A Survey of Malware Exploit Kits: Economic Influences of Exploit-as-a-Service

Ryan Gabet

Department of Computer and Information Technology
and CERIAS, Purdue University

Problem Overview:

In the digital realm of cybercrime, Exploit Kits (EKs) have emerged as a popular delivery method of malware, due in part to their ability to circumvent malware detection software. As their primary functionality, EKs leverage compromised servers, email accounts, websites, software, and application vulnerabilities to deliver malware to a victim's machine. Often in the form of a packaged file, the malware is downloaded and installed without the knowledge of the user or malware scanner. This study conducts a survey of security firm yearly security reports to better understand how malware economics have influenced the growth and development exploit kits and Exploit-as-a-Service (EaaS).

Significance:

Trends in EK usage bare a significant challenge to cyber security professionals. Through the frequent usage of zero-day vulnerabilities, new EKs are difficult to identify and thwart until observed in widespread usage. As exploit kits have been used in the past and are currently being used to attack IT infrastructures large and small, protection of customer and user data is a paramount challenge to IT security teams. As such, understanding the motivations, success rate, and type of malware distributed by EKs provide IT security professionals with a wealth of knowledge about how to better align corporate and enterprise level security postures to prevent wide scale data breach.

Methodology

Yearly security reports of four leading computer security firms were surveyed to address three components:

- Malware Economics
- Trends in Exploit Kits
- Trends in Exploit-as-a-Service

The following computer security firms with yearly published security reports used for this research were:

- Cisco
- Dell Securworks
- Symantec
- McAfee

General EK Infection Chain: