TRUSTEDSEC CASE STUDY

TrustedSec
Evolve beyond threats

Swift Response Decreases Damage of Business Email Compromise and Attempted Invoice Fraud

A manufacturing company reached out to TrustedSec after falling victim to a business email compromise (BEC) and had begun transferring funds to a malicious account disguised as the company's law firm. The TrustedSec Incident Response team leveraged their experience and collaborative approach to quickly assess the situation, stop the attempted invoice fraud, and put in place measures to prevent future attacks.

PERSONNEL PROFILE

Engagement Lead:
Tyler Hudak,
Practice Lead, Incident Response

Tyler has over 20 years of real-world experience in incident handling, malware analysis, computer forensics, and Information Security for multiple organizations. He has spoken and taught at a number of security conferences about topics, ranging from Incident Response to penetration testing techniques.

The Weakest Link

It is often said that the weakest point in an organization's security infrastructure is its people. This notion is illustrated by the rapid rise of business email compromises (BECs), which saw a 100% increase globally between May 2018 and July 2019, according to the Internet Crime Complaint Center (IC3).

In 2019 alone, TrustedSec handled more than 20 BEC investigations. A manufacturing company contacted TrustedSec when an employee received a bank alert after remitting payment to who they believed was the company's legal counsel. Incident Response Lead Tyler Hudak and his team brought their extensive experience with BECs to the table and were able to ensure the invoice fraud attempt stopped there.

"When we get called by a client, we first do a scoping call to figure out what happened, what the attacker has access to, and for how long," Hudak explains. "In this case, we told the client to get off the phone with us and contact the bank immediately to stop payment, because money cannot be recovered easily beyond 48-72 hours."

A Manual Search

Next, TrustedSec consultants combed through logs and email records, searching for an unusual login, such as an IP address originating from Nigeria or Russia, as well as recently implemented email rules and any actions performed by the attacker, such as searching for certain keywords.

TrustedSec utilizes automated systems that allow consultants to load logs directly and yield information for a relatively quick turnaround. "With BECs, from the moment you discover they happened, time is of the essence—especially if money was transferred," Hudak says.

As with 99% of all BECs, the manufacturing company used Office 365 for email without multi-factor authentication (MFA) in place. As a result, the attacker used a brute-force attack to glean credentials and passwords, which gave them email access. Once the attacker was in the account, they clicked through previous emails to find the names of frequent company vendors.

In this case, the attacker picked the company's law firm. The attacker created an email address using a similar domain name as the law firm and sent an email to the targeted account, saying that the wire transfer account number had changed, and payment should be sent to the new number as soon as possible. To further delay the discovery of the ruse and prevent legitimate emails from being sent, the attacker set up mail deletion and forwarding rules so that emails with specific words or phrases were forwarded to a separate, attacker-controlled mailbox.

A BUSINESS EMAIL COMPROMISE TIMELINE

- Attacker gains access to an employee's email account using a brute-force attack
- Employee receives alert from bank indicating that a payment appears fraudulent
- Business reaches out to TrustedSec for Incident Response
- Scoping call takes place to provide TrustedSec with all necessary information
- Business contacts bank to stop payment
- TrustedSec begins incident investigation
- TrustedSec provides summary of logs and email records to determine suspicious activity
- TrustedSec compiles timeline of entire BEC attack along with recommendations to thwart future attacks
- TrustedSec's GRC team provides additional remediation suggestions

Consulting the Experts

From there, TrustedSec created a timeline to document when the attack occurred and what attackers did within the time period. A list of best-practice recommendations was compiled as well, so the organization could plan for (and hopefully prevent) future attacks.

"In BEC cases where the client's email was compromised, all of them used Office 365 without multi-factor authentication (MFA) in place," Hudak says. "We recommend that organizations turn on MFA in the Office 365 email system as it is the number one way to prevent attackers from accessing email accounts through stolen, leaked, or brute forced passwords."

To provide the best guidance possible, TrustedSec utilized access to a knowledge consortium in which team members share intelligence and common indicators of compromise with each other and the greater cybersecurity community.

Since the manufacturing company had begun transferring the requested funds before the bank flagged it, TrustedSec recommended that the payment processes be reviewed and reimplemented. TrustedSec's own Governance, Risk, and Compliance team suggested that the organization have additional procedures in place where they have to call someone directly in order to change account numbers or transfer money. From there, TrustedSec's Remediation team took the extra step of implementing MFA across the organization's environment.

"Our team is made up of individuals who are experts in their fields with a diverse set of talents," Hudak says. "Because of our experience with a large volume of BECs, we are able to quickly jump in and turn them around."

HOW TO HANDLE A BEC ACCORDING TO THE IC3

In a 2018 PSA released by the FBI, the bureau included information about the activity and a set of recommendations about how to handle a BEC.

Initial steps to take if a BEC is detected:

- Contact the originating bank and request a wire call
- Immediately file a complaint with IC3.gov
- Save and retain all messages and evidence associated with the incident

What to report to the IC3:

- Any messages pertaining to the attack
- Victim information
- Overall losses associated with the BEC
- If a payment associated with the attack was sent, provide transaction details
- Victim impact statement (e.g., impacted services/operations)
- IP addresses used to send fraudulent emails