Industrial Espionage (9): Blocking Chinese Hackers

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last article, I summarized an interesting case in which an information systems security officer at Sandia National Laboratories discovered that a flood of data thefts was originating from three servers in China. This case was investigated by the FBI and has the code name “Titan Rain.”

Scott Granneman wrote a thoughtful and stimulating commentary about Chinese hacker attacks in _The Register_ on the 31st of August <http://tinyurl.com/9g3zo>. He also mentioned the Titan Rain case but he focused first on the experience of some personal friends of his who run Web-hosting services. They both independently discovered that their systems were being swamped by a flood of peculiar requests originating in a wide range of sites in the People’s Republic of China (PRC). He wrote, “Both of my friends thought about their situations, and both came to the same conclusion: block the entire IP ranges! Use WHOIS to look up the IP address' range, then block 'em with the server's firewall. This quickly grew into a mammoth, seemingly neverending task, but it immediately began to pay off. Fishy web server requests tapered off greatly, and while there are still a few every day, it's now become a manageable problem. If things keep up at the same pace, sometime in the next few months they're going to have blocked every IP in China.”

Granneman asked whether his friends had told their clients about their new policy of blocking all packets originating in the .CN domain; they said no.

Granneman, to his credit, raises two ethical questions:

1) Should his friends have told the clients about the global block on Chinese access to their Web sites?

2) Is there something wrong with blocking all access to a Web site for all users in a national domain?

For the first question, I think that simple ethical rules dictate that his friends should indeed have informed their clients of the new policy. One rule in ethical decision making is to consider all the stakeholders affected by a decision, and their clients are potentially affected. Another is that openness characterizes appropriate actions; a desire for secrecy always raises questions about whether a course of action is ethical (it doesn’t mean that all secrecy is bad, just that it raises questions that should be answered).

However, for the second, I cannot conceive of how anyone could reasonably argue that the owners of a private Web site have any limits whatsoever on how they restrict access to their information. The Web is a method for voluntarily sharing documents (and now, much more) using standard protocols (http, html and so on). Nothing in the technology removes the absolute
right of the data owner to control how that information is shared. For example, if a copyright holder chooses to restrict access to published documents by requiring registration, that’s fine. If they require access controls using a userID and a password, that’s fine. If they require users to buy smart cards and log in using one-time passwords, that’s a real pain but it’s also fine. If they require users to have biometric equipment for retinal scans, brain-wave measurements and a signature in blood giving away rights to the user’s house, that may be crazy but it’s also perfectly legal. The worse the restrictions, the fewer the users, but no one has an absolute right to access any document on a privately-owned site on the Web.

So if a private Web-site owner wants to block all packets originating from the PRC, there is absolutely nothing morally or legally wrong with such a decision.

Personally, I have blocked all e-mail with country domains from which large amounts of spam originate; if someone in those countries wants to communicate with me, they can write me a letter. Immoral? No. Unethical? No.

MY e-mail. MY Web site. Don’t bother me if I don’t like you, your ISP or your country!

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.