A Comparative Analysis of Exploit Kits: How Are Exploit Kits Infecting Machines?

Kaitlyn Gurule
Purdue University

Problem

The first piece of malware was thought to be created in 1971 by Bob Thomas and was called Creeper. This piece of malware printed "I'm the Creeper. Catch me if you can!" to the screen. Since then, malware has increased in complexity. There are pieces of malware that hold a users files 'hostage' until a ransom is paid, called Ransomware. There was even a piece of malware called BlackEnergy that left 1.4 million people without electricity for hours. Currently, exploit kits are being used to take advantage of the vulnerabilities found in machines and infect them with malware. In one year the use of exploit kits increased by 75%. The use of exploit kits is increasing the number of machines being infected with malware. Increased knowledge of these kits can help to mitigate the problem they are creating.

Objective

Analyze different exploit kits to determine how they operate.

- How by-pass anti-virus software?
- How is the malware delivered?
- How is it infecting the machines?

Significance

Determining how the exploits work, will help to provide information to combat exploit kits.

- Vulnerabilities commonly exploited can be fixed.
- Users can be educated on the social engineering aspect of malware infection.

Approach

- Determine which are the more popular exploit kits.
- Determine how the exploit kits are being delivered.
- Determine what vulnerabilities the exploit kits are using and how these vulnerabilities are being taken advantage of.
- Determine how the malware infects the machines.

Once these determinations have been made, a comparative analysis is done to see what are the popular methods used by the most widely used exploit kits.

Analysis

The most widely used exploit kits in 2015 include: Angler and Nuclear. In January of 2015 the Angler exploit kit was used 38.7% of the time. By May 2015, it was used 82.2% of the time. Nuclear was the second most popular, being used 16% of the time in May of 2015. The software these exploit kits target are Flash, Internet Explorer, Java, Microsoft Silverlight, and Adobe Reader. They also use malvertising, or malware advertising, and phishing emails. Exploit kits are commonly targeting end-users. Therefore, users need to be more aware of the websites they explore, the software they download, the emails being sent, and they need to make sure their software is up to date. This awareness can to protect them from being infected.