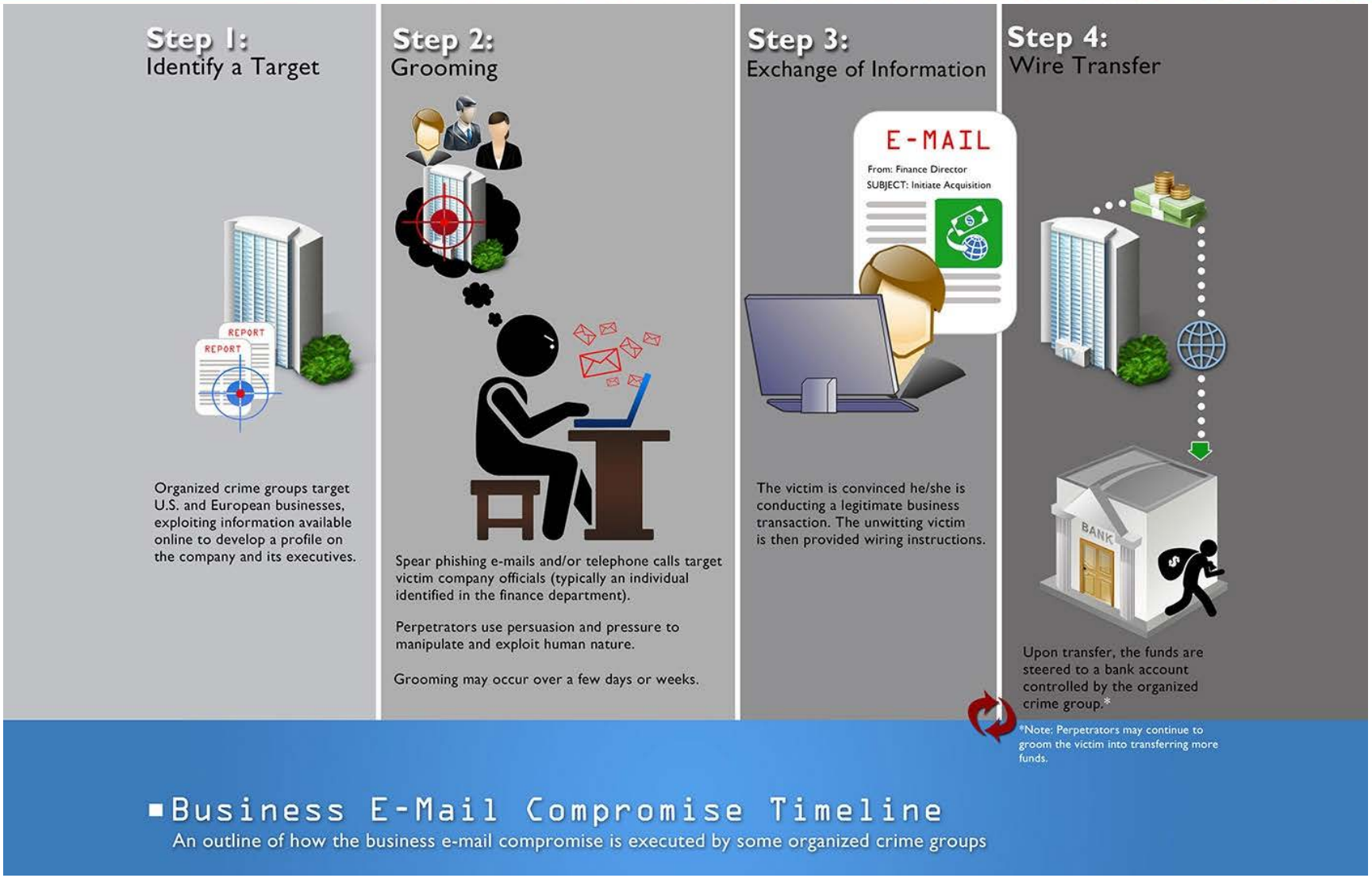


Image Source: FBI

BEC Attack Phases

What are some common indicators of phishing attempts?

Suspicious email address of sender	• Email address of sender(s) can mimic legitimate businesses. Threat actors often leverage email addresses that resemble reputable organizations, but alter or omit a few letters and numbers.
Generic greetings and signatures	• Lack of contact information in an email signature block, or generic greetings such as “Sir/Ma’am” or “Dear Valued Customer” are strong indicators of a phishing email.
Misspelling and layout	• Odd sentence structure, misspellings, poor grammar, and inconsistent formatting are strong indicators of a potential phishing attempt.
Spoofed websites and hyperlinks	• When hovering a cursor over links in body of an email, if links do not match, the link may be spoofed. Malicious variations from legitimate domains leverage different spellings or domains such as .net, vs .com. Other tactics include usage of URL shortening services to conceal the true destination of links.
Suspicious attachments	• Unsolicited emails which request users to open or download attachments are common delivery mechanisms for malware.

(CISA, 2009)

BEC TTPs and Case Studies – Spoofing

TTPs – Email

- Email accounts of businesses are targeted by threat actors
- The spoofed emails can be made to look like they are coming from anyone

TTPs - Target

- Target employees with transactional authority (accounts payable, check signers, authorized individuals) or access to systems managing PII/W-2 data.
- Emails often display a sense of urgency culminating in a request for money transfers, data, or gift cards.

CASE STUDY- Nursing Home & Rehabilitation Facility

- In December 2019, a nursing home and rehabilitation firm in New York fell victim to a BEC attack.
- An employee received an email request for data that was spoofed to appear as if from a legitimate source, posing as a senior staff member requesting PII and patient data.
- Employee sent 600 patient records to an email controlled by the attacker. Possible value of approximately $300,000 to over $600,000.

(Panda Security, 2020) (FBI, 2017)

BEC TTPs and Case Studies – Fake Invoicing

TTPs - Email

- Emails sent to employees with transactional authority (accounts payable, check signers, authorized individuals)
- Threat actors may also send a link to what appears to be an invoice. Link may transmit sensitive information to the attackers or download malware.

TTPs - Target

- Threat actors target businesses with established relationships with a vendor or supplier
- Leveraging fake invoices, threat actors request payment through social engineering to a financial account under their control.

CASE STUDY – State Government and Health Care Providers

- State government and healthcare providers in the U.S. aiming to procure personal protective equipment (PPE) and other supplies during the COVID-19 pandemic were duped into sending funds to accounts controlled by foreign and domestic threat actors
- A threat actor claimed to represent an entity with which the purchasing department had an existing relationship with. A wire transfer was completed and funds transferred outside the U.S.

(Panda Security, 2020) (FBI, 2017)

BEC TTPs and Case Studies – Malware

TTPs

- Email accounts of businesses are targeted by threat actors who use malware to obtain sensitive information
- Malware is often utilized to infiltrate networks in order to gain access to internal data and systems
- This data is then used to avoid raising suspicions when a falsified wire transfer is submitted

CASE STUDY – SilverTerrier and Covid-19

- 3 SilverTerrier groups launched ten COVID-19-themed malware campaigns over Q1 2020 with over 170 phishing emails.
- Targets were healthcare agencies, local and regional governments, universities with medical programs and centers, medical publishing firms, and insurance companies across the U.S.
- None of the observed SilverTerrier malware Covid-19 themed attacks have been successful

(Panda Security, 2020) (FBI, 2017)

BEC TTPs and Case Studies – Phishing

TTPs - Email

- Phishing emails often appear as if sent from a legitimate organization or known individual.
- Emails attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate or click on malicious attachments.

TTPs - Target

- An attempt by attackers to solicit personal information from unsuspecting users through social engineering techniques.
- Users may be asked to provide personal information, such as account usernames and passwords, these fraudulent websites may contain malicious code.

CASE STUDY – Substance Abuse Treatment Center

- In February 2020, a substance abuse treatment center in Ohio was victim of a BEC phishing attack
- An employee clicked on a phishing lure, which was designed to facilitate a request for a wire transfer to an international bank account under the attacker's control.
- While the wire transfer was successfully requested, it was detected as fraudulent and subsequently blocked, and no funds left the treatment center's account.

(Panda Security, 2020) (FBI, 2017)

BEC Success Story

- A pharmacy avoided a $500,000 BEC attack by simply comparing the address on an email and the address in their records.
- The pharmacy received a large order, purportedly from a large medical center for an order of $500, 000 in prescription drugs.
- All the paperwork was in order and looked authentic except that the address was different than the address the pharmacy had on file.
- An employee called the Medical Center to verify the address change and the Medical Center alerted the pharmacy that it had not placed the order.

(FBI, 2017)

Recommendations and Mitigations

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are examples from HICP that can be used to mitigate some common threats.

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
Provide social engineering and phishing training to employees.	[10.S.A], [1.M.D]
Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported.	[10.S.A], [10.M.A]
Ensure emails originating from outside the organization are automatically marked before received.	[1.S.A], [1.M.A]
Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.	[7.S.A], [7.M.D]
Implement Intrusion Detection System (IDS); Keep signatures and rules updated.	[6.S.C], [6.M.C], [6.L.C]
Implement spam filters at the email gateways; Keep signatures and rules updated.	[1.S.A], [1.M.A]
Block suspicious IP addresses at the firewall; Keep firewall rules are updated.	[6.S.A], [6.M.A], [6.L.E]
Implement whitelisting technology to ensure that only authorized software is allowed to execute.	[2.S.A], [2.M.A], [2.L.E]
Implement access control based on the principal of least privilege.	[3.S.A], [3.M.A], [3.L.C]
Implement and maintain anti-malware solution.	[2.S.A], [2.M.A], [2.L.D]
Conduct system hardening to ensure proper configurations.	[7.S.A], [7.M.D]
Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2.	[7.S.A], [7.M.D]

(HHS, 2018)

Non-Technical Recommendations and Mitigations

Training and Awareness

- Alerts for employees and customers regarding phishing scams targeting specific organizations or interest groups
- Reminders of policies in place such as account changes
- General information on phishing tactics posted to organization web site or emails

Establish out-of-band communication.

- Use an alternate form of communication than email, such as a telephone call, to verify transactions over a particular dollar amount. And set up this verification process early in the business relationship. Do not use email to set up the verification process.

Confirm significant or out-of-pattern changes.

- Beware of sudden changes in business practices. For example, if a vendor suddenly asks to be contacted at a personal email address when all previous official correspondence has been on a company email, verify via other channels that you are still communicating with your legitimate business partner.

Email forwarding vs email reply

- Instead of hitting reply on important emails, use the forward option and either type in the correct email address or select it from your email address book to ensure you're using the real email address.

(FBI, n.d.)

Technical Recommendations and Mitigations

Email Banners/Flags.	• This is a simple way highlight that extra scrutiny is needed for external emails. It can also identify when an adversary creates a fraudulent domain that looks similar to an HPH legitimate domain.
Domain-based Message Authentication Reporting and Conformance (DMARC).	• The DMARC protocol enables domain owners to specify which authentication method is used when sending emails. DMARC helps email receivers determine if the purported message "aligns" with what the receiver knows about the sender. If not, guidance is provided on how to handle the message. Learn more at DMARC.org.
Two-Factor Authentication	• Something you know (password or PIN) and something you have (token). TFA/MFA aims to protect users if authentication credentials have been captured. The nature of changing token limits attackers ability to leverage captured credentials. 99.9% effective
Passwords	• Review password policies to ensure they align with the latest NIST guidelines, and deter the use of easy-to-guess passwords. • Review IT helpdesk password management related to initial passwords, password resets for user lockouts, and shared accounts. IT helpdesk password procedures may not align to company policy, creating an exploitable security gap. • Regularly audit user passwords against common password lists, using free or commercial tools. • Provide pragmatic advice to users on how to choose good passwords.
Data Mining	• Data mining abuse box/phishing reporting and using the intelligence gained to prevent future attacks.

(Milletary, J., n.d.) (CISA, 2020) (NCSC, 2018) (CISA, 2018) (Maynes, 2019)

Conclusion

- BEC and Cybercrime Ecosystem
- BEC Statistics
- Evolution of Targets
- BEC Interdependencies in Cybercrime
- BEC Attack Phases
- BEC TTPs and Case Studies
- Recommendations and Mitigations

Image Source: FBI

Reference Materials

References

- CISA. (March 27, 2018). Alert (TA18-086A) Brute Force Attacks Conducted by Cyber Actors. Accessed May 13, 2020 at: https://www.us-cert.gov/ncas/alerts/TA18-086A
- CISA. (May 5, 2020). APT Groups Target Healthcare and Essential Services. Accessed May 13, 2020 at: https://www.us-cert.gov/ncas/alerts/AA20126A
- CISA. (October 22, 2009). Avoiding Social Engineering and Phishing Attacks. Accessed June 22, 2020 at: https://www.us-cert.gov/ncas/tips/ST04-014
- FBI. (April 13, 2020). FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic. Accessed June 22, 2020 at: https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic
- FBI. (February 27, 2017). Business E-mail Compromise: Cyber Enabled Financial Fraud on the Rise Globally. Accessed June 22, 2020 at: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise
- FBI. (n.d.) Protected Voices: Business Email Compromise. Accessed June 22, 2020 at: https://www.fbi.gov/video-repository/protected-voices-business-email-compromise-102319.mp4/view
- FBI. (September 10, 2019. Alert I-091019-PSA Business Email Compromise the $26 Billion Scam. Accessed June 22, 2020 at: https://www.ic3.gov/media/2019/190910.aspx
- HHS. (December 28, 2018). Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Accessed June 4, 2020 at: https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

References

- IC3. (December 4,2019). Alert I-120419 Money Mules: What is a Money Mule? Accessed June 22, 2020 at: https://www.ic3.gov/media/2019/191204.aspx
- IC3. (n.d.) Internet Crime Complaint Center Annual Reports. Accessed June 22, 2020 at: https://www.ic3.gov/media/annualreports.aspx
- Maynes, M. (August 20, 2019). One simple action you can take to prevent 99.9 percent of attacks on your accounts. Microsoft.com. Accessed July 2, 2020 at: https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/
- Milletary, J. (n.d.). Technical Trends in Phishing Attacks. US-CERT. Accessed June 29, 2020 at: https://www.us-cert.gov/sites/default/files/publications/phishing_trends0511.pdf
- NCSC. (May 15, 2018). Spray you, spray me: defending against password spraying attacks. Accessed May 13, 2020 at: https://www.ncsc.gov.uk/blog-post/spray-you-spray-me-defending-against-password-spraying-attacks.
- Panda Security. (February 17, 2020). A BEC Scam Leads to a Healthcare Breach. Accessed June 22, 2020 at: https://www.pandasecurity.com/mediacenter/news/bec-scam-medical-center/
- Renals, P. (May 7, 2020). SilverTerrier: New COVID-19 Themed Business Email Compromise Schemes. Accessed June 22, 2020 at: https://unit42.paloaltonetworks.com/silverterrier-covid-19-themed-business-email-compromise/

Questions

Future briefings:

- DDoS Attacks (7/16)
- Cybercrime and the Healthcare Industry (7/30)

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.**

Health Sector Cybersecurity Coordination Center (HC3) Background

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 document and 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