December 20, 2013 Release # 245

-- Begin Transmission --

Phishing 2.0 Targets Business Firms – Part 1

Phishing 2.0, a new version has emerged, fueled by new cybercriminals and new phishing techniques. New types of phishing campaigns are particularly worrisome because of the following:

- ❖ They are aimed at businesses (including small and midsize businesses) rather than consumers.
- ❖ They evade traditional antivirus and anti-phishing products.
- ❖ They can fool even security-savvy computer users by using information gathered from social media and other web sources.
- ❖ They often target employees with access to the most sensitive information, such as bank accounts, customer lists and intellectual property.

The Rise and Decline of Phishing 1.0

Most computer users are familiar with phishing campaigns that broadcast identical emails to thousands of email addresses. These emails appear to be from banks, online retailers, social networking sites and other widely used websites. They entice readers to go to a website controlled by the cybercriminals and fill in a form or download a file containing a Trojan, key logger or some other type of malware. The goal of Phishing 1.0 campaigns is to obtain information that can be used for identity theft, such as but are not limited to user IDs and passwords, and credit card information.

However, information security companies have diminished the effectiveness of standard phishing campaigns through countermeasures that:

- ❖ Recognize common phrases used in phishing messages (lexical analysis).
- ❖ Flag websites known to send phishing messages and others known to capture information from victims (reputation analysis and blacklists).
- ❖ Identify attachments containing known malware (signature recognition).

Also, the number of naïve email users has fallen as accounts of these attacks have circulated in the press. These factors have limited the potential for financial gain from standard "mass" phishing attacks.

To be continued…

-- End of Transmission –

Information Security: It's a Shared Responsibility

REFERENCE(S): www.webroot.com