Business Email Compromise

Business Email Compromise (BEC) has surpassed ransomware and currently tops the list of cyber threats in terms of financial loss and victims as per Federal Bureau of Investigation (FBI) and American International Group (AIG). BEC targets individuals and businesses who are authorized to perform fund transfers and deceives them into performing fraudulent fund transfers and/or Data Theft.

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 10, 2019

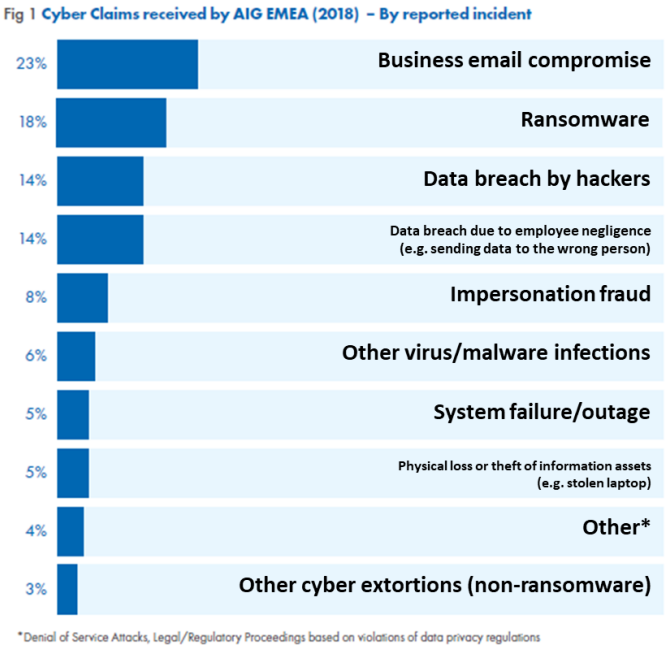
Alert Number
I-091019-PSA

Questions regarding this PSA should be directed to your local FBI Field Office.

BUSINESS EMAIL COMPROMISE THE $26 BILLION SCAM

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

Source: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise



Source: https://www.aig.co.uk/content/dam/aig/emea/regional-assets/documents/aig-cyber-claims-2019.pdf

Below are some BEC attack scenarios...

Scenario 1 – *Change payroll account information*

Attacker sends spoofed email impersonating an employee to the HR to change the salary account details to Attacker's account number. Salary account details are modified by the HR based on the mail.

Scenario 2 – *Authorize a fund transfer impersonating a high-profile executive or an authorized user*

Attacker sends a spoofed email impersonating to be a high-profile executive or an authorized user, requesting the finance department to initiate a fund transfer to attacker's account. Based on this email, the finance department performs the transfer to the attacker's account without further checks.

Scenario 3 – *Account compromise*

Account compromise may occur due to a malware or phishing or via social engineering attack where the perpetrator Impersonates IT personnel in the target user's company and the user discloses credentials without further verification. Attacker connects to authorized user's email account with the compromised credentials and sends an email to transfer funds to attacker's account number.

Best Practices for Protection against BEC

- ✓ Periodic cybersecurity awareness programs.
- ✓ Multi Factor Authentication - protection against static password Compromise.
- ✓ Web Security (web proxy) - to prevent access to bad websites and block unauthorized downloads.
- ✓ Mail security - Protection against email threats.
- ✓ Enable email to display complete email address instead of only names.
- ✓ Use dual authorization to verify the authenticity for requests related to sensitive data modification.
- ✓ Prevent users from installing or running unauthorized software.
- ✓ Do not share login credentials or Personally Identifiable Information (PII) Data with others.
- ✓ Do not store login credentials in plaintext.
- ✓ Do not click on the links on email without verifying the link.
- ✓ Deploy Latest version of Anti-Virus (AV) along with Endpoint Detection and Response (EDR) for endpoints.
- ✓ Share sensitive documents in a secured way such as secure file share, encrypted transfer etc.
- ✓ Cyber Insurance with BEC Protection.