

Dangers of Rootkits

If an approach to endpoint security does not include anti-rootkit strategy, then it will fail. If the security solution cannot confirm or rule out the presence of a rootkit on a computer, it is no better than playing Russian roulette.

Rootkits pose an especially big challenge because they go undetected from anti-virus scans. Most IT administrators take it for granted that deploying anti-virus on the desktops and servers is the final answer to their endpoint security needs. More savvy organizations know that relying only on the anti-virus products for endpoint security has severe shortcomings and they deploy additional network or endpoint-based security solutions to improve their security coverage.

Because of limitations of the anti-virus technology, most anti-virus vendors are providing additional tools to detect rootkits, and even these tools are not sufficient.

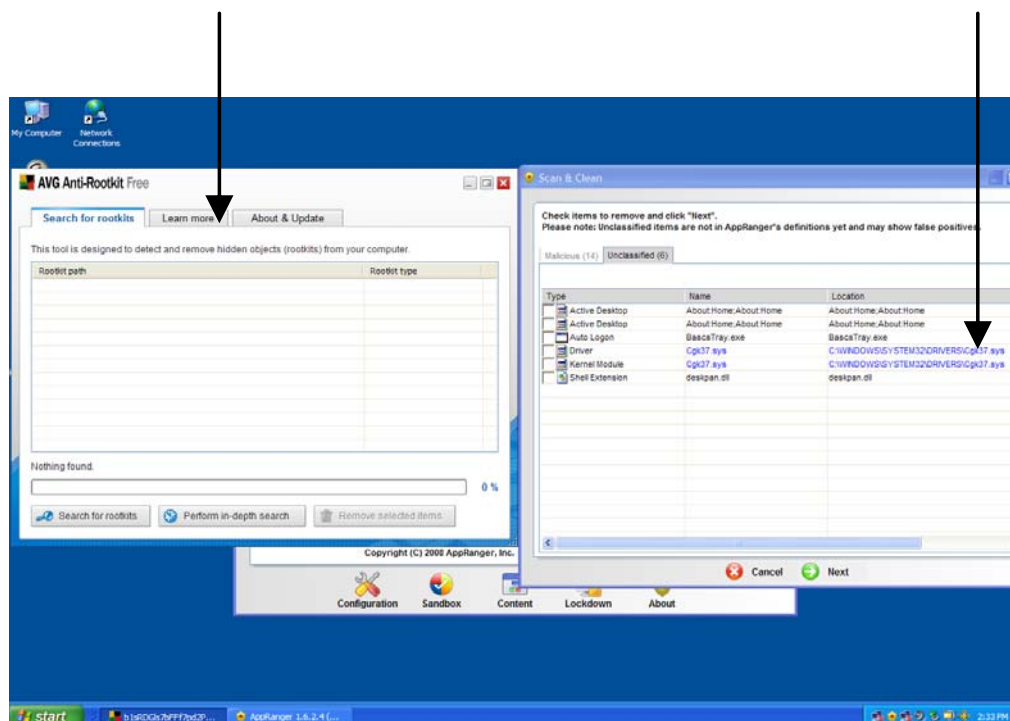
Picture below shows scan results of an infected computer by one such anti-rootkit tool and by AppRanger

The anti-rootkit tool does not detect any rootkit components.

AppRanger scan exposes the hidden rootkit driver.

Anti-virus tool scan does not find rootkit components

AppRanger finds rootkit components



AppRanger Exposes All Rootkits

AppRanger uses a patent pending technology that can expose any rootkit and it is the only product that has 100% rootkit detection rate. AppRanger can provide a definite answer if a computer is infected or free of rootkits.

AppRanger provides comprehensive endpoint protection by:

- Protecting applications
- Enforcing lockdown
- Rootkit detection and removal

Even if a malware manages to run on the PC, it will be detected by AppRanger and will not be able to cause any damage.

To download a 30-day trial version of AppRanger, please visit:

www.appranger.com/try.php

To learn more about AppRanger, please visit:

www.appranger.com