South Korea's net nirvana spawns good, bad and ugly results

Jonathan Hopfner, Reuters

On a single, dimly-lit floor in the towering central Seoul headquarters of Korea's National Police Agency, dozens of hard drives and mobile phones sit on shelves awaiting dissection.

Officials flit between cubicles, comparing notes, as above their heads massive LCD screens churn out graphs and charts for experts to interpret as all-clear signals or dire warnings.

It may lack the chaos of a physical battlefield, but the agency's Cyber Terror Response Center is the front line in South Korea's growing struggle against computer and Internet-related crime.

Established more than a decade ago, the response center now commands a network of 1,000 officials nationwide who monitor computer systems for viruses, hacking and related attacks and who conduct post-mortem investigations into those systems that have been compromised.

In one of the world's most wired countries, the center has no shortage of work.

South Korea, with its near-ubiquitous Internet access and lightning-fast broadband connections, was ranked by the United Nations Telecommunication Union recently as the world's most advanced nation in terms of information and communication technology usage.

The country is also known as the home of such technology giants as Samsung Electronics and LG Electronics.

Unfortunately, the country also holds less laudable titles. Data from U.S.-based Internet security research firm Team Cymru indicates South Korea is, by far, Asia-Pacific's leading host of peer-to-peer "botnets," compromised, Internet-connected computers typically used for illegal activities and usually without the owner's knowledge.

Steve Santorelli, Team Cymru's director of global outreach, says this represents the downside of being "one of the most connected places on the planet."

"Peer-to-peer based botnets are virtually impossible to kill...(the number in South Korea) is deeply disturbing," he said.

Computer security firm Symantec ranked South Korea seventh worldwide in terms of malicious online activity last year, up two notches from 2009 and trailing only far larger China and India in Asia.

"The cybercrime problem is constantly increasing," sighed Jung Suk-hwa, the Cyber Terror Response Center's soft-spoken investigation director. "Basically, Korea is a good place for it."

CYBERCRIME EPIDEMIC

A series of high-profile attacks this year have highlighted vulnerabilities in South Korea's cherished communications infrastructure and thrust cybercrime squarely into the public spotlight.

In late November a hacking attack that targeted Korea-founded, Japan-based online gaming firm Nexon Co exposed the personal information of more than 13 million subscribers to one of its popular titles, casting a pall over its up to $1.3 billion Tokyo IPO.

That followed a data breach of record scope in July at Nate and Cyworld, popular social networking sites operated by SK Communications. The incident affected the accounts of some 35 million users, equivalent to around 70 percent of the country's entire population.

In April hackers managed to access data on 23 percent of the 1.8 million customers of Hyundai Capital, a joint venture of GE Capital and Hyundai Motor.

The Nexon and SK Communications cases are still being investigated with the trail in the latter leading to China, where most attacks against Korean firms appear to originate, according to Jung.

Cybercrime has also rocked the political and national security spheres.

Police are currently investigating a distributed denial of service (DDoS) attack that crippled the National Election Commission's website during October by-elections, which the opposition alleges was the work of ruling party officials. And authorities in South Korea have linked North Korea to a series of hacks affecting financial, government and military websites.

Hacking and data theft have been issues for some time in South Korea's highly wired society, but "this is the first time we're seeing crimes of this magnitude," Jung says.

The local operations of global firms have not been immune. An August attack on a hosting provider temporarily brought down the local website and online banking operations of HSBC, while the same month an intrusion into Epson's Korea website exposed the personal details of around 350,000 customers, according to a company spokesman.

REAL NAME CONTROVERSY

The spike in personal data leaks this year has fueled the debate over the country's

real name verification rules, which have been controversial since their introduction in 2005 in an attempt to moderate online discussions during election periods.

These require websites with more than 100,000 visitors daily to collect the names and personal details of users before the users can upload content or post comments.

By amassing private data, usually national resident registration numbers, on hundreds of thousands of people, South Korean websites create a tempting target for cybercriminals, says Park Kyung-sin, a professor of law at Korea University.

While the real name rules do not specifically require companies to store personal data, according to Park they are left with little choice in practice.

"If websites require identification each time people log on, people won't use them," Park said. "This makes it economically impractical for them to use one-time identification. The rules practically require the accumulation of personal data and also make it enormously profitable for companies to retain it."

Politicians such as Kim Sung-hoon, head of the digital policy committee of Korea's ruling Grand National Party (GNP), have campaigned for real name verification to be revoked.

In addition to restricting freedom of expression, the rules leave "no company safe at the moment, and we have to take fundamental action by abolishing them immediately," he said.

The country's Internet regulator, the Korea Communications Commission, is sticking to its guns. The agency acknowledges "questions over the effectiveness and suitability" of the rules and is "investigating every single step toward their improvement," said Oh Jung-taek, chief of the KCC's Network Ethics Department.

But real name verification is needed to discourage the online dissemination of defamatory remarks or rumors, particularly concerning North Korea, which "could give rise to serious trouble or social turmoil," Oh said.

"Given the special situation we have, it's inappropriate to talk about revoking the rules just a few years after they were implemented."

TAKING MATTERS INTO THEIR HANDS

With the rules unlikely to disappear anytime soon, many companies are developing their own responses. Epson Korea no longer collects resident registration numbers, the company spokesman said. Hyundai Capital has established a separate information security unit and now assigns more than 10 percent of its IT budget to security, according to spokeswoman Fiona Bae.

Some companies have moved to bypass the rules altogether. Google, for example, has prevented users from uploading content or posting comments to the South

Korean version of YouTube, stating that real name verification rules do not "fall in line with Google's principles."

The fight against cybercrime has seen some successes. In October the suspected hacker in the Hyundai Capital incident was apprehended in the Philippines. Incidents of online harassment, illegal website operations and piracy have dropped sharply over the last couple of years.

Authorities are trying to help companies shore up their online defenses, with both the KCC and Cyber Terror Response Center offering information security training. The center also plans to boost manpower and cooperation with international authorities such as the Chinese police and Interpol, the National Police Agency's Jung says.

But with the number of hacking cases continuing to climb, Jung admits agencies like his lack the resources to turn a rising tide.

Critics of the real name requirements say their abolishment would do more to bolster the country's online security than any new software or hiring spree.

"No matter how much we invest in security to prevent cybercrime, it'll make no economic sense," says the GNP's Kim. "We'd do better to revoke the real name rules."

(Additional reporting by Seongbin Kang; Editing by David Chance and Matt Driskill)

Posted by Jason Lomberg, Technical Editor