

New Geo-Location Service Could Help Track Cyber Thieves

By Larry Greenemeier

InformationWeek, June 14, 2007

<http://www.informationweek.com/story/showArticle.jhtml?articleID=199903929>

Quova's new software is designed to help organizations identify in real time any devices connecting into their Web sites.

Since the day criminals figured out how to use the Web to steal and profit from both personal and corporate information, investigators have been confounded by an inability to trace criminal activity back to its source.

Thanks to a variety of factors -- the use of networks of proxy servers to avoid leaving digital evidence and a lack of cooperation among international law enforcement -- cyber crooks are often able to throw off the scent of even the most seasoned Internet investigators.

With Quova Inc.'s announcement Wednesday of its new services for tracking Web traffic, help may be on the way for companies and law enforcement investigating cyber crimes. The company's new Internet Location Intelligence Platform, a combination of data, software, and services, is designed to help organizations identify in real time any devices connecting into their Web sites. The platform includes the latest version of Quova's GeoDirectory Server, which includes a proxy locator component that determines if a Web visitor is accessing an organization's Web site through a proxy server, a technique often used to mask the original IP address of malicious activity.

Through a combination of data, software, and services, Quova has since 2000 helped organizations understand key demographic information about traffic to their Web sites, including the local language spoken and currency used at the point the traffic originated, rules and regulations that apply to that location, and whether the users in that location are licensed to use the organization's products and services. This has helped organizations detect and even prevent fraud, comply with government regulations and licensing agreements, localize advertisements, and better manage digital rights.

But the same technology also helps law enforcement and businesses investigate the origin of malicious attacks and fraud. "If I'm coming in to a Web site through some sort of proxy, it looks like I'm trying to hide rather than coming straight from a DSL connection right by my home," Quova president CEO Marie Alexander told InformationWeek. "We saw with our customer base that they would look at the country of origin of their orders and check to see if it made sense for an order to come from a particular domain." A shipping or billing address that's located on the side of the world from the IP address where the order is originating should set off red flags.

GeoDirectory Server 6.0, set to ship by the end of September, is a Java-based application through which Quova delivers the geographical location and network connection data for each IP address accessing a customer's Web site. Quova developed the latest addition of

its software to address situations when simply looking at an IP address's geographic location isn't enough to accurately determine the location of a Web visitor. The GeoDirectory's IP intelligence capability determines additional network characteristics, including the type of connection used to access a Web site (such as DSL or dial-up), the route taken to a site (whether it passed through a corporate proxy server, mobile gateway, or an open proxy), and domain information associated with IP addresses. Quova's new Internet Location Intelligence Platform will be offered in conjunction with Mexens Technologies' Navizon wireless positioning system and software. Together Quova and Mexens will provide Internet location intelligence to determine the most effective means of locating a user. When Quova's IP geo-location capabilities don't provide detailed enough information, organizations will be able to use Wi-Fi, cellular, and global positioning system information from Navizon to triangulate signals from Wi-Fi access points and cellular towers to help determine location.

Quova has worked with online gambling sites including Wagerworks UK Ltd., Ladbrokes International Ltd., Gaming Online, Luckyskills Ltd., and Tournament Gaming Ltd. to ensure those sites don't do business in places where gambling is illegal. "We have provided gambling sites in the U.S. with information about how their users were connecting into the site and the likelihood they were not based in the U.S.," Alexander said. The company also counts Major League Baseball, the BBC, and Cisco Systems as customers.

Not everyone is convinced that a service such as Quova's can be applied cyber crime fighting. "It's not difficult to find an open proxy server (universities often have them on their networks), assign the IP address of one such proxy to your computer, and launch an attack or start a spam or denial of service campaign," Yuval Ben-Itzhak, CTO of Web security vendor Finjan Inc., told InformationWeek. "A service that tracks where attacks are coming from could say where the source is, but it can't necessarily tell you where to send the police."

Others are less skeptical. If a given proxy server keeps a detailed audit log, it's possible to backtrack through the log to study how the server was used, Andrew Colarik, an information security consultant who holds a Ph.D. in information systems security from the University of Auckland, told InformationWeek. "Of course, there are proxy servers put out on the Internet specifically to cause investigators to hit a brick wall," he added. "This has been quite a big issue."

If companies and law enforcement act quickly enough, they can work with an ISP to find the root path where an IP address originated, but that works only when the attacker or fraudster has established a continuous connection to a server that can be documented, Colarik said.

And catching cyber criminals is another story. "Jurisdictional issues are a nightmare," Colarik said. By the time investigators approach officials in foreign countries and get permission to question possible suspects, they've already moved on. "We don't have a

universal treaty to address cyber crime," he added. "I don't think we're prepared as a civilization for the consequences of our technology at this time."

One answer is to create a league of cyber communities that includes the top 20 countries in terms of gross domestic product, a factor that has a strong correlation to the top 20 countries in terms of Internet users, Colarik said, adding, "Each member would monitor their own cyber crime activity. Any member that couldn't control this activity would be shut off from Internet access to the other countries in the league."

It's this kind of thinking, combined with creative new uses for existing technologies such as Quova's, that could eventually help turn the tide of cyber crime.