TLP: WHITE

JUNE 2018

Growth of Business Email Compromise in the Retail Sector

R-CISC Retail ISAC Insights

A Closer Look at Business Email Compromise (BEC) Attacks

Over the past few years, business email compromise (BEC) attacks have expanded significantly. Threat actors have employed these attacks due to their combination of simplicity and effectiveness and the low level of sophistication needed to execute the attacks.

The Internet Crime Complaint Center (IC3) has broken down the five most common BEC attacks into the following categories:

- **The Bogus Invoice Scheme** – As the name suggests, this involves the use of a fake invoice to trick organizations. BEC actors typically use this scheme against companies that deal with foreign suppliers.

- **CEO Fraud** – In this scenario, attackers pose as an executive of the company to send an email to employees—usually to those in finance—requesting a money transfer to accounts they control. The attackers usually design "urgent" messages to throw their targets off-guard.

- **Account Compromise** – An executive or employee's email account is hacked and used to request invoice payments to vendors listed in their email contacts. Payments are then sent to bank accounts the BEC actors control.

- **Attorney Impersonation** – Attackers pose as a lawyer or someone from the law firm supposedly in charge of the company's crucial and confidential matters. Such bogus requests are usually done via email or over the phone, and around the end of the business day.

- **Data Theft** – BEC actors target employees in HR or bookkeeping to obtain personally identifiable information (PII) or tax statements of employees and executives. Such data can be used for future attacks.

Types of BEC Attacks

The two most common types of BEC attacks observed being utilized by threat actors are malware-employed and email only. Malware-employed BEC attacks use off-the-shelf software often available on the dark web, which provides less sophisticated threat actors with the basic features needed to operate the scam. Ardamax and Lokibot are two examples of such software readily available on the dark web.

Types of BEC Attacks (Cont.)

- **Ardamax**, which is currently advertised as a keylogger, has been discovered being used in recent BEC attacks. The keylogger is available for around US$50 and includes essential features that a BEC operator would find useful. The program consists of various options to retrieve stolen credentials, which is a significant advantage and selling point for potential buyers. Ardamax can send the stolen data via SMPT or FTP and features an option to send out encrypted logs that users can view in its log viewer. Ardamax is advertised as legitimate surveillance software for purposes such as online safety for children, employee monitoring, and evidence gathering. While Ardamax can certainly be used for these purposes, criminals typically use them for different reasons.

- **LokiBot** is another malware variant being used in BEC attacks. LokiBot was initially advertised as a browser password stealer and coin wallet stealer in 2013, frequently sold in Russian hacking forums. Lokibot notably features a password stealer module integration for different applications such as browsers, email clients, FTP/SSH/VNC clients, IM clients, online poker clients, and crypto coin wallet stealers. A newer version of the malware has added a feature that can capture screenshots of the infected host. It also came with additional browser support and the ability to target password managers. There has been no direct indicator showing that the bot has been used solely for BEC attacks, but the type of data it targets and the lures it uses are very similar to those being used for BEC.

Email only attacks are slightly more complicated and require a level of sophistication by threat actors to successfully compromise a victim. Social engineering techniques coupled with targeting techniques utilizing clever subject lines and legitimate looking email addresses designed to impersonate executives are commonly used.

Retail Sector Activity

Over the course of the last couple of months, the R-CISC has observed a slight uptick in BEC attack activity within the retail sector. A somewhat different variation of the CEO Fraud attack scenario targeting gift cards has been observed by retailers. Threat actors have posed as executives and requested gift cards be purchased on their behalf and the codes be sent via email. These requests are sent with an urgent temperament so that the tasks are concluded in a hasty manner and without question.

BEC attack activity has also grown in the last few years overall and shows no sign of receding. The low level of technical knowledge needed to begin targeting victims only adds to this growing level of activity. It is essential for organizations to be aware of the attack techniques present in BEC campaigns and educate their employees on how to prevent them. Policies and controls should be put in place to prevent losses associated with BEC attacks.

Sources:
https://www.ic3.gov/media/2017/170504.aspx
https://documents.trendmicro.com/assets/TrackingTrendsinBusinessEmailCompromise.pdf