infosec@pjlhuillier.com
ICT GROUP
INFOSEC 101
CONFIDENTIALITY • INTEGRITY • AVAILABILITY

January 3, 2013 Release # 247

-- Begin Transmission --

Phishing 2.0 Targets Business Firms – Part 3

Phase 3: Creating Spear Phishing Emails

Think before you link.
PHISHING
Watch for sensitive information requests and never click on suspicious looking links.
Be wary of contextually relevant emails from unknown senders.

Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.

As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

In classic phishing fashion, the emails contain links to:
1. A website controlled by the cybercriminal
2. A legitimate website compromised by the cybercriminal
3. A file with a title interesting to the victim, but containing malware

Phase 4: Plant malware on the victim's computer

In some examples of spear phishing, the cybercriminal simply entices the victim to fill out a web form with confidential information like account number, home address, telephone number or user ID and password. More commonly, though, the goal is to lure the victim into downloading a malware file, either by clicking on an attachment in the email, clicking on a link in the email that requests a file download, or clicking on a link in a webpage. download" merely However, if there is an un-patched vulnerability in a browser or application on the victim's computer, the cybercriminal can often execute a "drive-by by luring the victim to a compromised webpage.

Phase 5: Exploit the Breach

The cybercriminal is now able to follow up by capturing the victim's keystrokes, finding and exporting files on the victim's computer, or investigate into the company network using then victim's credentials. The last approach is the method typically used as part of advanced persistent threats, which are systematic campaigns to capture large quantities of confidential data over a period of time.

To be continued…

-- End of Transmission –

Information Security: It's a Shared Responsibility

REFERENCE(S): www.webroot.com ; http://searchsecurity.techtarget.com

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.