Lecture 30: Mounting Targeted Attacks for Cyber Espionage with Trojans and Social Engineering

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

April 23, 2017

3:33pm

Goals:

- Phishing and spear phishing attacks
- Can a well-engineered network be broken into?
- Socially engineered email lures
- Trojans and surveillance software tools (R.A.T, R.C.S, etc.)
- Cyber espionage
- Exploiting browser vulnerabilities

CONTENTS

30.1: SPEAR PHISHING ATTACKS THROUGH EMAIL

- As was mentioned previously in Section 17.10 of Lecture 17, the goal of a general phishing attack is to steal sensitive personal information (such as credit-card and banking information) for computers at large. Such attacks are also aimed at getting people to reveal the usernames and passwords they use for entry into different entities.

- Spam email is a commonly used medium for launching general phishing attacks. Examples of such spam include messages that appear to be from your bank, from an e-commerce site, from your email service provider, etc. These messages look deceptively real — including what *you see* for the URLs in the body of the messages. However, under the hood, these URLs point to malicious websites that are frequently located in countries with questionable law enforcement.

- As an example of phishing that we commonly see at Purdue, the students and staff at Purdue frequently receive email [If you are at Purdue and not seeing such email, it is probably because ITaP's spam filter has successfully filtered it

out from your email stream.] that appears to come from a sysadmin and that informs you that your mailbox is full and cannot receive any further messages. It then asks you to log into a website to add to the storage allocated to your mailbox.

- When phishing is directed at a specific individual, it is known as spear phishing. Spear phishing is a prime example of a social-engineering based attack since it frequently requires careful research by the bad guys into what it would take to get the targeted individual to do their bidding, which in most cases amounts to getting the victim to either download an attachment or to click a link. The attachment, which is often a Microsoft Word or PowerPoint document, when executed results in the victim's machine creating a backdoor for downloading additional malware. And the link, when clicked, takes the victim to an authentic looking website where the victim is asked to enter his/her username and password and other such personal information.

- As you can imagine, once the bad guys have a victim's username and the password, any email generated by the bad guys *under the guise of the victim* will be trusted by the victim's colleagues and friends. And that trust can be taken advantage of to break into the computers of these other individuals for the installation of trojans and other malware. In this manner, an entire organization can be infected through and through, resulting in a massive stealing of proprietary information by the adversaries. For obvious reasons, such wide-scale infection makes it that much more

difficult to carry out an organization-wide cleansing of the malware after the intrusion is discovered.

- When spear phishing attacks involve getting a victim to visit what is a fake website that looks exactly like the real thing, the fake website is typically supported on machines in countries with lax law enforcement.

- As an example of a highly successful spear phishing attack in a high-stakes presidential contest in the US, you have surely already heard of how John Podesta, Chairman of the Hillary Clinton's presidential campaign, fell prey to such an attack. In an email message that looked completely authentic, he was told that he needed to change his password and he was asked to click on a link for the purpose. The link led to a web page that also looked totally authentic — except that it was not. No sooner had he entered his new password that it was scooped up by the bad guys who immediately gained access to his accumulated trove of 60,000 messages. The web page in which he entered his new password was hosted on servers with a domain address assigned to a cluster atolls in the South Pacific.

- There is an excellent description of the specifics of the spear phishing attack on John Podesta in a June 1, 2016 NYT article titled *"Was It a 400-pound, 14-year Old Hacker, or Russia? Here's Some of the Evidence,"* by Jeremy Ashkenas. You can find this