Agnieszka Rachwał[1]

Rootkits

Introduction

Every computer user knows what a computer virus is, and what kind of danger it brings. An avarage user knows also about trojan horses, worms or spyware. However, not every user heard about rootkits. These small applications - which are still not talked about much enough – appear to be the most vicious type of maleware. Concealed, invisible, hardly detectable can sit in infected system for months stealing our information. What are they, how do they work, how to protect our system from them, and finally how to get rid of them – this are questions I try to answer in present article.

What is rootkit?

IT people from The University of Minnesota at their site *safecomputing.umn.edu* define rootkit as a special kind of malware that is specifically designed to hide the activities of other viruses and worms, and compromise the operating system so that it may not be repaired. In their opinion if your machine is infected with a rootkit, you will very likely not be able to regain complete control of the system, and hence reinstallation is highly recommended[2]. Rootkits have their origin in relatively benign applications, but in recent years have been used increasingly by other malware to help intruders maintain access to systems while avoiding detection. Rootkits exist for a variety of operating systems, such as Linux, Solaris and versions of Microsoft Windows. Rootkits often modify parts of the operating system or install themselves as drivers or kernel modules[3].

Origin

Wikipedia says that the term "rootkit" (also written as "root kit") originally referred to a set of recompiled Unix tools such as "ps", "netstat", "w" and "passwd" that would carefully hide any trace of the intruder that those commands would normally display, thus allowing the intruders to maintain "root" on the system without the system administrator even seeing them[4].

---

[1] Graduate of University of Silesia, Faculty of Computer Science and Materials Science.

[2] Source: *http://safecomputing.umn.edu/guides/scan_unhackme.html* [access: 1 of July 2007]

[3] Source: *http://en.wikipedia.org/wiki/Rootkit* [access: 1st of July 2007]

[4] Source: *http://en.wikipedia.org/wiki/Rootkit* [access: 1st of July 2007]

Ed Tittel and Justin Korelc in their article titled „Rootkit levels of infection and mitigation" explain that today, the term rootkit is separated from operating system dependency. While a strong security implementation can help mitigate the effectiveness of rootkit installation, removal of such malware is - unfortunately - an inexact science, and usually requires a drive format and full re-installation of the original operating system to ensure a clean and proper restoration[5].

Methods of infection

Methods of infection are the same as in case of other kinds of maleware (e.g. viruses or trojan horses), thus you should be cautious while surfing in the Internet as this is the major source of unwanted, malicious programs. Your computer is especially vulnerable to attack if you:

– download/share files;
– use network which is not secure enough;
– install applications coming from unknown sources.

At NCComputerTech website we can read that although rootkits have been around for a long time in the Unix world, experts predict they are going to be used more and more for malicous intent on the Windows platform. While there're programs that can discover a rootkit, removing it without destroying crucial data is usually a different story. Even programs that claim they can find a rootkit and remove them safely from your system aren't guaranteed to work[6].

According to Kurt Dillard, program manager from Microsoft, in order to install a rootkit on a system, an attacker must somehow compromise it and gain administrator privileges. He will attempt to accomplish this in a variety of ways. He can:

- trick a user into executing malicious code that's embedded in what appears to be a benign download from the Web, such as a game, screensaver or file sharing utility
- figure out an easy-to-guess password
- take advantage of a missing security hotfix
- exploit a poorly configured system
- install his rootkit once he gains control of the system

- wrote Dillard in his article "How does an attacker install a rootkit?"[7].

---

[5] Source: *http://searchenterpriselinux.techtarget.com/tip/0,289483,sid39_gci1149598,00.html* "Rootkit levels of infection and mitigation" Ed Tittel and Justin Korelc [access: 1st of July 2007]

[6] source: *http://www.nccomputertech.com/rootkit.htm* [access: 1st of July 2007]

[7] source: *http://searchwindowssecurity.techtarget.com/originalContent/0,289142,sid45_gci1086466,00.html* [access: 1st of July 2007]

Symptoms of infection

NCComputerTech[8] provides us with some examples of potential infection symptoms:

- Excessive network traffic
- Free space on the hard drive not being reported accurately or missing
- Random lockups
- Anti virus program no longer runs
- Windows settings have changed
- Weird sites showing up in Trused Internet Sites in IE
- Folders showing up with long HEX names
- Folders showing up with illegal files in them..i.e. programs, games, movies, audio files
- Services running that you do not recognize or haven't noticed before

How does rootkit work? What rootkit can?

The concealment aspect is what distinguishes rootkits from other types of malware, and it's what makes them so difficult to detect and remove, says Kurt Dillard. He warns that rootkits can provide the attacker with a backdoor for future attacks, launch and hide other applications, and gather sensitive data to be collected by the attacker at a later time[9].

According to Wikipedia a rootkit's **only** purpose is to hide files, network connections, memory addresses, or registry entries from other programs used by system administrators to detect intended or unintended special privilege accesses to the computer resources. However – we are reading - a rootkit may be incorporated with other files which have other purposes. It is important to note that the utilities bundled with the rootkit may be malicious in intent, but a rootkit is essentially a technology; it may be used for both productive and destructive purposes[10].

From further part of the article we learn that a rootkit is often used to hide utilities. These are often used to abuse a compromised system, include so-called "backdoors" to help the attacker subsequently access the system more easily. For example, the rootkit may hide an application that spawns a shell when the attacker connects to a particular network port on the system. Kernel rootkits may include similar functionality. A backdoor may also allow processes started by a non-privileged user to execute functions normally reserved for the superuser. All sorts of other tools useful for abuse can be hidden using rootkits. This includes tools for further attacks

---

[8] source: h*ttp://www.nccomputertech.com/rootkit.htm* [access: 1st of July 2007]

[9] source:

http://searchwindowssecurity.techtarget.com/originalContent/0,289142,sid45_gci1086469,00.html

[access: 1st of July 2007]

[10] source*: http://en.wikipedia.org/wiki/Rootkit*

against computer systems which the compromised system communicates with, such as sniffers and keyloggers. A possible abuse is to use a compromised computer as a staging ground for further abuse. This is often done to make the abuse appear to originate from the compromised system or network instead of the attacker. Tools for this can include denial-of-service attack tools, tools to relay chat sessions, and e-mail spam attacks. A major use for rootkits is allowing the programmer of the rootkit to see and access user names and log-in information for sites that require them. The programmer of the rootkit can store unique sets of log-in information from many different computers. This makes the rootkits extremely hazardous, as it allows trojans to access this personal information while the rootkit covers it up.

Rootkits are not always used to attack and gain control of a computer. Some software may use rootkits to hide from 3rd party scanners to prevent detection or tampering. Some emulation software and secure software is known to be using rootkits. Alcohol 120% and DAEMON Tools are commercial examples of the use of non-hostile rootkits – conclude authors[11].

Types of rootkits and list of the most popular

Kernel mode

Kernel mode rootkits works inside the system kernel. They can add or replace its original code with modified one in order to hide malicious processes and to take control over the system. In Windows family systems infection with rootkits is usually accompanied by installing device drivers. Since device drivers – to be able to function correctly - need an access to basic system resources, it is the easiest way for intruder to install rootkit on remote system. Thus, we should be cautious while deciding to use device drivers from unknown sources. In case of Linux, rootkit may be installed via loadable modules (Linux Loadable Kernel Modules).

This kind of rootkits is very difficult to detect only when written correctly. Any mistakes in code may result in system instability, crashes, and Windows bluescreens. Such extraordinary situation usually makes user suspicious, and forces him to scan the system with appropriate software. This is the reason why kernel rootkit is very difficult to create.

User mode

User-mode rootkits run as separate application or within an existing one. They tend to intercept system calls to API in order to modify the API's output results. Having control over these output results, rootkits can remove from the returned list of processes and files any entries that could identify their existence in the system. In consequence, user recives filtered, uncomplete list of files and processes which unable him to realize that the system is victimized.

[11] source*: http://en.wikipedia.org/wiki/Rootkit*

This kind of rootkit can only conceal itself from user-mode tools. It cannot hide itself from kernel-mode tools.

Application mode

This kind of rootkit doesn't have any access to system kernel. As its name indicates, it operate on different application binary files. Rootkit replace original ones with those modified by itself. In this way rootkit can have influence on functioning of other applications.
The most widespread application mode rootkit is persistent Hacker Defender.
They intercept system calls and filter output application programming interfaces (APIs) to, for example, hide processes, files, system drivers, network ports, registry keys and paths, and system services.

Persistent Rootkits

Persistent rootkits are relatively easy to detect because of their open, permanent presence in a system. Their code files are usually stored on hard disk. Persistent rootkits change registry entries, influence system files, and introduce such system configuration changes which allow them to be launched automatically along with system start.

Memory-based rootkits

Memory-based rootkits exists only in volatile memory and they may be installed secretly via a software exploit. Although reboot removes them completely from system, they should not be ignored. There are two reasons why they are worth our attention. First of all, they are hard to detect, as rootkit-detecting software scan only content of hard disk. Hence, they cannot be found while existing in volatile memory. Secondly, server systems hardly ever are rebooted. They remain online for weeks, or months. In practice, such rootkit has great condicions to stealthy operate in infected system. The most reliable way of detecting memory-based rootkit seem to be by creating memory image which can be made with help of special special tools e.g. Tribble, CoPilot or RAM Capture Tool.

Detecting

As I have already mentioned, rootkits are the most difficult to detect kind of maleware. They conceal themselves effectively from antimaleware software, and what is more, sometimes they can even switch it off In victimized system it is rootkit who controls any processes, applications, API results or intercepts system calls. Such system cannot be trusted, it is not reliable. Therefore traditional anivirus applications or other kinds of maleware scanners simply fail. We need to use different ways of system examination.

The most often used detection technolody is cross-checking, where 2 lists of files from the folder are compared: one - returned by operation system's API, and second one - read directly from file system. The register in Windows system is verified in the same way (result from API and directly from registry file). In clear system both results should be the same, records existing at second list, and not returned by API, are probably concealed by rootkit.

Other method is comparing binary programs code or dynamic libraries (DLL) at hard drive, and right after loaded them to operation memory. In some cases modification of executive code in operating memory is result of rootkit actions.

The best and most reliable method for rootkit detection is to boot computer from different media, for example rescue CD-ROM or USB flash drive. Ideal solusion is booting from live CD which contains antivirus program along with up-to-date signatures. Example of such tool is G Data Internet Security 2007. After booting from CD and launching Linux OS, we can connect to the Internet in order to update virus base of enclosed on CD antivirus application. Since we do not boot system from hard disk rootkit cannot be launched. And a non-running rootkit cannot hide its presence from appropriate software.

According to Wikipedia, security vendors envision a solution by integrating rootkit detection into traditional antivirus products. Should a rootkit decide to hide during the scan process, it will be identified by the stealth detector. If it decides to temporarily unload from the system, the traditional antivirus will find it using fingerprint detection[12].

In some cases, especially if rootkit is commonly known, traditional antivirus or antirootkit software can be successful in identyfying and removing malicious applications. Here are the most popular detecting programs:

- Chkrootkit
- F-Secure BlackLight
- Gmer
- IceSword
- Microsoft Strider GhostBuster
- Rkhunter
- Rootkit Revealer
- Sophos Anti-Rootkit
- Spy Sweeper
- System Virginity Verifier

Bad news is that many rootkits are tailor-made for particular system. It means they were written on purpose to steal informations from particular system or to do some damages to the system. Such rootkits are almost impossible to detect for traditional scanning software.

[12] source: *http://en.wikipedia.org/wiki/Rootkit* [access: 6th of July 2007]

Another method is to encrypt “clean” system install disks. Cryptography appears to be very helpful in monitoring data integrity. “By ‘fingerprinting’ the system files immediately after a fresh system install and again after any subsequent changes made to them (e.g. installing new software), the user or administrator will be alerted to any dangerous changes to the system's files. In the "fingerprinting" process a cryptographic hash function is used to create a fixed-length number which is dependent on every bit of data contained in the file being "fingerprinted". By calculating and comparing hash values (the "fingerprint") of files at regular intervals, changes not made by any intended user of the system can be detected” – says Wikipedia[13].

Removing

There are three ways of getting rid of rootkit from infected system: using special software, using another filesystem driver or simply re-istalling system from scratch.

The most radical solution – system reinstalation - is consider to be the most practical. Even if system administrator is experienced and possess all necessary skills to remove rootkit from system by using other methods, it would take him too much time and effort to fix the system in this way. There so many applications allowing to make drive images and restore OS in few minutes that there is no sensible reason not to take advantage of those benefits they give, even if we know composition of the rootkit, and the way of whipping it out.

But what if we did not make drive image, and cannot decide on system reinstalation in fear of losing important data? We can try to reapair system using one of special programs, such as for example UnHackMe or Gromzon Rootkit Remover. Bad news is that software like this cannot guarantee a success in handling our problem. It is often ineffective, and fails to remove rootkit or even to idetify it. However, it is good to try this option out. Sometimes they can really help.

The last option I mentioned about it is to use another filesystem driver while the system is online. Program Rkdetector v2.0 implements a way to wipe hidden files when the system is running using its own NTFS and FAT32 filesystem driver. Rkdetector includes: filesystem scanner, data recovery, secure data deletion, ADS scanner, and registry analyzer. Application is run from command line. After hidden tasks are identified Rkdetestor will try to kill them, and then rescan service database in order to detect hidden services installed by intruders and hidden regkeys. After system reboot, rootkit files will not be loaded because data contained is corrupted.

[13] source: *http://en.wikipedia.org/wiki/Rootkit* [access: 6th of July 2007]

Conclusions

Among all malaware tools rootkits seem to be the biggest problem for computer users. They are almost undetectable, and have great possibilities to harm and control our system. The best way to protect ourselves against rootkits is – like in case of all other maleware – prevention. Regular system updates, good antivirus program, firewall, not opening any application for unknown sources etc.

Bibliography

1. http://pl.wikipedia.org/wiki/Rootkit html [access. 4th of January 2007]
2. http://safecomputing.umn.edu/guides/scan_unhackme.html [access: 1st of July 2007]
3. http://searchenterpriselinux.techtarget.com/tip/0,289483,sid39_gci1149598,00.html "Rootkit levels of infection and mitigation" Ed Tittel and Justin Korelc [access: 1st of July 2007]
4. http://searchwindowssecurity.techtarget.com/originalContent/0,289142,sid45_gci1086466,00.html [access: 1st of July 2007]
5. http://www.nccomputertech.com/rootkit.htm [access: 1st of July 2007]
6. http://www.pcworld.pl/news/75985.html [access. 4th of January 2007]
7. http://www.securitystandard.pl/news/85231.html html [access. 4th of January 2007]
8. http://www.viruslist.pl/glossary.html?glossid=29 html [access. 4th of January 2007]

Rootkits

Abstract

Rootkits are set of malicious tools created by intruder in order to achive unauthorized access to remote system, and to take total control over it. Unlike other maleware applications, rootkits are very difficult to detect due to their concealed existance. They hide both themselves and other malicious applications (e.g trojan horse or keylogger) to allow attacker to steal important data or do some damages to the victimized system. Rootkits remove any records about themselves from actual process list and from files list returned by API. Hence, they are invisible to antivirus scanners or to system administrator's eye. Depending on type of rootkit it may constantly exist on hard disk (persistent rootkit), stay in volatile memory (memory-based rootkit), may modify other application's binary files (application mode rootkit), intercept system calls to API (user mode rootkit), do some changes in system registry or file system or even modify system kernel (kernel-mode rootkit).

Since system infected with rootkit cannot be trusted, any attempts of detections of this maleware with tradicional antivirus software in most cases fail. The best method to detect rootkit is cross-checking where two lists of files in directory are compared: one returned by API, and one read directly from file system. Alternative way of detection is also comparing binary files or dynamic libraries read from disk with loaded to operation memory ones. Scanning potentially infected hard disk from system launched on different media (e.g. rescue CD) is also very effective. Finally, there are some special diagnostic tools available. However, they are not always successful.

Once we discover rootkit in a system, the easiest way to handle it is via system reinstalation. Manual removing or removing it with special application is usually more complicated, and not always effective.