Cybersecurity through Crowdsourcing

Deloitte

Use Case Two
BEC Scam Identification through Corporate-Level Crowdsourcing

April 30, 2018

Group Two:
Yiqing(Alice) Guo
Steve Cardozo
Li Chen
Pan Deng
Mengwen Zhou

Information Technology Master's Capstone
ITWS-6800

Prof. Richard M. Plotka

Use Case Two

Table of Content

Targeted Issue

According to the FBI's announcement last year, business email compromise (BEC) scams have continued to grow and evolve over the past three years[1]. The victims range from small businesses to large corporations and span all 50 states and more than 130 countries. Based on complaint data, this kind of scams caused more than $5 billion in losses between October 2013 and December 2016. Usually, this kind of scam email does not contain detectable payloads such as a malicious URL or a malicious attachment. The most alarming thing of this scam is that fraudsters always perform in-depth reconnaissance of the victims beforehand in order to make the final attack as convincing as possible. The reconnaissance can be done through social engineering using publicly available information or phishing/scam emails to obtain confidential information.

There are five major scenarios of a BEC scam:

- Mimicing a longtime supplier of the business to send fraudulent payment requests
- Sending a request for a wire transfer to a second employee or a financial institution from a compromised email account of a senior executive
- Sending fraudulent requests for invoice payment from a compromised personal email of an employee to multiple vendors
- Faking emails of a lawyer or a representative of a law firm to contact victims and pressure them to handle time-sensitive or confidential issues involving the transfer of funds
- Sending requests for PII or W-2 to certain employees who are responsible for the confidential data from a compromised email account of a senior executive

Solution Purpose

Although businesses increasingly pay attention to BEC scams, they can hardly make sure that all of their employees are able to identify the continually evolving BEC scams by personal experience. The proposed solution will build a scam identification network to harness the power of different companies in the world.

In carefully planned scams, fraudsters might target different employees at different stages so that victims can hardly identify the scams by themselves at an early stage. The solution will allow businesses to identify scams systematically and effectively with the contributions of individual employees.

[1] "Business E-Mail Compromise E-Mail Account Compromise The 5 Billion Dollar Scam." *Internet Crime Complaint Center (IC3)*, Federal Bureau of Investigation Public Service Announcement, 5 May 2017, www.ic3.gov/media/2017/170504.aspx.

Crowdsourcing Approach

The proposed crowdsourcing approach is to build enterprise-wide crowdsourcing networks for scam email identification and supplier/vendor/partner email identification, and an inter-enterprise network which collects the data of scam emails from all participating companies and trains identification models using machine learning and data science.

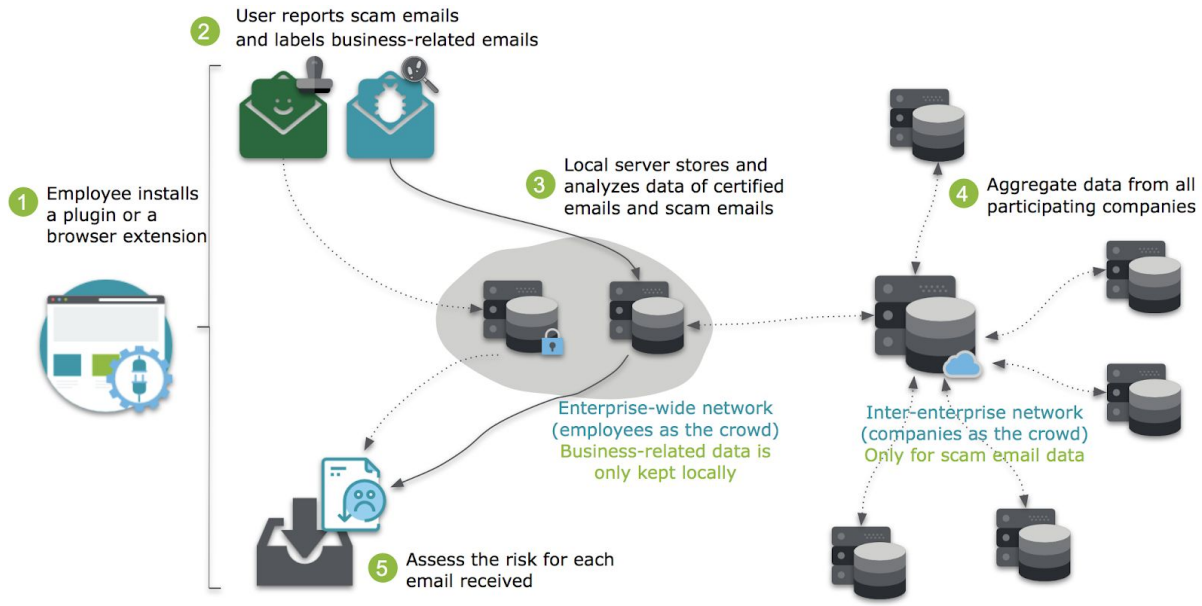

Figure 1 : High-level Work Flow Diagram.

The solution will be based on a plugin or browser extension. It will be compatible with various email applications including Apple Mail, Gmail and Outlook. It can also be customized to be compatible with the clients' own email application. The browser extension will be compatible with different browsers including Chrome, Safari, IE and Firefox. It will provide users on-click services to report suspicious emails or label business-related emails. Besides keeping the blacklists and certified lists of email addresses, it will train models for patterns of scam emails and models for business partners' email habits. It will show a warning message when a user receives an irregular email. It will also show likelihood reports on emails from addresses that are neither in the blacklists nor certified lists.

Apart from the big data driven process, the network can also identify compromised emails by using the open standard DMARC and keeping records of email sending activities. DMARC can help identify spoofing attacks which fake their email addresses via corrupted server. Typically, DMARC will attach a signature to each email sent from a legitimate server so that the system can identify and block emails that are sent from a corrupted server. The plugin/extension will keep a record every time a user sends or receives an email to/from another user. This will be useful for automatically detecting a compromised email. For example, if a financial manager receives an email from an executive, but no records show that

the executive sent the email, the solution will alert the financial manager that this might be a compromised email.

Scenario	DMARC	Display Name in the Trusted Contact List	Address Matches the Display Name	User of the Network	Record of the Sent Email	Correspond-ing Action
Scenario 1: Spoofing Attack	✘	N/A	N/A	N/A	N/A	Block
Scenario 2: Display Name Deception	✔	✔	✘	N/A	N/A	Alert / Block
Scenario 3: Email from a Stranger	✔	✘	✘	N/A	N/A	Warning, Risk Report
Scenario 4: Email from a Trusted Contact, but not a user of the Network	✔	✔	✔	✘	N/A	Risk Report
Scenario 5: Compromised (Acount Taken Over)	✔	✔	✔	✔	✘	Alert
Scenario 6: Safe Email	✔	✔	✔	✔	✔	Certified

Table 1 : Senarios & Corresponding Actions.

In the 1st scenario, a user receives an email which does not have a DMARC signature. Our system will simply block this email without checking the contact or the sent record. In the 2nd scenario, the email is sent from a legitimate server, but it fakes its display name as a trusted insider. Our system finds the name on the list of trusted contacts, but the address does not match. Thus, it will alert the recipient or just block this email. In the 3rd scenario, the email is verified by the DMARC system, but the sender is not in the list of trusted contact. The recipient will receive the email and will be warned that it is from a stranger. The recipient can identify whether it is a scam email with the help of the risk report generated by the scam identification model. In the 4th scenario, the email is sent from a trusted contact but the sender is not a user of our network. The user can also identify the email with the help of the risk report. In the 5th scenario, the sender is verified as another user of the network, but the system can't find the sent record of the email. Thus, it will alert the user that it is potentially compromised. In the last scenario, the email is sent by another user of the network and the activity is recorded by the system. Thus, the system will tell the recipient that this

email is trusted.

Potential Clients

According to the statistics from the FBI, financial institutions, especially banks located in China, are the prominent destinations of BEC scams[2]. Financial institutions are major potential customers of the service. In fact, every company that uses a corporate email may be interested in the service as long as the service guarantees privacy. Companies may be more interested in the service when its business partners, suppliers, or clients are using the service. The larger the crowdbase is, the more effective the service will be.

List of Requirements for the Crowd

Only the employees of the participating corporations are allowed to install the plugin/ extension in their work computers. The participating companies must be legitimate, and they must have their own corporate emails.

Potential Issues

Companies may be worried that the data sent out by the plugin/extension includes some of their confidential information and that other companies might take advantage of it.

Possible Solutions

Only preprocessed and encoded data will be sent to the data center. The data and models of client/partner emails will be kept privately by each company itself. The modeling and identification process will be driven by machine learning algorithms. Users will only receive the results. No one but the service provider who signed a confidentiality agreement will be able to access the data.

The team also decided to provide customized options on data sharing for each company. Companies may choose to share only scam related data, sent or received records, or nothing at all with the inter-corporate network. In these cases, however, depending on what the company shares, the company will only get a corresponding level of service.

[2] "Business E-Mail Compromise E-Mail Account Compromise The 5 Billion Dollar Scam." *Internet Crime Complaint Center (IC3)*, Federal Bureau of Investigation Public Service Announcement, 5 May 2017, www.ic3.gov/media/2017/170504.aspx.