How the Chinese cyberthreat has evolved

October 5 2017, by Dorothy Denning

Credit: AI-generated image (disclaimer)

With more than half of its 1.4 billion people online, the world's most populous country is home to a slew of cyberspies and hackers. Indeed, China has likely stolen more secrets from businesses and governments than any other country.

Covert espionage is the main Chinese cyberthreat to the U.S. While disruptive cyberattacks occasionally come from China, those that cause

overt damage, like destroying data or causing power outages, are more common from the other top state threats, namely Russia, Iran and North Korea.

But Chinese cyberaggression toward the U.S. has been evolving. Before their espionage became a serious threat, Chinese hackers were conducting disruptive cyberattacks against the U.S. and other countries.

Hackers unite

Chinese hackers were among the first to come together in defense of their country. Their first operation against the U.S. occurred in 1999 during the Kosovo conflict, when the U.S. inadvertently bombed the Chinese embassy in Belgrade, killing three Chinese reporters. The patriotic hackers planted messages denouncing "NATO's brutal action" on several U.S. government websites.

Chinese hackers struck the U.S. again in 2001 after a Chinese fighter plane collided with a U.S. reconnaissance aircraft. The midair collision killed the Chinese pilot and led to the forced landing and detention of the American crew. Both Chinese and American hackers responded with disruptive cyberattacks, with the Chinese hackers defacing thousands of U.S.-based websites, including the White House site.

What is especially important about this incident, though, is what happened next. The People's Daily, China's Communist Party newspaper, issued an editorial decrying the attack against the White House. The paper called it, and the other attacks, "web terrorism" and "unforgivable acts violating the law." On the anniversary of the incident in 2002, the government asked Chinese hackers to forgo further attacks against U.S.-based sites. They complied.

That was the last big cyberattack from Chinese patriotic hackers against

the U.S. While Russia seems to condone, if not outright encourage or even sponsor, its patriotic hackers, China has taken a stance against that sort of activity, at least with respect to U.S.-based sites.

Targets at home

In addition to reining in its patriotic hackers, China appears to have refrained from conducting cyberattacks that cause overt damage to critical infrastructure in other countries, like the Russians did to Ukraine's power grid. However, it has used disruptive cyberattacks to help enforce censorship policies within its own borders.

The Chinese government's "Great Firewall" keeps internet users in China from accessing censored foreign sites such as those that advocate Tibetan autonomy. Users' traffic is filtered based on domain names, internet addresses and keywords in web addresses.

Chinese hackers have also used denial-of-service attacks to temporarily take out sites whose activity the government wants to block. These attacks overwhelm target servers with large amounts of activity, preventing others from using the sites and often knocking the servers offline.

Back in 1999, the government launched DoS attacks against foreign websites associated with Falun Gong, a spiritual movement banned in China. Then in 2011, a Chinese military TV program showed software tools being used in possible cyberattacks against Falun Gong sites in the U.S. The tools were developed by the Electrical Engineering University of China's armed forces, the People's Liberation Army.

More recently, in 2015, U.S. and other foreign users visiting sites running analytics software from the Chinese search engine provider Baidu unwittingly picked up malware. The malicious code was injected

into traffic going back to the users by a device collocated with the Great Firewall. The malware then launched DDoS attacks against GreatFire.org, a site that helps Chinese users evade censorship, and the Chinese language edition of The New York Times.

Espionage at the forefront

By 2003, China's interest in cyberespionage was apparent: A series of cyberintrusions that U.S. investigators code-named "Titan Rain" was traced back to computers in southern China. The hackers, believed by some to be from the Chinese army, had invaded and stolen sensitive data from computers belonging to the U.S. Department of Defense, defense contractors and other government agencies.

Titan Rain was followed by a rash of espionage incidents that originated in China and were given code names like "Byzantine Hades," "GhostNet" and "Aurora." The thieves were after a wide range of data.

They stole intellectual property, including Google's source code and designs for weapons systems. They took government secrets, including user names and passwords. And they compromised data associated with Chinese human rights activists, including their email messages. Typically, the intrusions started with spear-phishing.

In 2013, the American cyberintelligence firm Mandiant, now part of FireEye, issued a landmark report on a Chinese espionage group it named "Advanced Persistent Threat 1." According to the report, APT1 had stolen hundreds of terabytes of data from at least 141 organizations since 2006.

The Mandiant report gave details of the operations and provided evidence linking those thefts to Unit 61398 of the People's Liberation Army – and named five officers of the unit. This was the first time any

security firm had publicly disclosed data tying a cyberoperation against the U.S. to a foreign government. In 2014, the U.S. indicted the five Chinese officers for computer hacking and economic espionage.

Mandiant described APT1 as "one of more than 20 APT groups with origins in China." Many of these are believed to be associated with the government. A report from the nonprofit Institute for Critical Infrastructure Technology describes 15 state-sponsored advanced persistent threat groups, including APT1 and two others associated with PLA units. The report does not identify sponsors for the remaining groups.

The Five-Year Plan

According to the institute, China's espionage supports the country's 13th Five-Year Plan (covering the years 2016 to 2020), which calls for technology innovations and socioeconomic reforms. The goal is "innovative, coordinated, green, open and inclusive growth." The ICIT report said most of the technology needed to realize the plan will likely be acquired by stealing trade secrets from companies in other countries.

In its 2015 Global Threat Report, the American cyberintelligence firm CrowdStrike identified dozens of Chinese adversaries targeting business sectors that are key to the Five-Year Plan. It found 28 groups going after defense and law enforcement systems alone. Other sectors victimized worldwide included energy, transportation, government, technology, health care, finance, telecommunications, media, manufacturing and agriculture.

China's theft of military and trade secrets has been so rampant that editorial cartoonists Jeff Parker and Dave Granlund depicted it as "Chinese takeout."

US-China agreement

In September 2015, President Obama met with China's President Xi Jinping to address a range of issues affecting the two countries. With respect to economic espionage, they agreed that their governments would not conduct or knowingly support cyber-enabled theft of business secrets that would provide competitive advantage to their commercial sectors. They did not agree to restrict government espionage, a practice that countries generally consider to be fair game.

In June 2016, FireEye reported that since 2014 there had been a dramatic drop in cyberespionage from 72 suspected China-based groups. FireEye attributed the reduction to several "factors including President Xi's military and political initiatives, the widespread exposure of Chinese cyberoperations, and mounting pressure from the U.S. Government." The ICIT believes China may also be asserting greater control over its operatives and focusing on unspecified high-priority targets.

The U.S.-China agreement also calls for the two countries to cooperate in fighting cybercrime. Just weeks after the deal was signed, China announced it had arrested hackers connected with the 2015 intrusions into the Office of Personnel Management's database. Those had exposed highly sensitive personal and financial data of about 22 million federal employees seeking security clearances. The Washington Post observed that the arrests could "mark the first measure of accountability for what has been characterized as one of the most devastating breaches of U.S. government data in history."

The cyberthreat to the U.S. from China is mostly one of espionage, and even that threat seems to be declining. Nevertheless, companies need to be wary of losing their data, not just to China, but to any country or group seeking to profit from U.S. trade secrets and other sensitive data.

That calls for staying ahead of the cybersecurity curve.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: How the Chinese cyberthreat has evolved (2017, October 5) retrieved 26 April 2024 from https://phys.org/news/2017-10-chinese-cyberthreat-evolved.html