December 27, 2013 Release # 246

-- Begin Transmission --

Phishing 2.0 Targets Business Firms – Part 2

Phishing 2.0: Anatomy of a New Attack

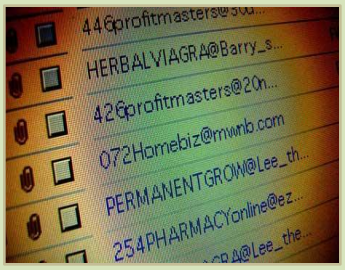
How do cybercriminals able to achieve such success in attacking businesses, which would seem to be better protected and more security-aware than consumers? The answer lies in the evolution of what is called Phishing 2.0 — a new breed of phishing campaigns designed to evade the countermeasures deployed against standard phishing attacks.

Phase 1: Targeting

The first phase of a Phishing 2.0 attack involves profiling a group of potential victims and targeting opportunities ranging from:

- Broad categories, such as "business people who ship packages" and "managers who book business travel," to
- General roles, say, finance executives, engineering managers or members of the legal staff, to
- Specific individuals in specific companies.

Phase 2: Reconnaissance



Finding personal information and email addresses of the targeted victims. For attacks targeting broad categories of victims, it might be sufficient to obtain lists of email addresses from legitimate mail houses or from black market sources of spam addresses. This is because a list of business managers will likely include a reasonable percentage who have sent overnight packages or booked airline reservations for business travel.

For attacks targeting business roles and specific individuals, cybercriminals may need to dig deeper to find names, email addresses and facts about the potential victims. But this is much easier today than in the past.

Company websites, industry and professional association websites, comment sections of blogs and bulletin boards often contain names and titles. Web searches make it relatively simple to find names and email addresses associated with given companies and professions. Social media sites like Facebook, LinkedIn, Google+ and Twitter, as well as video- and photo-sharing sites such as YouTube, Vimeo, Pinterest and Flickr, make it easy to gather names and very detailed personal and professional information. It is clear that the value of social media has not been lost on cybercriminals. By one estimate, 40% of social media users have been attacked by malware.

To be continued…

-- End of Transmission –

Information Security: It's a Shared Responsibility

REFERENCE(S): www.webroot.com