writeup

Kevin Turkington

I. Overview

In Eric Peterson's lectures he gives an overview of phishing/spam emails and messages. Everything from how to identifying spam and phising emails and how these identification methods are streamlined and automated. Through the use of simple regex matching on all fields of a SMTP email. Or the use of yara signiture like matching by the use of heuristic filtering which allows the cyber security analyst to create filters that can find spam and targeted phishing emails by automatically analyzing subject fields, content, etc for specific keywords or simple characteristics of the email itself.

II. Phishing/Spam characteristics

Phising emails in some cases are a targeted attack against an individuals or a group of individuals. The purpose of a phishing attack is to gain access to a victims confidential data with malicious intent. The most common reasons for phising attacks is to gain financial information of a target a great example is the classic prince of Nigeria scam which requires a victim to to provide an upfront payment with the promise of more money in the future.

The other type of malicious emails is spam emails, they tend to pray on a victim misjudgment of a product or service being presented. Spam emails in nature tend to cast a wider net than phishing emails because they are usually filtered however the less than one percent that do fall for them make it worth it for the attacker. A phishing email in content will usually serve a victim with a product with the prime example being male performance enhancing drugs when in reality they are just sugar pills.

III. Attack vectors and defence

The primary distribution method of these emails and messages are through the use of mass automated emailers or message bots. However overtime these methods can be tracked and blocked for high SMTP traffic. To avoid detection of a single server being caught spammers as well as phishers have employed the tactic of using botnets to generate mass amounts of SMTP messages, in order to spread out the ips being used to send mail to groups of individuals. To counter the use of botnets cyber security developers have used simple regex matching methods looking for common keywords used by spammers in their mail examples can incudle: viagra, oprah, and dr. Oz. However for a more distinct approach mail can be filtered out via huristics. Adding weights to speficic high risk categorys like where the mail was sent, any attachments associated with the mail, and links to known spam sites or possible spam sites.