Email Fraud – It's Only Getting More Sophisticated

Source: *FedFocus – January 2016*

Since the early 1990s, businesses have been using email as a cost-effective communication, collaboration and information-sharing tool. Email has, for many organizations, become the primary method for corresponding with colleagues, customers and business partners. Unfortunately, adversaries often take advantage of this reliance on email to attack information infrastructures.

Adversaries use a number of methods – stand-alone and in combination with others – to carry out their attacks. These methods range from viruses that can corrupt mission-critical applications to spam that can impede the performance of your organization's communications infrastructure. Email security threats, if exposed, have the ability to greatly impact operations. To help keep financial institutions well informed, below is an overview of some of the most common email security threats.

Spam

Spammers send unsolicited commercial email advertising for products, services or websites. While most spam is recognizable and simply annoying, some of it can be downright dangerous. Spam can include links to malicious software and other cyber threats. Adversaries use spam in an effort to "trick" recipients into opening malicious emails to increase the spread of viruses, spyware and malware.

Phishing

Internet scammers use email as bait to "phish" for passwords, personal and financial information from Internet users. Phishing schemes are typically used to perpetuate identity theft or financial fraud by posing as "authorized" emails from established and trustworthy institutions. In the past, these campaigns were mainly aimed at individuals, but as adversaries have become more sophisticated, they have begun targeting businesses in hopes of obtaining:

- Corporate credit card numbers
- Login IDs and passwords to gain access to customer databases or financial systems
- Business critical information

Viruses

A virus is malicious software that is attached to another program for the purpose of executing a particular unwanted function on a workstation. Viruses are very sophisticated and often appear to be harmless correspondence such as personal notes, jokes or marketing promotions. Most viruses require recipients to download attachments in order to infect the system and spread, but some are designed to launch automatically, with absolutely no user action required. The effects of email viruses can be significant and, in just a matter of hours, can bring down critical communication systems, hindering the performance of networks and corrupting vital business documents.

Spyware

Spyware is a stand-alone program that monitors a system's activities in an effort to detect passwords and other confidential information and then sends this information to another computer. Spyware enables adversaries to record all activities and data on the infected computer via a program that dynamically gathers information and transmits it via an Internet connection. Spyware is often bundled in with shareware and freeware programs, and usually installs and runs without the knowledge of the user.

Adversaries will try every trick imaginable to obtain confidential information or gain access to an organization's information infrastructure. Protecting your institution's critical information infrastructure in an increasingly sophisticated cyber threat-scape requires tools, but the most important deterrent is user vigilance.