Principles and Methods of Attack for Smartphones Virus

Wenjie Zheng

Power University Baoding, Baoding 071000, China

2893687936@qq.com

Abstract

With the rapid increase in the threat of smart phones, mobile phone virus research has been urgent. This article first briefly describes the basic knowledge of smart phone viruses, which help readers to have a preliminary understanding of mobile phone viruses. Then, the paper expatiates on the attack principle and attack mode of mobile phone virus in details and analyzes the virus attack process with the kernel level Rootkit attack technology as an example.

Keywords

smartphone, virus, rootkit technology.

1. Introduction

According to the "Statistical Report on China's Internet Development" released by the China Internet Network Information Center, as of June 2016, the number of Internet users in China reached 710 million, of which mobile phone users amounted to approximately 656 million, which increased from 90.1% at the end of 2015 to 92.5%.

While people enjoy the convenience of mobile Internet access, they also have to face the security problems caused by mobile Internet access. Once the smart phone device is connected to the network, it will be immediately exposed to the risk of a high degree of cyber threat just like a networked ordinary PC. It also poses a serious threat to the security of networked PCs, such as viruses and hackers. Slowly began to pose the same threat to smartphone devices. Attack software such as spyware, phishing, domain spoofing software, malware, browser attacks, and botnets is rapidly spreading [1]. Mobile phone viruses are being developed at a faster and faster rate, becoming the main security issue encountered by people when using mobile phones.

2. The Principles and Methods of Attacks

2.1 Conception of Mobile phone virus

The mobile phone virus is a smartphone infected object, a malicious program as a carrier, a mobile phone network as a platform, and is transmitted by sending SMS, MMS, e-mail, browsing websites, downloading ringtones, Bluetooth, etc., thereby causing the mobile phone to automatically shut down and crash. , personal information is deleted, personal information is leaked, spam is sent, calls are automatically placed, and even hardware such as chips and SIM cards are destroyed, causing the user's mobile phone to fail to function properly [2]

Some literature even believe that mobile phone virus is also a computer program [3]. In reality, cell phone viruses have almost all the characteristics of computer viruses: infectious, latent, destructive, targeted, parasitic, triggerable, unpredictable, expressive, and covert.

2.2 The Principles of Attacks

The relevant application software in the smart phone and the embedded operating system installed on the mobile phone are generally written in languages such as JAVA, C++, etc. The smart phone is equivalent to a small intelligent processor, so it is vulnerable to the invasion of the mobile phone virus. Moreover, in addition to text information, text messages sent by smart phones also include information such as ringtones and pictures. To display the information to the user, an operating system in the smart phone is required to interpret the information.

In addition to the external interfaces (USB, Bluetooth, Infrared, etc.) and the Internet, the data transmission capabilities provided by mobile operators are also a condition for mobile virus transmission and operation. Due to the existence of mobile phone software vulnerabilities, many smart phones with Internet access and downloading functions may be infected with mobile phone viruses [5].

2.3 The Methods of Attacks

Although the ultimate target of mobile phone virus is a mobile phone, it does not necessarily directly attack the mobile phone terminal itself. The current mobile phone virus attack methods mainly include:

Attack the smart phone terminal directly, making the phone unable to work

This is the most important method of infection of mobile phone viruses. At present, mobile phone viruses mainly use the bugs in mobile phone chip programs and loopholes in mobile phone operating systems to attack mobile phones. The virus will send “Virus SMS” or “MMS” to the mobile phone. When the user browses and sees the SMS and MMS, it will cause abnormalities such as shutdown, crash, and restart of the smartphone.

The continuous increase in mobile phone features, on the one hand, provides users with a better experience. On the other hand, it also provides a stage for the virus to work hard. Perhaps one day you download from the Internet is just a virus disguised as a game program. Even more frightening is that the more comprehensive the phone's functionality and the more complex the games or applications it can support, it means that it can also run more complex virus programs, and the more serious the consequences.

Attack the WAP server

WAP is the abbreviation of wireless application protocol. It can make the mobile phone easily access the Internet and complete some browsing and operating functions. If the mobile phone virus discovers some security holes in the WAP server and attacks it, the smartphone will not receive normal information.

Attack Control Gateway

Gateways are the major link between networks. We know that if there is a loophole or threat in the connection of a network, the entire network will be threatened. Just as the main connecting route of the traffic highway is damaged, the entire traffic is affected. Therefore, if some hackers write mobile phone viruses and attack them against the vulnerabilities of the gateway, once the attack is successful, the entire mobile phone network will be affected and the service of the mobile phone will also be stopped. It can be seen that the attack on the gateway will cause the mobile phone network to be more threatened and the loss caused is also huge.

Using the Internet to Attack the Smartphone Network

The use of the Internet to spread cell phone viruses has a very large impact. For example, some mobile phone viruses use e-mail or web pages to spread viruses, which is one of the ways to use the Internet to attack. In June 2000, the world’s earliest mobile phone virus “Timofonica” was the way to use the Internet. The carrier of this virus is e-mail, but it is not like the ordinary e-mail virus only sends e-mail to the e-mail address in the address book, it can also use SMS server to send large amounts of spam and poisoned text messages to the mobile phone. When the mailbox receives too much spam, the mobile phone also accepts a large number of short messages, which results in the cost of credit.

3. Kernel-level Rootkit Attack Technology Analysis of Android Platform

3.1 Preliminary knowledge

Directly attacking a smart phone terminal and making the mobile phone unable to work is currently the most important method of infection of the mobile phone virus. The following takes the Android platform Rootkit kernel-level attack technology as an example for analysis.

Rootkit technology is a direct attack on the smart phone terminal, which first appeared in the computer field. The technology that uses the highest operating system permission to hide the program process has gradually become a means to hide the traces of hackers and camouflage malicious programs. Rootkit technology needs to rely on the operating system to run, because most smart phones have used independent operating systems, which makes the rootkit virus have a platform and space for survival.

According to their different levels of operation, they can be divided into application-level rootkits and kernel-level rootkits. Application-level rootkit attacks are accomplished by modifying or replacing system tools. The kernel-level rootkit can modify or replace the underlying system kernel, such as the system call interface, system interrupt handlers, and file systems, so it can escape the detection of the application layer tools, and bring the greatest threat.

3.2 The Process of Rootkit Attack

Under normal circumstances, when the mobile phone receives the text message and the incoming call, the RIL layer reads the Modem driver file through the system call read, and then reports it to the application layer. Finally, the short message and the incoming call are displayed on the user interface.

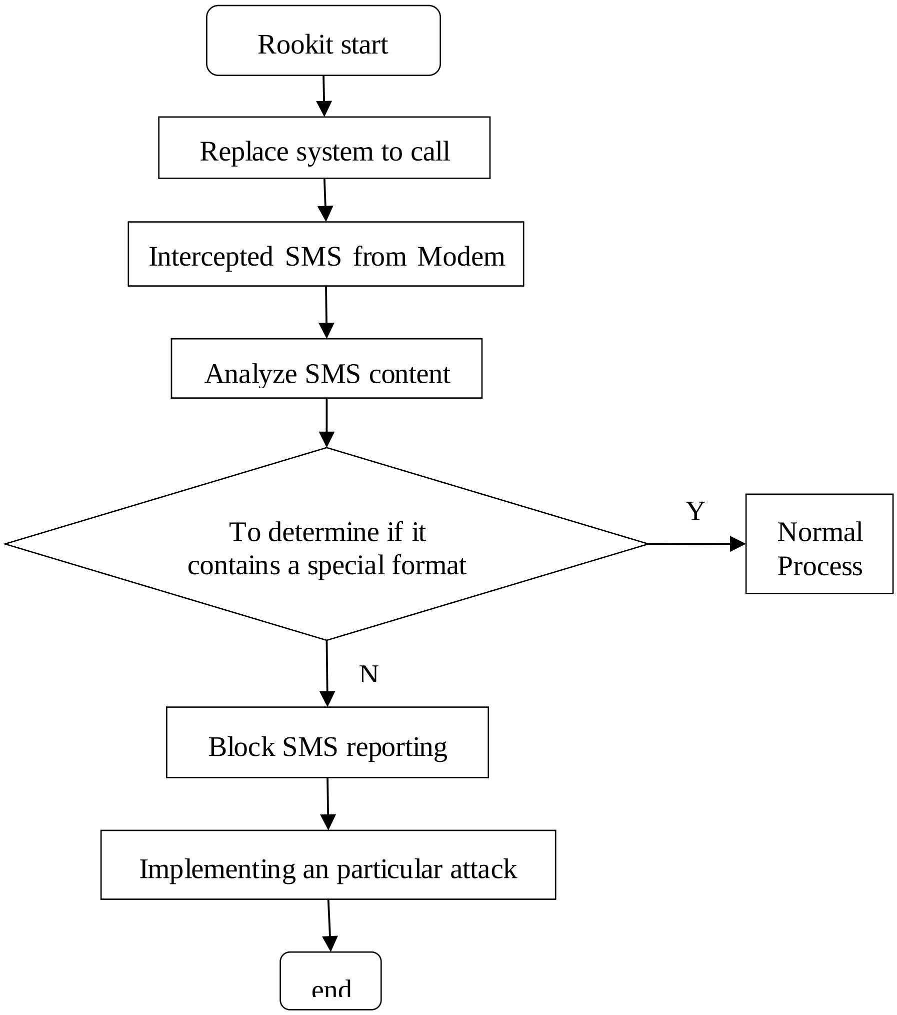
Rookit start
Replace system to call
Intercepted SMS from Modem
Analyze SMS content
To determine if it contains a special format
Y
Normal Process
N
Block SMS reporting
Implementing an particular attack
end

Fig. 1 The Process of Rootkit SMS Form Attack

Once the rootkit is successfully implanted in the mobile phone, it will begin to destroy the normal processing flow of the SMS. By replacing the system call read, the kernel-level rootkit tool can intercept SMS messages and calls reported by the Modem. Analyze the content. If it is not from the attacker's host or mobile phone, the rootkit will report to the application layer according to the normal process; if it is, the rootkit will trigger the analysis of the content of the message, triggering the application layer. Attack, or create a bounced shell, remote control of the phone.

In addition, the attacker can also use Rootkit to obtain the user's current position. [8] First, a trigger message is sent to a mobile phone that has a rootkit implanted. The message is intercepted before the message is reported to the upper application, the announcement is cancelled and the message is deleted, and then the user's position is detected using GPS and sent back to the attacker via a short message.

The rootkit virus is often installed as a driver in the kernel of the mobile system, and the core data of the system is changed by modifying the kernel code of the system. The usual anti-virus tools can only run in user mode, so the virus running in kernel mode can easily bypass the detection of anti-virus tools. Because of its good concealment, rootkit technology is becoming an important direction for mobile virus development. [9]

4. Conclusion

A large amount of research data shows that the mobile virus's propagation environment is more and more mature. The harm of mobile phone viruses is also becoming more and more rampant like computer viruses. However, people are not paying enough attention to mobile phone viruses. This will bring very serious harm to mobile phone users. It is also not too late to remedy the situation. Although mobile phone virus research is still in its infancy, as long as we increase the level of emphasis and find ways to prevent and control viruses, this will be very significant.

References

[1] Tian Wei. Research and implementation of Android mobile platform intrusion detection system [D]. University of Electronic Science and Technology, 2016.

[2] Zou Xuebiao. Research and implementation of intrusion detection system based on smart phone[D]. Wuhan Institute of Posts and Telecommunications, 2014.

[3] Liu Yijing, Sun Ying, Yu Yang. Research on mobile phone virus attack[J]. Information Security and Communications Security, 2007,(12):96-98. [2017-10-13].