Defeating Rootkits and Keyloggers

Today, one in seven malware programs use rootkit technology to obfuscate their actions. According to McAfee, by 2008 over 84% of all malware are expected to be disguised by rootkits.

Keyloggers and rootkit based malware are viewed as the kings of malware. They are:

- Hardest to detect and remove,
- Capable of causing considerable damage to the network infrastructure, and
- Pose an unprecedented risk to personal information.

For example, the SONY rootkit went undetected by firewalls and all anti-virus software. It was able to spy on users and created loopholes that other hackers were able to exploit.

The current generation of the anti-virus and anti-spyware products has proven hopelessly inadequate in detecting, removing, and blocking rootkits and keyloggers. This is because the defense principles relied upon by these products can be trivially bypassed by rootkits and keyloggers.

What are Rootkits and Keyloggers?

A rootkit is a tool to conceal information. Malware can use rootkits to actively hide, escape detection, and to enable a hacker to remotely control the computer. There are two types of rootkits, “kernel mode” and “user mode” rootkits. User mode rootkits are more common, but kernel mode rootkits are much more difficult to detect or remove.

A keylogger can be an application, or a kernel driver, or a dll inside an application that records keyboard strokes. They are often used to steal private information, e.g. passwords, credit card or bank account numbers, etc.

How Computers Get Infected With Rootkits and Keyloggers?

Two main methods used to infect computers with Rootkits and keyloggers are:

- Bundling rootkits and keyloggers with other software
- Exploiting application (web browser, IM, or e-mail) vulnerability

A significant fraction of free software available on the web has been maliciously modified and bundled with rootkits and keyloggers. When someone downloads software from a less reputable site and installs it, there is a high probability of getting infected with rootkits and keyloggers along with other spyware and malware. If proper controls are not exercised to prevent users from freely downloading software from the web, the risk exposure for the enterprise will increase.

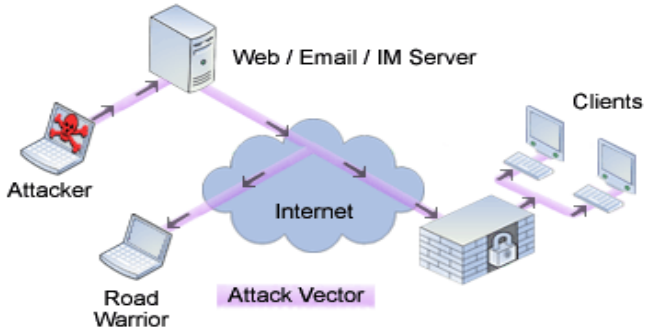
Another method used to infect computers with rootkits and keyloggers is via application exploits. It is relatively easy to exploit a known vulnerability of the application to gain

unauthorized access. Applications such as web browsers, IM clients, VoIP clients, e-mail etc. provide a direct, even real time, window into the enterprise environment.

The windows metafile (WMF) exploit is a good example. In this case, computers were getting infected via banner ads even though the user was browsing a reputable and legitimate Web site. The year 2005 saw largest increase in infections propagated via application exploits.

Computers can get infected with rootkits by

- Downloading compromised software
- Visiting a compromised/malicious site that exploits a known vulnerability
- Malicious e-mails or IM messesges



Importance of Detecting and Removing Rootkits/Keyloggers

Nobody wants spyware on their network, let alone a rootkit or a keylogger. A hacker or competitor gaining unauthorized access to critical corporate information, via the use of rootkits or keyloggers, can have very negative consequences for the corporation. Loss of corporate or customer data because of rootkits or keyloggers infestation has additional legal consequences for the corporation and can irreparably tarnish their image. Ability to detect, remove, and prevent rootkits is business critical.

Technical Challenge in Detecting and Removing Rootkits/Keyloggers?

The most common method used against malware is “Scan and Clean.” Rootkits and keyloggers use four methods to defeat the “Scan and Clean” approach’

- Polymorphism
- Stealth
- Regeneration
- Disabling anti-malware application

Because the “Scan and Clean” approach is based on signatures derived from an observed specimen of the rootkit/keylogger, morphing the code can easily evade detection.

The second method to evade detection is "Stealth." You cannot judge what you cannot see. This method is what separates most other malware from rootkit based malware. Rootkit technology can make malware "invisible" and evade detection. By modifying applications or even the OS kernel, rootkits malware can become nearly impossible to detect and remove. Even if a rootkit malware is detected, it can prevent its removal by regenerating itself or by attacking and disabling the anti-malware solution.

Advantages of Trlokom's Solution

Trlokom's SpyWall Web browser sandbox is the first comprehensive solution that addresses all aspects of the rootkit and keylogger problem:

- Detection (Of even the most well hidden ones)
- Removal (Even if they try to regenerate)
- Prevention (Keeping them out is the best solution)

If a computer gets infected with a new rootkit malware or keylogger for which definitions are not available, SpyWall will still detect it based on behavior analysis at the application and kernel layer. Behavior analysis technique includes "deduced behavior" and "observed behavior" analysis to catch rootkits or keyloggers without using signatures.

SpyWall finds hidden files, registries, processes, keyloggers, unauthorized hooks etc. It also performs application and kernel audit to find rootkits hidden deep inside the kernel.

If a rootkit malware is detected, SpyWall uses its patent pending sandbox architecture to neutralize the rootkit and takes away its ability to regenerate or launch counterattacks. Thus the system can be restored to its healthy and rootkit free state in just four easy steps. The steps are rootkit scan, initiate lockdown, delete rootkit signatures, and reboot.

Trlokom's solution even prevents rootkits from entering the computer. It nips the rootkit problem in the bud and closes the biggest security threat to the enterprise network, i.e. Web access. According to a survey by TrendMicro, an overwhelming majority of attacks are web based and take place via the web browser.

SpyWall comprehensive protection also includes:

- Preventing 0-day exploits via Web browser (responsible for 85% of the attacks)
- Detailed monitoring of web usage (easy to read charts on hourly web usage)
- Web site blocking (prevent employees from visiting sites like MySpace.com)
- Spyware scan and clean (it even removes spyware like Aurora and CWS)
- Exercising control over files downloaded from the Web
- Strong central management capabilities for remote installation and management

The leading edge and patent pending technology used by SpyWall will not only detect and remove rootkits, but it will ensure that the computers do not get infected.

Additional Resources

Download links:

SpyWall client : www.trlokom.com/my/download/spywall_installer.exe
Central manager : www.trlokom.com/my/download/rm_installer.exe

For further details:

Send e-mail to info@trlokom.com or visit www.trlokom.com

626-357-3706
602 E. Huntington Drive, Suite F,
Monrovia, CA 91016
USA