

When Government Sides With The Crackers

February 27, 2007

By Larry Seltzer

Sometimes standing up for individual rights is not just a matter of principle, it's common sense.

[The prosecution of former Orange County, Calif., Superior Court Judge Ronald C. Kline for child pornography](#) is a case that stands out in this respect, and for reasons which have a lot to do with computer security.

ADVERTISEMENT



**ZERO-DAY ATTACKS.
DENIAL OF SERVICE.**

**An exposed network
is a big risk.**

Kline had downloaded images of child porn, including some that contained a trojan horse and had been left there by Brad Willman, a Canadian who calls himself Citizen Tipster. Based on what I've read, it appears that the images probably exploit some vulnerability that allows them to run malicious code.

RELATED LINKS

[Symantec: Profit-Driven Cyber-Crime Won't Stop](#)

[Crime Ring Targets IE 'Setslice' Flaw](#)

[Crime Rings Target IE 'SetSlice' Flaw; ZProtector Released](#)

[Helping Law Enforcement Fight Cyber-Crime](#)

[Virginia Official Discusses the Fight Against Cyber-Crime](#)

Once Kline loaded the images, Willman, like any other bot herder, could gain access to his computer

and do what he wished, including looking for evidence of who Kline was and passing it on to the authorities, and this he did. The government was willing to accept this evidence even though it was obtained by clearly illegal means. And the government made it clear they weren't going to prosecute Willman, which effectively encourages him to continue his activities.

Indeed the legal standard is that such evidence can still be admissible if it wasn't obtained by the government or an agent of theirs. The government successfully made the case to the famously liberal 9th Circuit Court of Appeals that Willman was not an agent of the government.

The case, believe it or not, is far from unique. I wrote about a very similar case several years ago. The hacker in that case was not even identified in court except by the handle "Unknownuser" and turned out to be a resident of Turkey. But the FBI, [and later the state of Virginia](#), were willing to accept evidence from an unnamed foreigner, who couldn't be cross-examined, and eventually the courts were willing to accept it, too.

The Virginia case was worse in many ways, in that the government actually had actively encouraged Unknownuser to continue his hacking activities based on earlier evidence he provided in another case, and they also made it clear to him that they weren't going to prosecute him. To my mind this makes him clearly an agent of the government, but the famously conservative 4th Circuit Court of Appeals sided with the FBI. There the case ended, at least so far.

Based on the reports I've read, and especially since he recently pleaded guilty, it's tempting to believe that Kline is guilty. But it's also possible that he just copped a plea based on the strength of the evidence against him.

In the hands of a talented hacker, a rootkit can do anything on your system and good luck proving that it's there. [Click here](#) to read about F-Secure's analysis of this "kernel malware."

And make no mistake about it, the evidence found by Willman and Unknownuser is not reliable. Trojan horses of the type they use (Unknownuser used Subseven) give them just as much ability to plant evidence as to find it. Under such a standard, I could hack into your computer (yes, you), plant kiddie porn on it and call the FBI anonymously to rat you out. I could also threaten to do this if you don't pay me. How's that for a legal system?

I can only understand the court's attitude as indicating either that they didn't appreciate just how tainted the evidence was, or that they overlooked it because of what the defendant was accused of. In Kline's case, he had been publicly pilloried for years, with one radio station camping outside his house.

Nowadays you'd garner a lot more respect defending the rights of al Qaeda members than alleged child porn owners. There's a good reason why everyone has certain rights, no matter what they're accused of. Some people accused of crimes are not guilty of them, and the evidence against them needs to be held to a high standard. Relying on the likes of Unknownuser and Willman doesn't meet that standard. You better hope they don't take a disliking to you.

Security Center Editor [Larry Seltzer](#) has worked in and written about the computer industry since 1983.

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at eWEEK.com Security Center Editor [Larry Seltzer's Weblog](#).

More from Larry Seltzer

[Copyright \(c\) 2007 Ziff Davis Media Inc. All Rights Reserved.](#)