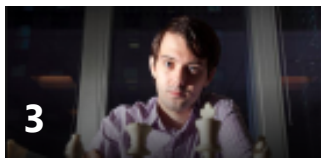
Hacker tracked to China's military

1918 tsar murder case reopened



CEO recedes from public

Meet the 5-year-old g who hugged the pop

Cyber Sleuths Track Hacker to China's Military

1 / 18

The Wall Street Journal.
Josh Chin
5 hrs ago

KUNMING, China—The email attachment would tempt anyone following the diplomatic standoff between China and other countries in the South China Sea. The Microsoft Word document contained text and photos depicting Thai naval personnel capturing Vietnamese fishermen and forcing them to kneel at gunpoint.

But the attachment was a decoy: Anyone who opened it inadvertently downloaded software that searched their computers for sensitive information and sent it to an obscure corner of the Internet. Manning that corner, according to a new report from U.S. security researchers, was Ge Xing, a member of a Chinese military reconnaissance unit.

The growing reach of China's army of cyberwarriors has become a flash point in relations between Beijing and Washington that President Barack Obama says will be a focus during Chinese President Xi Jinping 's state visit to the U.S. this week.

Cyberspace is the newest domain in warfare, and China's relentless testing of its boundaries has flustered the U.S. The story of the Chinese military staffer's alleged involvement in hacking provides a detailed look into Beijing's sprawling state-controlled cyberespionage machinery.

Mr. Ge doesn't appear to fit the hacker stereotype. His published academic papers identify him as an expert in a nontechnical subject: Thai politics. Frequent posts on Chinese social media that researchers have linked to him show him to be a new father and avid bicyclist who drives a white Volkswagen Golf sedan and occasionally criticizes the government.

But his activity elsewhere on the Internet links him to a Chinese hacker collective that attacks targets in an area of strategic interest to the U.S., according to the report by cybersecurity concern ThreatConnect and security consulting firm Defense Group Inc.

The U.S. has been caught flat-footed in recent months by a string of cyberintrusions in which Chinese state-sponsored hackers are the leading suspects. They include the theft of sensitive personal data on millions of government employees from computers at the U.S. Office of Personnel Management, and similar network breaches at health insurers and other companies.

Under pressure to respond, the White House has begun preparing a list of sanctions against Chinese companies that U.S. officials believe have benefited from cybertheft of U.S. corporate secrets, Mr. Obama said last week. Those sanctions, if implemented, wouldn't address state-to-state hacking.

Beijing has bristled at U.S. finger-pointing on cybersecurity and portrayed itself as a victim of hacking, pointing to disclosures by former U.S. security contractor Edward Snowden of U.S. government cyberspying on China. "Cybertheft of commercial secrets and hacking attacks against government networks are both illegal," Mr. Xi told the Journal in a written interview prior to embarking on his U.S. visit. "Such acts are criminal offenses and should be punished according to law and relevant international conventions."

The ThreatConnect-DGI report helps throw new light on a still little-understood aspect of China's cyber operations: the relationship between the country's military and an aggressive corps of Chinese-speaking hackers that appear to be pressing the country's interests abroad.

Through accounts allegedly tied to Mr. Ge, the report draws a direct link between his unit, People's Liberation Army Unit 78020, a military intelligence arm based in China's southwest, and a hacker collective known as Naikon that security researchers say has successfully penetrated key computer networks in countries competing with China for control over the South China Sea.

"What we see from Chinese intrusions is that they have a very grass roots, bottom-up kind of model," said James Mulvenon, director of DGI's Center for Intelligence Research and Analysis.

"They have a lot of groups that are encouraged with relatively vague guidance to go out and develop hundreds of accesses and bring back lots of data."

Two academic papers on Thailand's political situation Mr. Ge published in 2008 identify him as working for Unit 78020, a technical reconnaissance bureau based in the southwestern Chinese city of Kunming. It is one of more than two dozen such bureaus within the PLA tasked with intelligence gathering, analysis and computer network defense and exploitation, according to Mark Stokes, executive director at Virginia think tank Project 2049 Institute and an authority on the role of China's military in signals intelligence like cyberspying.

Unit 78020 is controlled by the PLA's Chengdu Military Region, which is responsible for securing Tibet as well as China's borders with Vietnam, Myanmar and India. Another reconnaissance bureau under the Chengdu Military Region was responsible for the hacking of computer networks connected to exiled Tibetan spiritual leader the Dalai Lama, Mr. Stokes said. Given the region's focus on the border, "it also makes sense that they would do collections related to the South China Sea," he said.

Staff with Unit 78020's propaganda office declined requests for an interview. A spokesman for Chengdu Military Region referred questions to the defense ministry, which didn't respond to requests for comment. The foreign ministry also didn't respond to requests for comment.

The ThreatConnect-DGI report makes the connection between the unit and the hacking group by matching Mr. Ge's alleged activity on social media, where he uses the name greensky27, with activity on a part of Naikon's network that also uses the greensky27 name. The Wall Street Journal reviewed the report before its publication, verifying its observations of Mr. Ge's social-media activity and other evidence linking him to Unit 78020 and Naikon.

Researchers at PassiveTotal, a U.S. cybersecurity threat analysis company that provided some of the data for the report, said the report offered fair insight into how data about the use of hackers' infrastructure can be used to track and identify potential threats.

In a brief phone conversation with the Journal in August, Mr. Ge confirmed he uses the greensky27 name on social media but declined to speak further when told he was the subject of a report. "If you publish, I'll call the police," he said and hung up before hearing the substance of the report. He didn't answer subsequent phone calls or questions later sent by text message.

The greensky27 Naikon domain went dormant within an hour of the Journal's phone conversation with Mr. Ge, according to ThreatConnect. Recent visits to the domain show it is still offline.

Named by experts after a piece of code found in malware it once used, Naikon sends well-crafted emails to trick recipients into opening attachments infected with malicious software, according to researchers. Infected attachments they have used include a calendar of Laotian

beauty contestants, news stories and memos on strategic topics in English and local languages, and memos that appear to be based on classified information, according to a May report by Russian antivirus maker Kaspersky Lab.

Relying on this technique—known as spearphishing—Naikon has penetrated the networks of governments, military, media and energy companies in Vietnam, the Philippines and other countries throughout Southeast Asia, Kaspersky said. "Their success rate has been high," said Kurt Baumgartner, principal security researcher at Kaspersky. "When they want to get in, they get in."

China's claims to sovereignty over vast swaths of the South China Sea—one of the world's busiest shipping routes—have sparked conflict with many of its neighbors, including U.S. ally the Philippines. Beijing has rejected U.S. criticisms of its claims, saying territorial disputes should be settled bilaterally between those directly affected. It has also pressed ahead with island-building in disputed areas, raising tensions the U.S. fears could destabilize the region.

The malicious software Naikon uses to spy on its targets is "stone age" compared with what Russian hackers use, said Richard Barger, chief intelligence officer at ThreatConnect, but it doesn't necessarily need to be advanced. "The targets they're most likely going up against, this would be sophisticated for them," he said.

© Yao Dawei/Xinhua/Zuma Press

ThreatConnect said it found Mr. Ge through a break in Naikon's usual pattern. To siphon off stolen information without being detected, Naikon uses hundreds of special Internet domains—akin to Web addresses—that are able to connect at various places around the Internet. The names of most of those domains appear to refer to targets or are designed to mimic legitimate websites in target countries, but the greensky27 domain didn't fit either of those criteria, ThreatConnect said.

Looking at the greensky27 domain's activity over a five-year period, researchers found it making an unusually large number of long-lasting connections to Internet addresses in the southwestern Chinese city of Kunming, according to the report. Chinese-language analysts at DGI followed that lead and discovered multiple Internet accounts making references to Kunming that used the same greensky27 name.

Comparing the domain with the social-media accounts, the researchers found a pattern. In February 2012, for example, the domain made a series of connections to Internet servers in Beijing on the same dates a user posting under greensky27 on Tencent Holdings Ltd.'s microblogging platform indicated that he was visiting the city. The domain went dormant for more than a week in November that same year, starting the day a user named greensky27 posted a message announcing the birth of a boy surnamed Ge on a discussion board maintained by Chinese search giant Baidu Inc., the report said.

DGI said it found a clue to Mr. Ge's identity in photos posted on the greensky27 Tencent account in 2013 that showed a visit to what it called the Ge family ancestral temple in Yuxi county, about 50 miles south of Kunming. Digging around further online, DGI said it found Mr. Ge's full name and phone number, as well as the academic papers listing Mr. Ge as working for Unit 78020. Mr. Ge's rank in the military and specific role within the unit are unclear, the researchers said.

A series of skyline snapshots Mr. Ge allegedly posted online during work hours between 2011 and 2013 confirm an affiliation with the military. Taken from the same vantage point, they show a view of a tall apartment tower that could have been captured only from inside a military complex located in downtown Kunming.

Another series of photos showed snow-covered cars in a parking lot with a water tower in the background that also indicated they were shot from inside the military compound, the report said. "Little Golf and his buddies," he wrote, in apparent reference to his car and to those parked around it.

On a recent visit to the complex by a Journal reporter, security personnel confirmed the compound belongs to Unit 78020 of the People's Liberation Army. Staff with the unit's propaganda office wouldn't say whether Mr. Ge worked there.

The user was coy about discussing his military background on social media. The Tencent account listed him as having attended PLA International Studies University in 1998. In 2014, he posted photos of a visit to the university's campus in the city of Nanjing with a short message: "Just posting photos, not explaining, look for yourself." A couple of weeks later he posted photos of a PLA firefighter demonstration and from an event celebrating the PLA's 87th anniversary. "Not explaining," he wrote again.

Some of his early posts contained cryptic political and social commentary. "Faith = Whatever the party tells me to do, I do," he wrote in a post in July 2012. In another post the previous fall, he repeated a common joke about China's state TV broadcaster's tendency to emphasize the positive in its nightly news show: "I have a dream—to always live inside Xinwen Lianbo."

After the birth of his son in late 2012, his posts focused on family life, the weather and travel. One post early the following year featured a picture of a cluster of villas. "Ten year goal," he

wrote. The Tencent account was deleted within a day of the Journal's call to Mr. Ge.

Activity on the greensky27 domain indicates a relatively regular work schedule. The domain connected to the Naikon network around 9 a.m., went quiet around lunch and typically signed off around 6 p.m., according to the report.

The domain also tended to go dormant around China's annual Spring Festival holiday, the report said, but there were exceptions. In early 2012, according to ThreatConnect, the domain went silent for Spring Festival only to suddenly come to life the weekend of Jan. 27, a day after news broke that a delegation from the Philippines had launched talks in Washington over military cooperation with the U.S.

Data collected by ThreatConnect show frequent connections between the hacker domain and Internet addresses in Thailand beginning in 2012. Those connections began to tail off in May 2014, after the U.S. indictments of five PLA officers on charges of commercial cybertheft. China has denied the allegations.

The social-media feeds attributed to Mr. Ge indicate he spends much of his time either playing with his son or riding, repairing and talking about his mountain bike. Xiong Junwu, a bike shop owner and founder of Kunming's Fattire Fun Bike Club, recognized a photo of Mr. Ge and said he occasionally joined the club's weekly rides in the Kunming area.

Like many Chinese outdoors enthusiasts, Mr. Ge sometimes turned wistful when contemplating polluted skies. "Today's air is only average," he wrote next to a photo of a gray sky taken from inside the Unit 78020 compound. "Wishing peace to everyone and tranquility to the world."

‹ PREVIOUS NEXT ›

Go to MSN Home

Go to MSN News

107 COMMENTS | JOIN THE CONVERSATION

MORE IN WORLD

Divided EU leaders to offer cash for Syria refugees

European Union leaders could promise billions of euros in new funding for Syrian

Reuters

Egypt pardons 100 prisoners, including Al Jazeera journalists

Egypt's President Abdel Fatta al-Sisi pardoned 100 prisoners, including Canadian

Reuters

'Witchcraft' Island Reveals Evidence of Stone Age Rituals

A Stone Age site where cave rituals may have been performed some 9,000 years

LiveScience

Burkina coup: 'Civilian rule restored'

Burkina Faso's interim President Michel Kafando has said he is back in charge and

BBC News

Amid battle against IS, Iraqis face cholera outbreak

Iraq, which is already facing a prolonged battled against the Islamic State group and mass

Associated Press

Philippine gunmen haul hostages into remote mountain region

Gunmen holding three foreigners and one Filipina hostage have slipped past a

AFP

MORE FROM THE WALL STREET JOURNAL.

They May Wear McDonald's Hats, but They Work for Bob

As long as “some guy named Bob” is paying the workers at a McDonald’s franchised restaurant, only Bob should be treated as their employer;

The Wall Street Journal.

Help a Government in Exile to Reclaim Syria

I suggest Mr. Eid, along with other capable Syrians, work to form a democratic Syrian government in exile and strive to gain recognition from the West and the U.N.

The Wall Street Journal.