(BN) How Hacker Sleuths Found Zhang in Trail From U.S. to China

+----------+

How Hacker Sleuths Found Zhang in Trail From U.S. to China
2013-02-14 11:01:00.0 GMT

By Dune Lawrence and Michael Riley
Feb. 14 (Bloomberg) -- Joe Stewart's day starts at 6:30 a.m. in Myrtle Beach, South Carolina, with a peanut butter sandwich, a sugar-free Red Bull, and 50,000 or so pieces of malware waiting in his e-mail in-box. Stewart, 42, is the director of malware research at Dell SecureWorks, a unit of Dell, and he spends his days hunting for Internet spies.
Malware is the blanket term for malicious software that lets hackers take over your computer; clients and fellow researchers constantly send Stewart suspicious specimens harvested from networks under attack. His job is to sort through the toxic haul and isolate anything he hasn't seen before: He looks for things like software that can let hackers break into databases, control security cameras, and monitor e-mail.
Within the industry, Stewart is well-known. In 2003 he unravelled one of the first spam botnets, which let hackers commandeer tens of thousands of computers at once and order them to stuff in-boxes with millions of unwanted e-mails. He spent a decade helping to keep online criminals from breaking into bank accounts and such. In 2011, Stewart turned his sights on China. "I thought I'd have this figured out in two months," he says. Two years later, trying to identify Chinese malware and develop countermeasures is pretty much all he does.

Continuous Invasion

Computer attacks from China occasionally cause a flurry of headlines, as did last month's hack on the New York Times. An earlier wave of media attention crested in 2010, when Google and Intel announced they'd been hacked. But these reports don't convey the unrelenting nature of the attacks. It's not a matter of isolated incidents; it's a continuous invasion.
Malware from China has inundated the Internet, targeting Fortune 500 companies, tech start-ups, government agencies, news organizations, embassies, universities, law firms, and anything else with intellectual property to protect. A recently prepared secret intelligence assessment described this month in the Washington Post found that the U.S. is the target of a massive and prolonged computer espionage campaign from China that threatens the U.S. economy. With the possible exceptions of the

U.S. Department of Defense and a handful of three-letter agencies, the victims are outmatched by an enemy with vast resources and a long head start.

Fair Play

Stewart says he meets more and more people in his trade focused on China, though few want that known publicly, either because their companies have access to classified data or fear repercussions from the mainland. What makes him unusual is his willingness to share his findings with other researchers. His motivation is part obsession with solving puzzles, part sense of fair play. “Seeing the U.S. economy go south, with high unemployment and all these great companies being hit by China ... I just don’t like that,” he says. “If they did it fair and square, more power to them. But to cheat at it is wrong.”
Stewart tracks about 24,000 Internet domains, which he says Chinese spies have rented or hacked for the purpose of espionage. They include a marketing company in Texas and a personal website belonging to a well-known political figure in Washington. He catalogues the malware he finds into categories, which usually correspond to particular hacking teams in China. He says around 10 teams have deployed 300 malware groups, double the count of 10 months ago. “There is a tremendous amount of manpower being thrown at this from their side,” he says.

Government Links

Investigators at dozens of commercial security companies suspect many if not most of those hackers either are military or take their orders from some of China’s many intelligence or surveillance organizations. In general, they say the attacks are too organized and the scope too vast to be the work of freelancers. Secret diplomatic cables published by WikiLeaks connected the well-publicized hack of Google to Politburo officials, and the U.S. government has long had classified intelligence tracing some of the attacks to hackers linked to the People’s Liberation Army (PLA), according to former intelligence officials. None of that evidence is public, however, and China’s authorities have for years denied any involvement.
Up to now, private-sector researchers such as Stewart have had scant success putting faces to the hacks. There have been faint clues left behind -- aliases used in domain registrations, old online profiles, or posts on discussion boards that give the odd glimpse of hackers at work -- but rarely an identity. Occasionally, though, hackers mess up. Recently, one hacker’s mistakes led a reporter right to his door.

Puzzle Solving

Stewart works in a dingy gray building surrounded by a barbed-wire fence. A small sign on a keycode-locked door identifies it as Dell SecureWorks. With one other researcher, Stewart runs a patchwork of more than 30 computers that fill his small office. As he examines malware samples, he shifts between data-filled screens and white boards scribbled with technical terms and notes on Chinese intelligence agencies.

The computers in his office mostly run programs he wrote himself to dissect and sort the malware and figure out whether he's dealing with variations of old code or something entirely new. As the computers turn up code, Stewart looks for signature tricks that help him identify the work of an author or a team; software writers compare it with the unique slant and curlicues of individual handwriting. It's a methodical, technical slog that would bore or baffle most people but suits Stewart. He clearly likes patterns. After work, he relaxes with a 15-minute session on his drum kit, playing the same phrase over and over.

Important Clues

A big part of Stewart's task is figuring out how malware is built, which he does to an astonishing level of detail. He can tell the language of the computer on which it was coded -- helping distinguish the malware deployed by Russian criminal syndicates from those used by Chinese spies. The most important thing he does, however, is figure out who or what the software is talking to. Once inside a computer, malware is set up to signal a server or several servers scattered across the globe, seeking further marching orders. This is known in the information security business as "phoning home." Stewart and his fellow sleuths have found tens of thousands of such domains, known as command and control nodes, from which the hackers direct their attacks.

Discovery of a command node spurs a noticeable rise in pitch in Stewart's voice, which is about as much excitement as he displays to visitors. If a company getting hacked knows the Internet Protocol (IP) address of a command node, it can shut down all communication with that address. "Our top objective is to find out about the tools and the techniques and the malware that they're using, so we can block it," Stewart says.

Fake Names

The Internet is like a map, and every point -- every IP -- on that map belongs to someone with a name and an address

recorded in its registration. Spies, naturally, tend not to use their real names, and with most of the Internet addresses Stewart examines, the identifying details are patently fake. But there are ways to get to the truth.

In March 2011, Stewart was examining a piece of malware that looked different from the typical handiwork of Russian or Eastern European identity thieves. As he began to explore the command nodes connected to the suspicious code, Stewart noticed that since 2004, about a dozen had been registered under the same one or two names -- Tawnya Grilth or Eric Charles -- both listing the same Hotmail account and usually a city in California. Several were registered in the wonderfully misspelled city of Sin Digoo.

Spying Teams

Some of the addresses had also figured in Chinese espionage campaigns documented by other researchers. They were part of a block of about 2,000 addresses belonging to China Unicom, one of the country's largest Internet service providers. Trails of hacks had led Stewart to this cluster of addresses again and again, and he believes they are used by one of China's top two digital spying teams, which he calls the Beijing Group. This is about as far as Stewart and his fellow detectives usually get -- to a place and a probable group, but not to individual hackers.

But he got a lucky break over the next few months.

Tawnya Grilth registered a command node using the URL dellpc.us. It was a little too close to the name of Stewart's employer. So Stewart says he contacted Icann (the Internet Corporation for Assigned Names and Numbers), the organization that oversees Internet addresses and arbitrates disputes over names. Stewart argued that by using the word Dell, the hackers had violated his employer's trademark. Grilth never responded, and Icann agreed with Stewart and handed over control of the domain. By November 2011 he could see hacked computers phoning home from all over the world -- he was watching an active espionage campaign in progress.

Asian Targets

He monitored the activity for about three months, slowly identifying victim computers. By January 2012, Stewart had mapped as many as 200 compromised machines across the globe. Many were within government ministries in Vietnam, Brunei, and Myanmar, as well as oil companies, a newspaper, a nuclear safety agency, and an embassy in mainland China. Stewart says he'd never seen such extensive targeting focused on these countries in Southeast Asia. He broadened his search of IP addresses

registered either by Tawnya Grilth or “her” e-mail address, jeno_1980@hotmail.com, and found several more. One listed a contact with the handle xxgchappy. The new addresses led to even more links, including discussion board posts on malware techniques and the website rootkit.com, a malware repository where researchers study hacking techniques from all over the world.

A Discovery

Then Stewart discovered something much more unusual: One of the domains hosted an actual business -- one that offered, for a fee, to generate positive posts and “likes” on social network sites such as Twitter and Facebook. Stewart found a profile under the name Tawnya on the hacker forum BlackHatWorld promoting the site and a PayPal account that collected fees and funnelled them to a Gmail account that incorporated the surname Zhang. Stewart was amazed that the hacker had exposed his or her personal life to such a degree.

In February 2012, Stewart published a 19-page report on SecureWorks’ website to coincide with the RSA Conference in San Francisco, one of the biggest security industry events of the year. He prefaced it with an epigraph from Sun Tzu’s The Art of War: “We cannot enter into informed alliances until we are acquainted with the designs of our neighbors and the plans of our adversaries.”

Stewart didn’t pursue Zhang. His job was done. He learned enough to protect his customers and moved on to the other countless bits of malware. But his report generated interest in the security world, because it’s so difficult to find any traces of a hacker’s identity.

Unmasking Tawnya

In particular, Stewart’s work intrigued another researcher who immediately took up the challenge of unmasking Tawnya Grilth. That researcher is a 33-year-old who blogs under the name Cyb3rsleuth, an identity he says he keeps separate from his job running an India-based computer intelligence company. He asked that his name not be used to avoid unwanted attention, including hacking attempts on his company.

Cyb3rsleuth says he’d already found a calling in outing the identities of Eastern European hackers and claims to have handed over information on two individuals to government authorities. Stewart’s work inspired him to post his findings publicly, and he says he hopes that unearthing more details on individual hackers will give governments the evidence to take action. The hackers are human and makes mistakes, so the trick is finding

the connection that leads to a real identity, he says.

Personal Photos

As Stewart's new collaborator dug in, the window into Tawnya Grilth's world expanded. There were posts on a car forum; an account on a Chinese hacker site; and personal photos, including one showing a man and a woman bundled up against the wind at what looked like a tourist site with a pagoda in the background.

Cyb3rsleuth followed the trail of the hacker's efforts to drum up business for the social media promotion service through aliases and forums tied to the Hotmail account. He eventually stumbled on a second business, this one with a physical location. The company, Henan Mobile Network, was a mobile-phone wholesaler, according to business directories and online promotional posts. The shop's website was registered using the Jeno Hotmail account and the Eric Charles pseudonym.

Cyb3rsleuth checked an online Chinese business directory for technology companies and turned up not only a telephone number for the company but also a contact name, Mr. Zhang, and an address in Zhengzhou, a city of more than 8 million in the central Chinese province of Henan.

Zhang Changhe

The directory listing gave three account numbers for the Chinese instant-messaging service called QQ. The service works along the lines of MSN Messenger, with each account designated by a unique number. One of those accounts used an alternate e-mail that incorporated the handle xxgchappy and listed the user's occupation as "education."

Putting that e-mail into Chinese search engines, Cyb3rsleuth found it was also registered on Kaixin001.com, a Chinese Facebook-style site, to a Zhang Changhe in Zhengzhou. Zhang's profile image on Kaixin is of a blooming lotus, a traditional Buddhist symbol. Going back to the QQ account, Cyb3rsleuth found a blog linked to it, again with a Buddha-themed profile picture, whose user went by Changhe -- the same pronunciation as the Kaixin user's given name, though rendered in different characters.

The blog contained musings on Buddhist faith, including this, from a post written in Chinese and titled "repentance":

"It's Jan. 31, 2012 today, I've been a convert to Buddhism for almost five years. In the past five years, I broke all the Five Precepts -- no killing living beings, no stealing, no sexual misconduct, no lies, and no alcohol, and I feel so repentant."

Amid his list of sins, from lack of sympathy to defensiveness to

lying, is No. 4: “I continuously and shamelessly stole, hope I can stop in the future.”

Peugeot Club

The same QQ number appears on an auto forum called xCar, where the user is listed as belonging to a club for owners of the Dongfeng Peugeot 307 -- a sporty four-door popular among China’s emerging middle class -- and where the user asked, circa 2007, about places to buy a special license-plate holder.

In a photo taken in 2009, Zhang stands on a beach, squinting into the sun with his back to the waves, arm in arm with a woman the caption says is his wife -- the same person as in the pagoda picture. His bushy hair is cut short over a young face.

In March, Cyb3rsleuth published what he found on his personal blog, hoping that someone -- governments, the research community, or some of the many hacking victims -- would act. He knows of no response so far. Still, he’s excited. He’d found the face of a ghost, he says.

Zhang’s Office

The city of Zhengzhou sprawls near the Yellow River in Henan province. The municipal government website describes it as “an example of a remarkably fast-changing city in China (without minor tourism clutter).” Kung Fu fans pass through on their way to the Shaolin Temple, a center of Buddhism and martial arts, 56 miles to the southwest. The city mostly serves as a gigantic transit hub for people and goods moving by rail to other places all over China.

About a 500-meter walk south from the central railway station is a tan, seven-story building with a dirty facade and red characters that read Central Plains Communications Digital City. The building is full of tiny shops, many selling electronics. The address listed for Zhang’s mobile-phone business is on the fourth floor, room A420.

Under dim fluorescent lights, two young clerks tell a reporter that they don’t know Zhang Changhe or Henan Mobile Network. The commercial manager of the building, Wang Yan, says the previous tenant of A420 moved out three years ago; she says she has no idea what the business had been, except that the proprietors weren’t there very often and that the operation didn’t last long.

Espionage Research

A Chinese-language search on Google turns up a link to

several academic papers co-authored by a Zhang Changhe. One, from 2005, relates to computer espionage methods. He also contributed to research on a Windows rootkit, an advanced hacking technique, in 2007. In 2011, Zhang co-authored an analysis of the security flaws in a type of computer memory and the attack vectors for it. The papers identified Zhang as working at the PLA Information Engineering University. The institution is one of China's principal centers for electronic intelligence, where professors train junior officers to serve in operations throughout China, says Mark Stokes of the Project 2049 Institute, a think tank in Washington. It's as if the U.S. National Security Agency had a university.

"Not Sure"

The gated campus of the PLA Information Engineering University is in Zhengzhou, about four miles north of Zhang Changhe's mobile shop. The main entrance is at the end of a tree-lined lane, and uniformed men and women come and go, with guards checking vehicles and identification cards. Reached on a cell-phone number listed on the QQ blog, Zhang confirms his identity as a teacher at the university, adding that he was away from Zhengzhou on a work trip. Asked if he still maintained the Henan Mobile telephone business, he says: "No longer, sorry." About his links to hacking and the command node domains, Zhang says: "I'm not sure." About what he teaches at the university: "It's not convenient for me to talk about that." He denies working for the government, says he won't answer further questions about his job, and hangs up.

Stewart continues to uncover clues that point to Zhang's involvement in computer network intrusions. A piece of malware SecureWorks discovered last year and dubbed Mirage infected more than 100 computers, mainly in Taiwan and the Philippines. Tawnya Grilth owned one of the command domains.

Zhang Again

Late last year, Stewart was looking at malware hitting Russian and Ukrainian government and defense targets. The only other sample of that kind of malware he could find in his database was one that phoned home to a command node at AlexaUp.info. The billing name used in the registration: Zhang Changhe. Stewart says Zhang is affiliated with the Beijing Group, which probably involves dozens of people, from programmers to those handling the infrastructure of command centers to those who translate stolen documents and data.

As Stewart discusses this, his voice is flat. He's realistic. Outing one person involved in the hacking teams won't

stop computer intrusions from China. Zhang's a cog in a much larger machine and, given how large China's operations have become, finding more Zhangs may get easier. Show enough of this evidence, Stewart figures, and eventually the Chinese government can't deny its role.

"It might take several more years of piling on reports like that to make that weight of evidence so strong that it's laughable, and they say, 'Oh, it was us,' " says Stewart. "I don't know that they'll stop, but I would like to make it a lot harder for them to get away with it."

--Editors: Jim Aley, Marcia Myers

To contact the reporters on this story: Dune Lawrence in New York at 1-212-617-4510 or dlawrence6@bloomberg.net; Michael Riley in Washington at 1-202-624-1982 or michaelriley@bloomberg.net.

To contact the editor responsible for this story: Marcia Myers at +44-20-3216-4172 or mmyers20@bloomberg.net