Masquerading for Cyber Espionage and Fraudulent Transactions

Masquerading is a fraud technique in which an attacker takes over an executive's account to pose as the executive or to conduct cyber espionage. The objective of the attacker is to obtain confidential information about the company or to complete a financial transaction to a bank account that the attacker controls. A company's loss of proprietary information, such as trade secrets and personally identifiable information (PII), as well as the financial loss can be devastating. According to the Federal Bureau of Investigation's Internet Crime Complaint Center 2014 Scam Alert report, the average monetary loss experienced by a victim is US $55,000; however losses upward of US $800,000 have been reported.

What Does Cyber Masquerading Look Like?

Executives that are victimized often are exploited through spear-phishing tactics. Compromised emails are sent directly to the executive, or their staff, in a fashion that looks like it is coming from a trusted source in order to gain information to compromise the executive's account. If the executive or staff opens the spear-phishing email and the account is successfully compromised, the attacker can send urgent emails or messages to employees within the company asking for confidential information or to authorize a wire transfer. Employees receiving the emails usually comply with the request since it appears to be coming from the executive and in some instances employees have bypassed security requirements to expedite the request.

Social Networking Sites (SNSs) have introduced a new platform for cyber espionage through masquerading. SNSs as a tool to engage in cyber espionage and criminal activities pose a threat to the reputation and confidential information of companies. Innovative SNS attackers are identifying a host of new vulnerabilities that are present in the use of SNSs. Cyber criminals can compromise a social network profile of an executive or simply pose as an executive by setting up a new account in the executive's name. The vulnerabilities associated with cyber actors utilizing SNSs to facilitate corporate espionage are rarely technically sophisticated or cutting edge. Through phishing tactics an SNS account can be compromised, but a malicious actor can also simply create an account in the name of the victim they want to masquerade.

Cyber Espionage Case Study: Iran's Newscaster

Cyber criminals, for financial and espionage purposes, are using SNSs to advance their malicious operations. Since 2011, actors tied to Iranian interests formed a large net of false social networking personas to target, compromise and collect intelligence from high-value targets. While no known Citi targets exist, the ramifications of the three-year operation are astounding: Iranian-attributed actors were able to have close access and presumably collect intelligence from high-value targets in the US Government, defense contractors in the US and Israel, and victims in the UK as well as Saudi Arabia and Iraq because they were able to develop and form trusted relationships.

Masquerading through an SNS account, and convincing others that it is legitimate, is relatively simple. For example, an executive named Jake Smith might not be on any SNS, but a malicious actor could create an account under the name Jake Smith. By adding a photo of Jake Smith, easily found on the internet, the malicious actor can request connections to people that legitimately know Jake Smith. Most people assume that an account name is who they say they are and would accept the

Cyber criminals can compromise a social network profile of an executive or simply pose as an executive by setting up a new account in the executive's name.

connection. By creating an account that is linked to legitimate people and known connections the malicious actor can elicit information from people, post corrupted links, or conduct other compromising actions with relative ease.

Executives are dependent on email communication and many have a desire to be on social media, therefore it is important that measures are taken to protect their communications, information, and reputations online. By using the following techniques, the threat of masquerading can be reduced.

Mitigation Techniques

Wire Transfers

- Establish a multi-person approval process for transactions above a specified dollar threshold. Two or more approvals are helpful in preventing internal or external fraud.
- Be on alert for wire transfer instructions that include tight deadlines.
- Be suspicious of confidentiality. Speak to the executive or manager requesting the transaction on the phone or in-person. If you still have doubts, speak to another senior executive.
- Many companies require a valid purchase order number as well as approval from a manager and the finance department to spend money.

Spear-phishing

- Avoid clicking on any links within e-mails or opening unexpected attachments, particularly when the e-mails are branded with your SNS logo. Instead, login to the SNS directly via the URL.

Browsing Awareness

- Exercise caution when clicking on links, especially shortened URLs, when on an SNS. This is a prime mechanism to infect a machine with malware.
- Ensure that your connection, particularly when signing into the SNS, is encrypted. This is reflected by a small green lock present near the address bar.

Aggressive Password Management

- Regularly change passwords for your email accounts and SNSs. Ensure that passwords are not duplicated on multiple SNSs or other sensitive platforms such as corporate accounts, bank accounts, and personal e-mail accounts.
- Enable multi-factor authentication, when available. This feature is oftentimes offered by popular SNSs; however the user elects to deactivate the feature.

Personal Device Management

- Manage SNSs from properly patched and secure machines. When accessing SNSs from personal devices, ensure that devices are updated with the latest patches for the Operating System (ex: Apple/Microsoft).
- Confirm that popular add-on software components, such as Adobe Flash and Microsoft Office, are properly updated.

Content Privacy

- Maintain familiarity with the privacy filters, privacy policy and terms of service to ensure awareness of how content is being shared and stored. Changes are frequently made by the SNSs, requiring periodic attention by the user to the settings.