Developments and Defenses of Malicious Code

Xin Luo
University of New Mexico, USA

Merrill Warkentin
Mississippi State University, USA

INTRODUCTION

The continuous evolution of information security threats, coupled with increasing sophistication of malicious codes and the greater flexibility in working practices demanded by organizations and individual users, have imposed further burdens on the development of effective anti-malware defenses. Despite the fact that the IT community is endeavoring to prevent and thwart security threats, the Internet is perceived as the medium that transmits not only legitimate information but also malicious codes. In this cat-and-mouse predicament, it is widely acknowledged that, as new security countermeasures arise, malware authors are always able to learn how to manipulate the loopholes or vulnerabilities of these technologies, and can thereby weaponize new streams of malicious attacks.

From e-mail attachments embedded with Trojan horses to recent advanced malware attacks such as Gozi programs, which compromise and transmit users' highly sensitive information in a clandestine way, malware continues to evolve to be increasingly surreptitious and deadly. This trend of malware development seems foreseeable, yet making it increasingly arduous for organizations and/or individuals to detect and remove malicious codes and to defend against profit-driven perpetrators in the cyber world. This article introduces new malware threats such as ransomware, spyware, and rootkits, discusses the trends of malware development, and provides analysis for malware defenses.

Keywords: Ransomware, Spyware, Anti-Virus, Malware, Malicious Code,

BACKGROUND

Various forms of malware have been a part of the computing environment since before the implementation of the public Internet. However, the Internet's ubiquity has ushered in an explosion in the severity and complexity of various forms of malicious applications delivered via increasingly ingenious methods. The original malware attacks were perpetrated via e-mail attachments, but new vulnerabilities have been identified and exploited by a variety of perpetrators who range from merely curious hackers to sophisticated organized criminals and identify thieves. In an earlier manuscript (Luo & Warkentin, 2005), the authors established the basic taxonomy of malware that included various types of computer viruses (boot sector viruses, macro viruses, etc.), worms, and Trojan horses. Since that time, numerous new forms of malicious code have been found "in the wild."

MALWARE THREAT STATISTICS: A REVISIT

The Web is perceived to be the biggest carrier transmitting threats to security and productivity in organizations, because Web sites can harbor not only undesirable content but also malicious codes. The dilemma for organizations is that the Web is an indispensable strategic tool for all the constituents to collaboratively communicate, though it is also an open route for cybercriminals to seek possible victims. Unlike the past in which most malicious code writers were motivated by curiosity or bragging rights, today's IT world is experiencing the transition from traditional forms of viruses and worms to new and more complicated ones perpetrated by active criminals intent on financial gain. This trend is due to the capitalization of the malware industry where most malicious code writers tend to exploit system vulnerabilities to capture such high profile information as passwords, credentials for banking sites, and other personal information for identify theft and financial

fraud. The trend of virus attacks is that new blended attacks that combine worms, spyware, and rootkits are the major infective force in the cyber world and will likely become more frequent in years ahead. In general, such malware are spreading via increasingly sophisticated methods and are capable of damaging more effectively. Such blended malware's invention is driven by their writers' pursuit for financial fraud.

According to Vass (2007), from a hacker's perspective, the motivation for employing malware attacks has moved from "let me find a vulnerability" to "let me find an application vulnerability and automate it and put it into a bot, load up pages and reinfect the client, which I can then use to populate my bot network." Furthermore, malware writers have paid increased attention to applications and have aimed at the application layer to seek and exploit system vulnerabilities. As such, IT anti-virus teams have encountered extremely difficult predicaments regarding how to proactively prevent the malware disaster and eventually eliminate any malware infection or breach. Table 1 lists the systems and applications most often targeted for attack, and Table 2 entails the top 10 malware attacks by December of 2006.

Computer systems are now less frequently infected via passive-user downloads, because malware is increasingly embedded on Web sites to which users are lured by spammed e-mail invitations. However, e-mail attachments are still a common method of malware distribution as well. E-mail is seen as one of the biggest threats to IT community because it can easily carry malicious codes in its attachment and masquerade the attachment to entice the user's attention. Table 3 shows the top 10 malware hosted on Web sites which can easily disseminate malware infection to unwary cyber visitors, and Table 4 lists top 10 e-mail malware threats in 2007.

In addition, most malware-detection software solely recognizes malware infection by searching for characteristic sequences of byte strings which act as the malware's signature. This out-of-date detection is based on the assumption that these signatures do not change over time. However, malware writers have already

Table 1. Systems and applications targeted (Adapted from Vaas, 2007)

Target: Security Policy and Personnel • Poorly-trained employees vulnerable to phishing scams • Unauthorized devices (USB devices, etc.) • Administrative-level authority for users, who may install unapproved software, and so forth • Employees using unapproved IM and file-sharing at work (tunnel through firewalls and introduce Malware, e.g. Skype)
Target: Network Devices • Common configuration weaknesses • VOIP servers and phones
Target: Operating Systems and Core Applications • Web Browsers (especially Internet Explorer) • DLLs, Windows Libraries • Macro Infections (MS Word and Excel) • Vulnerabilities in MS Outlook and other Office apps • Windows Service Weaknesses • Mac OS X and Leopard OS • Unix Configuration Weaknesses
Target: Cross-Platform Applications • HTML and Java - Web Applications • Microsoft ActiveX controls and Javascript Activity • Database Software • P2P File-sharing Applications (Kazaa, etc.) • Instant Messaging (tunnel through firewall) • Media Players • DNS Servers (URL redirection, etc.) • Backup Software • Servers for directory management • Other enterprise servers