TAIPEI TIMES
SUNDAY FEATURES
SUNDAY, APRIL 19, 2009

The GhostNet in the machine

Cybercrime is big business — and perhaps nowhere more so than in China, where many attacks were initially motivated by nationalism and others allegedly sanctioned by the Chinese government

BY **DANNY BRADBURY**
THE GUARDIAN, LONDON

IT wasn't until Sunday of last week that Scott Henderson knew he'd been duped. The former US army intelligence officer, along with his colleague "Jumper" had been tracking an alleged Chinese hacker, nicknamed Lost33, who had promised him an interview. "Lost33 did not make contact with Jumper last night. In fact, it seems he spent the night changing his QQ number" — QQ is a popular Chinese instant messaging service — "and deleting all info from his blog. The Web site is now completely empty, except for a change to his personal data," said Henderson on his blog (bit.ly/darkvisitor).

Henderson had been tracking Lost33 after his e-mail address — losttemp33@hotmail.com — turned up in an investigation called GhostNet (bit.ly/ghostnet2). GhostNet started when Information Warfare Monitor (IWF, bit.ly/infowar), a team of cyberwarfare researchers created by the University of Toronto and the Canadian security think tank SecDev, had been asked to conduct a security audit for the Tibetan government in exile. It had found malicious software on the Dalai Lama's most sensitive computers.

The investigation found links back to command and control servers located mainly in China. From there, the IWF found infected computers under the control of those servers in 103 countries. They identified roughly a third of them, and found them all to be sensitive computers in organizations important to Chinese interests, including numerous embassies, telecommunications companies, and even Vietnamese petroleum firms. Just as Lost33's identity and motives are shrouded in mystery, the final link between GhostNet and the Chinese government is also lacking.

Ostensibly, this looks like a state-sponsored cyber-spying ring. Especially when you read the part of the report in which a member of an online Tibetan outreach project was detained for two months and interrogated by Chinese officials. They presented her with copies of her Internet chat logs. The project's machines were compromised by the same malware that filched the Dalai Lama's files, and communicated with the GhostNet control servers.

But there could be other motives and actors, says the IWF. GhostNet could be a for-profit initiative, operated by cyber-criminals. It could be operated from outside China, using compromised Chinese computers as proxies (one of the control servers — also the first to be shut down when GhostNet was discovered — was based in the US).

"Even 'patriotic hackers' could be acting on their own volition, or with the tacit approval of their government, as operators of the GhostNet," says the IWF report. The problem is that all of these things are happening in China anyway. Henderson says that patriotic hacking has been a mainstay of the Chinese hacking underground since the mid-1990s.

After the Internet arrived in China in 1994, people began experimenting with the technology, and in 1997, the Green Army hacker group was formed. This gave way to the Red Hacker Alliance, a loosely connected set of groups that emerged after the Jakarta riots of 1998, when Chinese nationals were accused of destabilizing the country. Indonesian Web sites were defaced by outraged Chinese hackers, and a nationalistic movement took on force.

Since then, for-profit motives have emerged. "The history has changed from being a group wanting to protect the motherland, to being specialized hacker groups that are there for the purpose of making money," Henderson says. Now, for example, hackers have broken the rule of thumb that prevented them from attacking Chinese IP addresses. That wouldn't have been appropriate when cyber-attacks were motivated by nationalism. Now, in the age of commercialized cybercrime, anyone is fair game.

Zhao Wei (趙薇), co-founder of the Chinese Anti-Malware Alliance (中國反惡意軟件聯盟), has been battling against the hacker underground since 2006. He says that hackers in China are growing in number, due in part to the economic downturn — and that Chinese nationals are just as vulnerable to poor security in Chinese cyberspace.

"At least 20 million people in China lost their jobs, and after they spend all of their money … then they may turn to cybercrime," says Wei. He adds that the online crime wave is spreading to smaller cities, which shot up in great numbers during the economic boom. Phishing and other cybercrime has supplanted physical crime in some of these places.

After all, why risk harsh punishment for ripping off a warehouse when you can rip off people electronically with scant fear of retribution? "The policemen think it's cool. There's no one on the street. They're all going to the bar, and they're working on phishing. The policemen love the Internet," Wei says.

In addition to phishing and hacking Web sites, Chinese hackers have also exploited flaws in local third-party applications, which are often badly written, Wei says. China, known for its lax view of intellectual property, is rife with pirated copies of Windows software — local companies now provide their own security update services for the company's software, he says.

So what are Chinese hackers looking for on their victims' machines? Much the same as hackers outside the country, but online games accounts are also targeted, and *World of Warcraft*, the most popular multiplayer game worldwide, is a particular prize. Accumulated gold and character points from this game can be sold on the open market.

Attacks from Chinese hackers can also be more sophisticated. Dennis Dwyer, a threat intelligence analyst at the Atlanta-based managed security services firm SecureWorks, says that targeted attacks are a signature technique perfected by Chinese cyber-criminals. They will conduct extensive research on an organization to understand which individuals work there and how they're related.

"What we have seen is very specific malware. They'll be looking for people using a certain version of Word," says Dwyer. The GhostNet report demonstrates how hackers persuaded victims to open infectious files by attaching them to e-mails supposedly from people they knew.

"We also see the use of zero-day or file format type exploits [malware applications]," confirms Dwyer. "In particular, we watch a group called Phantom. They're very public about what they do. What they typically don't do is use [the exploits] themselves. They sell them for others to use."

This trend of selling exploits on the open market is now gravitating toward selling toolkits. SecureWorks has identified a new kit — Leopard in a Hole — that automates the kind of SQL injection attacks for which Chinese hackers have become famous. This time last year, Chinese hackers compromised tens of thousands of Web sites with malicious JavaScript. Versions of Leopard in a Hole that essentially allow non-technical attackers to do this with a just a few mouse clicks have been found on sale for up to US$500. Online crime is now big business.

In all of this, one unanswered question remains. Who was responsible for GhostNet? "It's convenient to have privateers. People who are given the king's warrant to act on his behalf, but who are kept at arm's length," says Rafal Rohozinski, principal analyst at the IWF and co-author of the report. He likens cyberspace to the high seas of old, which were populated by what amounted to freelance warships sanctioned by the state. "I think these are third-party actors. Whether they're deliberately commissioned, protected or allowed to raise money from other activities that are overlooked, I don't know."

In China, more than perhaps anywhere else in the world, there is a bountiful supply of such cyber-swashbucklers. Who knows how many other treasure chests people may have buried in the world's networks — or whether we will ever be able to prove the true identity of those that put them there?

How to protect your PC

BY **BILL HUSTED**
NY TIMES NEWS SERVICE, ATLANTA

If someone offered to build a house for you that was completely safe from burglars, you'd know they were either mistaken or lying.

It's the same when it comes to adding protection to make your computer completely safe. It just can't be done.

But that doesn't — and shouldn't — stop you from doing your best. It's smart to do what you can, but remain aware you're never totally out of danger.

All this has been on my mind because of news stories recently — among them one about Canadian researchers who found a giant network of Chinese hackers who had tapped into computers worldwide, including one owned by the Dalai Lama.

Then there's the highly sophisticated Conficker worm that's been in the news recently. Those threats were created by sophisticated computer criminals and can't be stopped completely. But there are things you must do to protect your computer against those who are just as malicious but not quite as talented.

Firewall

That's the No. 1 line of defense — the equivalent of a deadbolt on your front door. Starting with Windows XP and continuing with Vista, the free firewall supplied with Windows is actually pretty good.

Since it's built into Windows, there is little chance it will interfere with the operation of your computer. Take a moment to make sure your firewall is turned on. If you don't know how to go about that, just type the word "firewall" into your Windows search menu.

NAT

Those letters stand for Network Address Translation. If you want to know how it works, go to this Web address: tinyurl.com/ehmmh. All you really need to know is that NAT also provides security.

Luckily, computer routers usually have NAT protection built in. So if you have a computer network, you already have this added layer of protection that lets your computer hide behind the router.

Malware protection

I'm using the term malware because I want to include spyware, adware, viruses, worms and other stealthy threats used by hackers to take over your computer. I know it sounds basic, but you must use good programs to check for all these threats.

I've listed many of them in the past and don't have the space to list the programs again. There are both good free and commercial programs.

Many readers, unwilling to go through the uncertainty and hassle of tracking down free programs, might be well-served to just pay the price for commercial protection from Symantec, McAfee or other providers. Check online reviews at cnet.com or pcworld.com for the best performers.

Once you add a program, keep it updated. Also regularly update Windows. As was true in the case of Conficker, Microsoft regularly issues patches to combat new threats.

One handy thing to know: If your anti-virus programs or Windows won't update, that's a sign that malware is active in your computer, blocking the update.

No software needed

One of the best defenses is common sense. Many threats are implanted in your computer from suspect Web pages. So avoid X-rated sites, hacker sites and Web sites that offer access to free versions of songs and commercial software.

Many sites offering free games are both well-done and amusing — along with being danger spots for adware and spyware.

Also be wary of e-mail attachments. Even a sender you know and trust could unknowingly send along something harmful. Ignore e-mails with attachments from people you don't know.

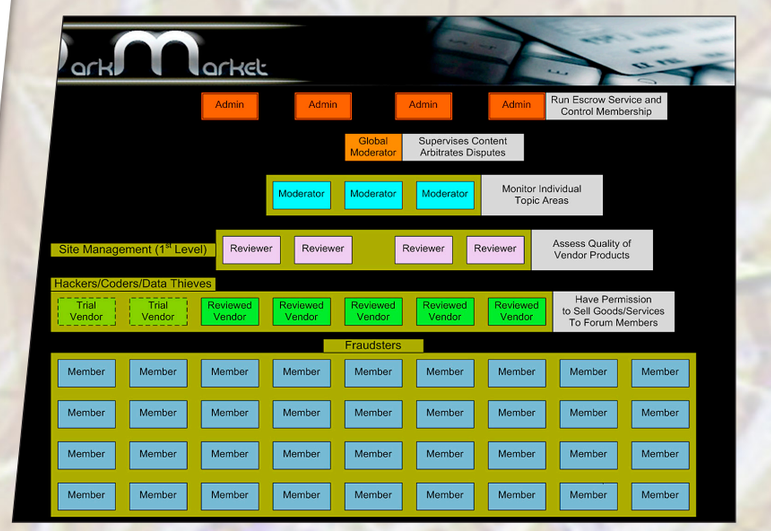
Now the deadbolts are locked and the alarm system is on. But stay suspicious. The best computer protection is a savvy and skeptical user.

Tracking an electronic espionage network

Information Warfare Monitor (IWF), a team of researchers from the University of Toronto and the Ottawa-based think tank SecDev, summarized its report on GhostNet, a vast cyber-spying ring that has infiltrated computers and has stolen documents from hundreds of government and private offices around the world, including those of the Dalai Lama, in *Tracking GhostNet: Investigating a Cyber Espionage Network*. IWF said that while its analysis points to China as the main source of the network, it has not conclusively been able to detect the identity or motivation of the hackers. The report is available online at www.tracking-ghost.net.

Two Cambridge University computer researchers who worked on part of the IWF investigation related to Tibetan exiles, Shishir Nagaraja and Ross Anderson, summarized their findings in an independent report, *The Snooping Dragon: Social Malware Surveillance of the Tibetan Movement*. Unlike the IWF report, *The Snooping Dragon* states that "agents of the Chinese government" were behind cyberwarfare attacks on the Dalai Lama's "computing infrastructure." An abstract of the report and a link to a PDF version are available online at www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.html.

Source: NY Times News Service and AFP



Top right: This Federal Bureau of Investigation computer screen image shows an online forum called Dark Market, which tells users where to buy skimming devices to penetrate bank accounts, how to distribute malware through spam and buy stolen credit cards, among other things.
Above: The Canadian academic researchers who are reporting on the spying operation dubbed GhostNet include, from left, Ronald Deibert, Greg Walton, Nart Villeneuve and Rafal Rohozinski
Left: Nobody is safe from being hacked, not even the Dalai Lama.

PHOTOS: AGENCIES