Chapter I
Malicious Software in Mobile Devices

Thomas M. Chen
Southern Methodist University, USA

Cyrus Peikari
Airscanner Mobile Security Corporation, USA

ABSTRACT

This chapter examines the scope of malicious software (malware) threats to mobile devices. The stakes for the wireless industry are high. While malware is rampant among 1 billion PCs, approximately twice as many mobile users currently enjoy a malware-free experience. However, since the appearance of the Cabir worm in 2004, malware for mobile devices has evolved relatively quickly, targeted mostly at the popular Symbian smartphone platform. Significant highlights in malware evolution are pointed out that suggest that mobile devices are attracting more sophisticated malware attacks. Fortunately, a range of host-based and network-based defenses have been developed from decades of experience with PC malware. Activities are underway to improve protection of mobile devices before the malware problem becomes catastrophic, but developers are limited by the capabilities of handheld devices.

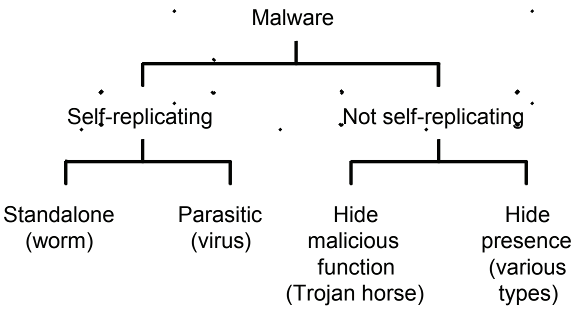
INTRODUCTION

Most people are aware that malicious software (malware) is an ongoing widespread problem with Internet-connected PCs. Statistics about the prevalence of malware, as well as personal anecdotes from affected PC users, are easy to find. PC malware can be traced back to at least the Brain virus in 1986 and the Robert Morris Jr. worm in 1988. Many variants of malware have evolved over 20 years. The October 2006 WildList (www.wildlist.org) contained 780 viruses and worms found to be spreading "in the wild" (on real users' PCs), but this list is known to comprise a small subset of the total number of existing viruses. The prevalence of malware was evident in a 2006 CSI/FBI survey where 65% of the organizations reported being hit by malware, the single most common type of attack.

A taxonomy to introduce definitions of malware is shown in Figure 1, but classification is sometimes difficult because a piece of malware often combines multiple characteristics. Viruses and worms are characterized by the capability to self-replicate, but they differ in their methods (Nazario, 2004; Szor, 2005). A virus is a piece of software code (set of instructions but not a complete program) attached to a normal program or file. The virus depends on the execution of the host program. At some point in the execution, the virus code hijacks control of the program execution to make copies of itself and attach these copies to more programs or files. In contrast, a worm is a standalone automated program that seeks vulnerable computers through a network and copies itself to compromised victims.

Non-replicating malware typically hide their presence on a computer or at least hide their malicious function. Malware that hides a malicious function but not necessarily its presence is called a Trojan horse (Skoudis, 2004). Typically, Trojan horses pose as a legitimate program (such as a game or device driver) and generally rely on social engineering (deception) because they are not able to self-replicate. Trojan horses are used for various purposes, often theft of confidential data, destruction, backdoor for remote access, or installation of other malware. Besides Trojan horses, many types of non-replicating malware hide their presence in order to carry out a malicious function on a victim host without detection and removal by the user. Common examples include bots and spyware. Bots are covertly installed software that secretly listen for remote commands, usually sent through Internet relay chat (IRC) channels, and execute them on compromised computers. A group of compromised computers under remote control of a single "bot herder" constitute a bot net. Bot nets are often used for spam, data theft, and distributed denial of service attacks. Spyware collects personal user information from a victim computer and transmits the data across the network, often for advertising purposes but possibly for data theft. Spyware is often bundled with shareware or installed covertly through social engineering.

Figure 1. A taxonomy of malicious software



Since 2004, malware has been observed to spread among smartphones and other mobile devices through wireless networks. According to F-Secure, the number of malware known to target smartphones is approximately 100 (Hypponen, 2006). However, some believe that malware will inevitably grow into a serious problem (Dagon, Martin, & Starner, 2004). There have already been complex, blended malware threats on mobile devices. Within a few years, mobile viruses have grown in sophistication in a way reminiscent of 20 years of PC malware evolution. Unfortunately, mobile devices were not designed for security, and they have limited defenses against continually evolving attacks.

If the current trend continues, malware spreading through wireless networks could consume valuable radio resources and substantially degrade the experience of wireless subscribers. In the worst case, malware could become as commonplace in wireless networks as in the Internet with all its attendant risks of data loss, identity theft, and worse. The wireless market is growing quickly, but negative experiences with malware on mobile devices could discourage subscribers and inhibit market growth. The concern is serious because wireless services are currently bound to accounting and charging mechanisms; usage of wireless services, whether for legitimate purposes or malware, will result in subscriber charges. Thus, a victimized subscriber will not only suffer the experience of malware but may also get billed extra service charges. This usage-based charging arrangement contrasts with PCs which typically have flat charges for Internet communications.

This chapter examines historical examples of malware and the current environment for mobile devices. Potential infection vectors are explored. Finally, existing defenses are identified and described.