United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

ANATOMY OF A BUSINESS EMAIL COMPROMISE

SETTING THE HOOK

The initial compromise into the victim network likely occurs well in advance (months) of any funds transfer. One or more email accounts are compromised through a phishing email or some other attack method where malware is used to expose email login credentials to access the company's web-based email system. The attacker targets the email accounts of management level employees with routine access to sensitive information regarding financial data and human resource information.

LAYING THE FOUNDATION

To lessen the probability of getting detected, the threat actor only conducts one unauthorized login on each compromised email account. During that login, the threat actor configures the following rules on each of the compromised accounts:

- **Auto-forwarding of all emails received to the threat actor's email account.**
- **All forwarded emails are automatically deleted from sender's email account once sent.**
- **As part of the set up process, the threat actor also registers several spoofed domains as derivations of the victim company along with several email accounts, all using some form of spoof deception.**

The threat actor gathers sensitive information needed to draft a convincing email to get the victim to conduct the wire transfer. The threat actor looks for financial account information, privileged and contemporaneous information regarding pending actions within a company, and the typical format and wording used by employees requesting/ performing money transfers. Personally identifiable information (PII) is also typically gathered to sell or use in other fraud schemes (identity theft, credit card fraud, loan fraud, etc.) as a secondary revenue source.

WATING TO STRIKE

It is very typical for the threat actor to monitor the email traffic of compromised accounts for several months to get necessary information to attempt the email redirecting a transfer of funds. Ideally, they look for opportunities where a victim company reveals they will be wiring funds or receiving funds. The threat actor then drafts and sends an email from previously setup spoofed email accounts. To convince the sender to wire the funds to the bank account provided by the threat actor in the fraudulent wiring instructions, the email contains format and language similar to the victim company. The use of incorrect grammar and syntax, and requests for urgency and/or secrecy about the transfer are important warning signs.

TIME IS OF THE ESSENCE

If the threat actor is successful and the funds are transferred from the victim company, the money moves very quickly. Often the threat actor will move the funds through several banks until they ultimately end up in an overseas account. If the victim detects the fraudulent wire transfer, actions must be taken immediately. The probability of reversing the wire transfer or recovering any of the misdirected funds decreases with every hour that passes. The U.S. Secret Service Guide to Business Email Compromises provides information on preventing and reporting BECs to law enforcement.