

Rooting Out Rootkits

By Ken Dunham

Windows rootkits are increasingly common in the wild since December 2005. Administrators are now battling rootkit codes on a daily basis and frequently do not have the skills required to properly identify and remove such code from a system. This article provides a brief introduction to Windows rootkits and highlights free-ware tools of great value to Windows administrators in battling rootkits in the wild.

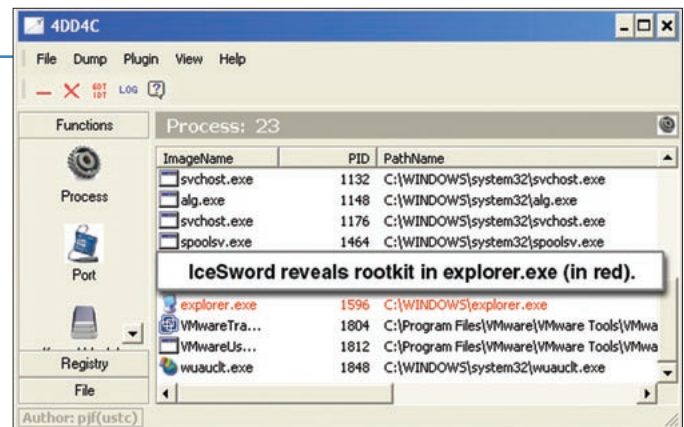
Rootkits attempt to conceal the presence of code on a computer. This concealment may be legitimate or illegal. For example, anti-virus software may use rootkit technology to undermine and detect a malicious rootkit installed on a computer illegally. The term rootkit stems from Unix systems, where an attacker traditionally installed modified programs or scripts (a kit) to maintain root on a computer. Some researchers also define rootkits as part of an ability to initiate an attack or compromise a computer. Today most rootkits are developed for the Windows operating system, bundled with other malicious codes for criminal gain.

In December 2005 a significant spike of activity in the prevalence of Windows rootkit families took place. At this time source code for rootkit functionality became popularized within multiple codes. One of the first families to use it on a regular basis, with great success, is the Feeps worm family and several bots in early 2006.

Many administrators now need training on how to identify and remove Windows rootkits. Early efforts arose with free-ware products like Rootkit Revealer and BlackLight. Today there are many products, of which some perform better than others. Additionally, rootkits like Rustock are specifically designed to undermine most of the anti-rootkit programs in the wild. As a result no single program “does it all” and a collection of scanning and analysis tools best enables an administrator to identify potential rootkit code on a Windows computer today.

A list of freeware anti-rootkit programs for Windows is below. There are other programs also available, such as the anti-rootkit components of the Encase Enterprise product (commercial software), and private anti-rootkit programs not available to the general public. Tools listed below are freely available and robust enough to deal with most Windows rootkit incidents in the wild to date:

AVG Anti-Rootkit – <http://free.grisoft.com/doc/5390/lng/us/tpl/v5#avg-anti-rootkit-free>



IceSword detects an injected rootkit in Explorer.exe.

BitDefender AntiRootkit – <http://beta.bitdefender.com/login.php>

BlackLight – <http://www.f-secure.com/blacklight/>

GMER – <http://martijn.be/tools/mieeeeeeeeeeeeeeeep/gmer.htm>

IceSword – http://202.38.64.10/%7Ejfan/download/IceSword120_en.zip

DarkSpy – <http://www.rootkit.com/newsread.php?newsid=474>

RKDETECTOR – <http://www.rkdetector.com/>

RKUnHooker – http://rku.nm.ru/rkunhooker_v3/RkU3.31.150.420.rar

RootKit Hook Analyzer – <http://www.resplendence.com/hookanalyzer>

RootkitRevealer – <http://www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.msp>

Sophos Anti-Rootkit – <http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html>

IceSword is the best analysis tool listed above, able to detect ports, processes, files, registry and more. For example, it color-codes suspected rootkit components and is able to detect processes (shown above), ports, registry, file, and similar changes made by rootkits.

BitDefender is one of the fastest as a scanner. If these programs fail to detect rootkits on a system, mounting the drive is a sure fire way to identify rootkit-protected changes on a compromised system.

About the Author

Ken Dunham, CISSP, GREM, GCIH, is Director of the Rapid Response Team at iDefense – A VeriSign Company. Ken can be reached at ken@kendunham.org.