

What makes SKorea cyberattacks so hard to trace?

PETER SVENSSON, AP Technology Writer



NEW YORK (AP) — The

attacks that knocked South Korean banks and media outlets offline this week appear to be the latest examples of international "cyberwar." But among the many ways that digital warfare differs from conventional combat: There's often no good way of knowing who's behind an attack.

South Korean authorities said Thursday that the attack, which shut down scores of cash machines and hampered business, had been traced to an "Internet Protocol" address in China. But that doesn't mean the attack was launched from there. The general assumption in South Korea is that the attack originated in North Korea.

"IP" addresses are, roughly speaking, the phone numbers of the Internet. Each connected computer has a number that identifies it uniquely on the network, so the Chinese IP address implies that a computer in China was involved in the attack.

However, that computer could have been controlled from elsewhere, either because someone bought access to it, or because it's been infected with malicious software. To determine the location from which it's being controlled, investigators would need access to that computer, or to the records of the company hosting the computer. That's unlikely to be forthcoming from a Chinese company.

"China is obviously a popular place to hide things," said Dan Holden, director of security research at Arbor Networks' Security Engineering & Response Team. Chinese authorities are difficult to work with and there's a language barrier, he said.

In addition, China is believed to be conducting its own campaign of cyber-

What makes SKorea cyberattacks so hard to trace?

Published on Electronic Component News (<http://www.ecnmag.com>)

espionage, which means that attacks launched from there are often simply attributed to the Chinese government, even if it isn't responsible for the aggression, Holden said.

"If you are any nation state or even any attacker right now, why wouldn't you hide in China right now?" Holden asked rhetorically.

Apart from tracing the path an attack takes through the Internet, there's another way to figure out who's behind it: analysis of the software involved. Malicious software, or "malware," can provide clues to its creator. Some of those are obvious, like comments inserted into the written code. However, such comments can be easily faked to lead investigators astray. More subtle analysis can be fruitful, according to Christopher Novak, managing principal of the global investigative response team at Verizon Communications Inc.

"In many cases, the malware that you see on the computer is very similar to a cold or an illness that a person gets ... The strain of the cold that I have and the strain of the cold that you have may be slightly different, but when we look at the DNA and makeup and see they're 99.9 percent the same, there's a pretty good chance one of us transmitted it to the other," Novak said. "When we analyze malware codes, we see the elements that are copied and reused, certain programming styles."

Such analysis can yield important clues, but rarely rock-solid attribution. The U.S. Department of Defense has said that a cyberattack can merit a violent response, but first you have to know who to target.

"Digital attribution is extremely difficult and if you want to do it, it takes some serious effort," Holden said.

Source URL (retrieved on 12/17/2014 - 4:33pm):

<http://www.ecnmag.com/news/2013/03/what-makes-skorea-cyberattacks-so-hard-trace>