Malicious Bots Hide Using Rootkit Code

By *srlinuxx*
Created *18/05/2005 - 1:24pm*
Submitted by srlinuxx on Wednesday 18th of May 2005 01:24:39 PM Filed under Security [1]

Computer viruses and remote control programs called bots are adopting features from stealthy programs called rootkits to avoid detection, according to researchers at Finnish anti-virus software company F-Secure.

New versions of Rbot, a malicious and ubiquitous remote control program, have features copied and pasted from a well known open-source rootkit called FU. The new features make Rbot invisible to system monitoring tools.

This is just the latest example of malicious programs borrowing strategies used by rootkits to evade detection on systems they infect, said Mikko Hyppönen, manager of anti-virus research at F-Secure Corp.

New versions of Rbot are identified almost daily, but recent variants come with a version of a software driver from FU, Hyppönen said.
When the driver is placed on an infected system, it allows Rbot to hide its process from the Windows task manager, or other task management tools that show users what programs are running on their Windows system.

The integration of FU with Rbot is crude and was probably done by an inexperienced hacker, or "script kiddie," who lifted the code wholesale from the FU source code, which was posted on the Internet by the rootkit's author, Jamie Butler (aka "Fuzen") as a proof of concept.

However, other malicious code authors are doing a more thorough job of tying rootkit features into their creations, Hyppönen said.

A recent variant of the Myfip worm, Myfip.h, incorporated features from FU that allowed it to manipulate data in the system kernel, or Windows core processing center, allowing it to hide its processes, he said.

The FU source code, available from Web sites like RootKit, is a rich source of information for malicious code writers. However, FU is not a true rootkit and doesn't try to evade detection.
That means that viruses and malicious programs that use FU components might still raise red flags from security programs that miss the virus processes running, but spot FU running on infected systems, he said.

Other virus authors seem to be catching on to tricks used by rootkit authors to avoid detection, also.

A recent version of the Sober worm, Sober.P, used a strategy called "I/O blocking" that doesn't prevent infected e-mails from being spotted, but can keep anti-virus products from detecting Sober.P on infected systems, according to experts.

F-Secure is testing a rootkit detection program called BlackLight that can spot some rootkits. Jamie Butler, author of the FU rootkit, has also released a free program called VICE that can spot FU, but most anti-virus companies don't have rootkit detection features in their products, he said.

Full Story [2].

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://www.eweek.com/article2/0,1759,1816972,00.asp