

Washington Post Caught in Metadata Gaffe?

By Ryan Naraine
2006-02-22

Metadata found in online images may help pinpoint the location of a 21-year-old hacker who openly admitted to breaking into computers and turning them into botnets.

The Washington Posts online arm has apparently been caught in a metadata gaffe that exposed the whereabouts of a 21-year-old hacker who confessed to controlling thousands of compromised PCs for malicious use.

The hacker agreed be interviewed by Washington Post reporter Brian Krebs on the condition that he not be identified by name or home town, but when the article was posted on the newspapers Web site, an accompanying photograph included metadata that pinpointed the location to Roland, Okla., a small town with a population of 2,842.

In the feature story titled [Invasion of the Computer Snatchers](#), the hacker known online as "0x80" (pronounced X-eighty) openly boasted about breaking into thousands of computers around the globe and infecting them with malware that turned them into botnet drones.

A botnet is a collection of compromised machines controlled remotely via IRC (Internet Relay Chat) channels to send spam or launch denial-of-service attacks.

In 0x80s case, the hacker openly admitted to illegally installing adware and spyware on infected computers and earning money from [online marketing](#) companies that pay for advertisements delivered to users.

However, because of the metadata slip-up by the Washington Post, it is very likely that law enforcement authorities will be looking in the direction of Roland, OK to find the hacker, who was described in the story as "tall and lanky, with hair that falls down to his eyebrows," and speaking with a "heavy Southern drawl and Midwestern nasality."

The reporter also wrote that 0x80 lives with his religious parents in a small town in Middle America where the nearest businesses are a used-car lot, a gas station and convenience store and a strip club, where 0x80 claimed he

recently dropped \$800 for an hour alone in a VIP room with several dancers.

"His bedroom resembles a miniature mission control center, with computers, television and [computer monitors](#), and what must be several miles worth of tangled wires plugged into an array of surge-protected power strips," Krebs wrote.

The article was published with several photographs, including one with a doctored image of half of the hackers face.

But, as eagle-eyed [Slashdot posters](#) discovered, the online images by photographer Sarah L. Voisin contained tags about the location of the shoot.

Immediately after the metadata discovery, the images were removed from the Washington Posts Web site.

Krebs declined to discuss the issue. "I would like to talk with you about this. However, due to confidentiality agreements I have made with my source, Im not at liberty to do so," he said in an e-mail exchange with eWEEK.

Asked if law enforcement authorities had contacted him to follow up on the since-published location of the hacker, Krebs again declined comment.

The Slashdot [community](#), however, insisted on attempting to track down the hacker. Using Google Maps and other search-related data, the posters were able to figure out that the male population of Roland, Okla., was just over 1,300.

"Any flatfoot could find him in an hour," said one Slashdot commenter who posted details of the metadata from the online image.