Evolutionary Malware: Mobile Malware, Botnets, and Malware Toolkits

Michael Brian Pope, Department of Management and Information Systems, College of Business, Mississippi State University, Mississippi State, MS, USA

Merrill Warkentin, Department of Management and Information Systems, College of Business, Mississippi State University, Mississippi State, MS, USA

Xin (Robert) Luo, Anderson School of Management, University of New Mexico, Albuquerque, NM, USA

ABSTRACT

Much as information systems themselves evolve and incorporate innovation, so too has malicious software, or “malware.” The increasing threat to those who use and trust in these systems is dangerous to overlook. This article examines recent trends in malware development. Reviewing statistics of dangerous infections of various malware families, it also expands on recent developments of actual exploit code. It further expands on the evolution of recent malware development techniques, particularly the use of malware development kits, or “exploit kits.” Mobile exploits taking advantage of smart phones, as well as malicious “polymorphic” code that self-mutates to evade detection are also discussed in detail.

Keywords: Anti-Virus, Exploit Kits, Information Security, Malicious Software, Malware, Malware Toolkits, Mobile Malware, Polymorphic Malware, Smart Phone

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 the cat-and-mouse predicament, it is widely acknowledged that, as new security countermeasures arise, malware authors always are able to learn how to manipulate the loop-holes or vulnerabilities of these technologies and can thereby weaponize new streams of malicious attacks.

From email attachments embedded with Trojan horses to recent advanced malware attacks such as Gozi programs, which compromise and transmit users’ highly sensitive informa-
tion 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 examines several strains of malware continuing to plague individuals and organizations alike, as well as touching upon some more recent trends with the use of 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. Internet-specific malware propagation was initially most common with email attachments, but new vulnerabilities continue to be identified and exploited by a variety of perpetrators who range from merely curious hackers to sophisticated organized criminals and identify thieves. Earlier examination of malware attacks (Luo & Warkentin, 2005; Luo & Warkentin, 2008) has included computer viruses, worms, and Trojan horses, as well as ransomware, spyware and rootkits. However, much as legitimate developers innovate with new code and approaches to problems, so too have new malware types perpetuated in recent years, and some old threats have become even more dangerous.

MALWARE THREAT STATISTICS: A REVISIT

The Web is perceived to be the biggest carrier transmitting threats to security and productivity in organizations, because websites can harbor not only undesirable content but also malicious code, often penetrating defenses through flaws in the operating system, browser, and accessory software. Estimates for infection sources encountered overwhelmingly named compromised or malicious web sites as the most frequent source at nearly 80% (Sophos, 2013). The dilemma for organizations is that the Web is an indispensable strategic tool for both internal and external interaction, 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 attacks proliferated 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. More complicated attacks can involve multiple malware approaches, such as a rootkit installed to allow further malware, such as spyware or ransomware, to be deployed much more easily. Once infected, the software continues to fight attempts to detect and purge it, through methods such as morphogenic code that disrupts code patterns used to detect malware, and accelerating development of malicious software, straining the resources of security firms as they press harder to keep up with new threats. Incentives and resource sources such as financial fraud make these combined and combative approaches more common, more dangerous, and more numerous.

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 aimed at the application layer to seek and exploit system vulnerabilities. As such, IT anti-virus teams have encountered extremely difficult predica-
Related Content

Resource Allocation using Dynamic Fractional Frequency Reuse: A Technique to Reduce Inter Cell Interference at the Cells Edges
[www.igi-global.com/article/resource-allocation-using-dynamic-fractional-frequency-reuse/198515?camid=4v1a](www.igi-global.com/article/resource-allocation-using-dynamic-fractional-frequency-reuse/198515?camid=4v1a)

Rethinking Realistic Wireless Network Mobility: Model and Trust
[www.igi-global.com/chapter/rethinking-realistic-wireless-network-mobility/58869?camid=4v1a](www.igi-global.com/chapter/rethinking-realistic-wireless-network-mobility/58869?camid=4v1a)
Weak GNSS Signal Acquisition for Indoor Environments
[www.igi-global.com/chapter/weak-gnss-signal-acquisition-for-indoor-environments/195723?camid=4v1a](www.igi-global.com/chapter/weak-gnss-signal-acquisition-for-indoor-environments/195723?camid=4v1a)

Capacity Limits of Base Station Cooperation in Cellular Networks
[www.igi-global.com/chapter/capacity-limits-base-station-cooperation/36547?camid=4v1a](www.igi-global.com/chapter/capacity-limits-base-station-cooperation/36547?camid=4v1a)