THREAT ADVISORY: ONLINE BANKING ADVANCED SOCIAL ENGINEERING

SBS CyberSecurity has been made aware of an attack on customer online banking accounts. This attack is a combination of:

- Social engineering
- Open-source intelligence (OSINT)
- Dark web content purchase

This new twist on an old attack is an advanced social engineering attack, targeting customers that are connected to their financial institution via social media. Attackers leverage social media and open-source intelligence (OSINT) to gather reconnaissance information on a customer, then contact the customer while posing as the financial institution.

The attacker's objective is to convince the customer that their online banking account has been compromised and the customer needs to change their online banking password to a "temporary" password and provide the MFA code. Once successful, this attack will give the attacker full access to the customer's online banking account, which has and will lead to a significant loss of customer funds.

SIEM or IDS/IPS cannot identify the attack, and no indicators of compromise are present until customers complain about their accounts being drained of funds.

The attacker starts by:

1. Using recon from a financial institution’s Facebook page. Individuals who “like” the financial institution’s posts appear to be the attackers' primary targets, giving the attacker a probable customer target list.
2. The attacker then performs OSINT on these customers, gathering details about the potential customer and creating their own social profile. OSINT allows anyone to be profiled for their public information, such as their street address, phone number(s), email addresses, other social media accounts, date of birth, etc.
3. The attacker utilizes the dark web and internet search resources for potentially compromised personally identifiable information (PII) for the customer, including Social Security Number (SSN) and any other account numbers from previous compromises.

Once the attacker has a complete OSINT profile of the potential customer:

4. The attacker may make some innocuous calls to the financial institution to verify that the person is indeed a customer at the financial institution.
5. Once verified, the attacker plans an advanced social engineering attack on the customer.
6. The attacker pulls up the financial institution’s online banking webpage and calls the customer.
7. The attacker spoofs the financial institution’s phone number to appear official.

8. The attacker convinces the customer that their online banking account has been compromised, asking the customer to then browse to the financial institution's online banking portal.
9. The attacker may use the customer's previously obtained information to convince them that they are official.
10. The customer is directed to the financial institution's website and asked by the attacker to reset their password to something simple, like "password1234". The customer might tell them that they do not want their password set to that. The attacker states they understand that, and this password reset is only temporary. Victims stated that the social engineers are very convincing and have even been able to convince the victims to provide the attackers with the resulting MFA authorization code, where needed.
11. Once the password is reset, the attacker has access to the customer's account and can drain customer funds in various ways.

Currently, the only known ways to potentially protect your online banking customers against this fraud are:

- Disable the "reset password" button on the online banking website for the short term. This will cause a potential customer service issue until the hackers move on to another target financial institution.
- Inform your customers of this ongoing social engineering attack and provide education on how the customer can best protect themselves.
  - Remind customers that the financial institution will never ask for passwords or MFA passcodes.
  - Encourage customers to set up appropriate online banking alerts (SMS or email), including alerts for password reset and large transfers.
- Review social media privacy settings and consider restricting which users can see who "likes" or comments on social media posts.

If you have a customer that has fallen victim to this attack:

- Collect incident details, including:
  - Phone number of the customer that was called
  - Date and time of the call
  - Call duration (if possible)
- Contact the FBI and be prepared to share details of any attack your financial institution is experiencing.

This attack is widespread. The FBI is aware of the issue and is actively working to mitigate the attack.