SECTIGO

Sectigo Email Security Solution

Email hacking is a commonly used malicious tactic in our increasingly connected world. Business email compromise (BEC), or email account compromise (EAC), is one such scheme that uses email hacking for potentially huge payouts for attackers. The Federal Bureau of Investigation (FBI) has described BEC/EAC as "…phishing schemes in which an attacker impersonates a high-level executive and attempts to trick an employee or customer into transferring money or sensitive data."

The total global losses due to BEC/EAC have reached US$12.5 billion this year. What is notable about BEC/EAC is that, unlike email-based ransomware and other malware-dependent attacks, its operators don't have to rely entirely on malicious components to defraud victims. The fraudulent email might claim, for example, that a supplier requires prompt payment for a service rendered.

Recently, a man in Los Angeles was arrested for a BEC/EAC attack that gave his accomplices unauthorized access to the emails of an attorney involved in real estate settlements. The attackers then sent spoofed emails, tricking a purchaser in a real estate transaction into transferring $531,981 to an account of a woman, who, in turn, transferred $60,000 to a fraudulent account.

Business email compromise (BEC), or email account compromise (EAC) is on the rise — and it's often difficult to prevent because it's so targeted. So, what do you need to do? How do you protect your organization?

"phishing schemes in which an attacker impersonates a high-level executive and attempts to trick an employee or customer into transferring money or sensitive data."

FBI guidance is - Use digitally signed emails.

What is digitally signed emails?

A digital signature attached to an email message offers a layer of security by providing assurance to the recipient that you—not an imposter—signed the contents of the email message. Your digital signature, which includes your certificate and public key, originates from your digital ID. And that digital ID serves as your unique digital mark and signals the recipient that the content hasn't been altered in transit. A digital signature on email provides following security attributes:

Business email compromise (BEC), or email account compromise (EAC) is on the rise — and it's often difficult to prevent because it's so targeted. So, what do you need to do? How do you protect your organization?

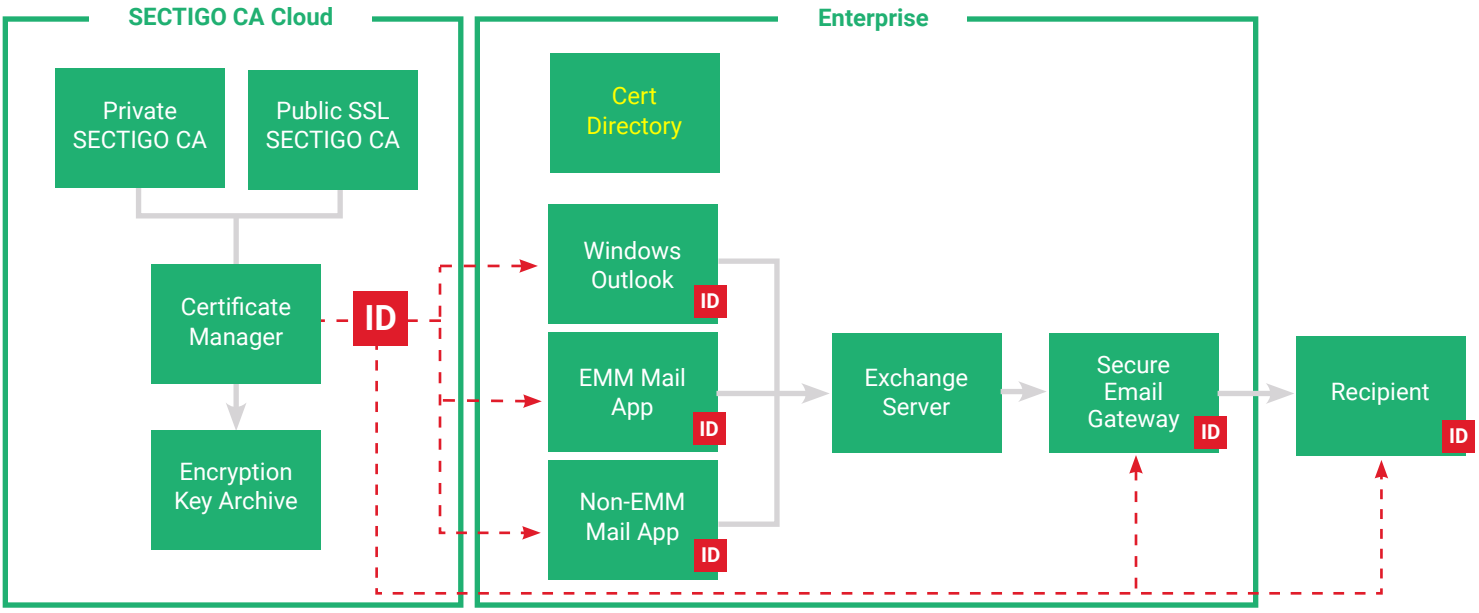
- *Sender verification:* the sender is who he/she claims to be
- *Integrity:* The message has not been altered during transit
- *Non-repudiation:* the sender cannot deny having sent the message

Another layer of defense - Encryption.

SMIME also provides end to end encryption. Emails are secured both in motion and at rest. Encryption protects email contents in cases when the credentials to the exchange server are compromised or when using a cloud mail server which can be accessed by the cloud service operator.

How to combat BEC/EAC or Email Phishing using Sectigo CA Email Security solution...

Sectigo CA offers best in class, fully automated, cloud-based email security/SMIME certificate solution. The certificates can be issued from either the Sectigo CA publicly trusted subordinate or from a privately trusted CA setup specifically for the enterprise.



In a nutshell, Sectigo CA Email Security solution provides following unique features:

- The publicly trusted CA allows any digitally signed email to be verified by most of the email applications being used by the email recipients world-wide. The intent is to ensure the recipient knows the email really came from the sender. The typical email application shows a checkmark that the signature is authenticate (Apple Mail example below).

Private CA SMIME is suitable when only encryption is required, or recipient validating digital signature belongs to same enterprise as the sender. All other cases should use Public SMIME.

- SMIME certificate **automatically** installed into all mail clients.
- Encryption key archive accessible to secure email gateway to sign and encrypt/decrypt at the gateway.
- Only vendor that delivers this capability, using publicly trusted digital signatures.
- Encryption keys along with entire key history are achieved, should the employee accidentally destroy the key --- they can continue to decrypt emails in the mail server. It eliminates the possibility of the employee backing up the key in a poor manner, or not backing it up at all and risk losing IP.

