

This story appeared on Network World at <http://www.networkworld.com/research/2008/081108-rootkits.html>

How to root out rootkits

By Deb Radcliff , Network World , 08/11/2008

Find out how and where they hide, what they're hiding, and how you can (and can't) stop them

If you want to know about the latest malicious rootkit, ask security researcher [Dino Dai Zovi](#). He'll tell you all about his proof of concept rootkit called Vitriol that uses virtual machine instructions in [Intel](#) processors to hide a rootkit at the [virtualization](#) layer.

He presented this information at BlackHat 2006, the same conference at which Joanna Rutkowska demonstrated her BluePill virtual rootkit that exploited [AMD](#) processors.

The good news is that neither rootkit has shown up in the wild. And Dai Zovi says such a hack is not imminent. The bad news: Dai Zovi says these hacks haven't been unleashed on unsuspecting enterprise networks because existing rootkits are working so well, there's no need for hackers to develop these more devious attacks.

Related Content

"If I'm an attacker and my user and kernel rootkits work 80% of the time, then why go create a virtual rootkit, which is infinitely harder to deploy?" asks Mike Dalton, CTO at [Revelogic](#).

That's not to say hackers are resting on their laurels either. User and kernel-level rootkits continue to get more insidious, burrowing deeper into enterprise networks, hiding themselves in the processor, and exploiting multi-processor systems for gaming-based hacks.

And, although it's hard to say how prevalent rootkits are because they're so darn hard to find, one need only look at the rate of rootkits being used in families of profit-driven malware – most commonly to hide remote-controllers, keyloggers, spambots and gameware.

Rootkits of all evil

"The use of rootkit technologies is prevalent in the malware families our filters are picking up today," says Christoph Alme, Secure Computing's antimalware team lead. "Most commonly these tend to be spambots. Recent examples include Srizbi and Rustock."

Detected in the wild in 2007, Rustock.C spreads like a virus to infect kernel drivers, uses polymorphism (self-changing) to avoid signature detection, loads and hides beneath Microsoft's trusted system driver, and includes a back door Trojan to open and hide two-way communications channels over Port 80.

When analyzed at Rootkit.com this year, Rustock.C was called the "most powerful rootkit ever found under Windows" because of these and other advanced hiding features. The analysis went on to predict that Trojans (back doors) and rootkits will ultimately blend into one malware family.

By combining such hiding technologies, rootkits such as Rustock.C can easily cloak a bot's existence not only from the system, but from the network, where monitoring for suspicious machine behaviors is the last line of defense in detecting the possible presence of rootkit-infected systems.

"Companies need to keep Port 80 open so their employees can use the Internet. Some malware uses that channel to piggyback HTTP traffic," Alme says. "HTTP traffic mainly goes inbound [rather than outbound] over this port, so you need to train your filters to scan outbound HTTP traffic with your network gateway appliance."

Malicious traffic can also piggyback on accepted outbound traffic – for example attaching to outbound DNS packets. So Alme also recommends monitoring these types of outbound channels for bursts of traffic, large files and other anomalies that might indicate remote control commands are being sent and received.

Traditionally, detecting a rootkit on a system can be even more difficult than detecting rootkit-hidden traffic on the network, because the rootkit always had as high or higher privilege than antivirus software, Dalton says.

Related Content

However, VMware's recent addition of antivirus support with their new VMSafe extensions allows antivirus products to run with VMM (virtual machine monitor, aka hypervisor) protection, at higher privilege and visibility into the kernel.

"It's always been a game of cat and mouse with antivirus looking for rootkits and rootkits looking for antivirus, so the rootkit can take control of the security software and continue controlling the infected computer," Dalton says. "Now, by putting security in the Virtual Machine Manager, a kernel rootkit can't even find the security to disable it."

Rootkit toolkit

Rootkit-specific tools such as [F-Secure's](#) BlackLight and RootkitRevealer look for discrepancies between the kernel system calls and direct inspection of the disk to detect hidden files, registry keys and other properties, Dai Zovi says. For example, on a Windows machine, they work by looking for discrepancies between Windows Task Manager process list and the internal system task list.

Note, however, that these tools also operate at a lower level of privilege than the rootkit.

"Rootkit defenders running in user-land are trying to do dynamic analysis of the machine to see whether the machine itself is lying. Now does that sound smart?" asks Gary McGraw, CTO of [Cigital](#), and editor of the definitive book, "Rootkits", by Greg Hogg and James Butler.

Digging deeper

The newest kernel rootkits, containing all types of malicious packaging, can also jump to processors and reboot back into the kernel at bios – even after a computer's been cleaned and restored. Bios is the first place software starts to run, finds its startup routines such as Ethernet and flash/ROM bios extensions.

Dai Zovi says this type is called a "persistent" rootkit. Researcher John Heasman debuted such a rootkit at BlackHat 06 that hides in the Advanced Configuration and Power Interface. Heasman has also discussed similar techniques against the System Management Memory, which two researchers from Clear Hat Consulting were slated to demonstrate at last week's BlackHat.

"If you can control the processing on a computer, how do you monetize that? You sell bots for spam, identity theft and [distributed denial of service]," McGraw says. "But the most efficient way to exploit processors for money is in online games. This is where the cutting edge of bot technology is being carried out."

Game bots are particularly fond of multiprocessors over which can be run multiple threads while balancing load, continues McGraw, who's also co-author of "Exploiting Online Games." The more games organized criminals can play or steal through automated bot programs, the more virtual goods they can acquire and sell for real money.

There are many paths from the kernel that rootkits can take advantage of to exploit the firmware – boot loaders, device drivers, flash and firmware updates, says Bill Johnson, president and CEO of TDITX.com.

"Hardware [security](#) is not something most security technologists understand well," he adds. "It's an area they'd better get familiar with."

His company's infrastructure management tool, ConsoleWorks, logs and audits what's happening on the Baseboard Management Controller portion of the processor, which is the gateway interface into the rest of the processors on the motherboard. It manages this layer with VPN authentication and access.

[Microsoft's acquisition in March of Komoku](#) is also an indicator of deeper inspection technologies eventually coming to market. Backed by the Defense Advanced Research Projects Agency, Department of Homeland Security and the Navy, Komoku's technology and its brain trust are being absorbed by [Microsoft's](#) ForeFront and OneCare antimalware projects, says a Microsoft spokesperson.

And so rootkit technologies drive security deeper, as the game of cat chasing mouse continues.

"It's foolish to believe that we'll ever be able to make systems completely invulnerable to attack," Dai Zovi says. "However, we must make them secure enough that attacking them is not worthwhile for most criminals."

Radcliff is a freelance writer in California. She can be reached at deb@radcliff.com. All contents copyright 1995-2008 Network World, Inc. <http://www.networkworld.com>