The New York Times | https://nyti.ms/XZRMHn

TECHNOLOGY

Chinese Army Unit Is Seen as Tied to Hacking Against U.S.

By DAVID E. SANGER, DAVID BARBOZA and NICOLE PERLROTH FEB. 18, 2013

On the outskirts of Shanghai, in a run-down neighborhood dominated by a 12-story white office tower, sits a People's Liberation Army base for China's growing corps of cyberwarriors.

The building off Datong Road, surrounded by restaurants, massage parlors and a wine importer, is the headquarters of P.L.A. Unit 61398. A growing body of digital forensic evidence — confirmed by American intelligence officials who say they have tapped into the activity of the army unit for years — leaves little doubt that an overwhelming percentage of the attacks on American corporations, organizations and government agencies originate in and around the white tower.

An unusually detailed 60-page study, to be released Tuesday by Mandiant, an American computer security firm, tracks for the first time individual members of the most sophisticated of the Chinese hacking groups — known to many of its victims in the United States as "Comment Crew" or "Shanghai Group" — to the doorstep of the military unit's headquarters. The firm was not able to place the hackers inside the 12-story building, but makes a case there is no other plausible explanation for why so many attacks come out of one comparatively small area.

"Either they are coming from inside Unit 61398," said Kevin Mandia, the founder and chief executive of Mandiant, in an interview last week, "or the people who run the most-controlled, most-monitored Internet networks in the world are clueless about thousands of people generating attacks from this one neighborhood."

Other security firms that have tracked "Comment Crew" say they also believe the group is state-sponsored, and a recent classified National Intelligence Estimate, issued as a consensus document for all 16 of the United States intelligence agencies, makes a strong case that many of these hacking groups

Help Times journalists uncover the next big story.

Subscribe to The New York Times.

See where The New York Times will take you.

SEE MY OPTIONS

0 articles remaining this month

Already a subscriber? **Log in.**

power grid, gas lines and waterworks. According to the security researchers, one target was a company with remote access to more than 60 percent of oil and gas pipelines in North America. The unit was also among those that attacked the computer security firm RSA, whose computer codes protect confidential corporate and government databases.

Contacted Monday, officials at the Chinese embassy in Washington again insisted that their government does not engage in computer hacking, and that such activity is illegal. They describe China itself as a victim of computer hacking, and point out, accurately, that there are many hacking groups inside the United States. But in recent years the Chinese attacks have grown significantly, security researchers say. Mandiant has detected more than 140 Comment Crew intrusions since 2006. American intelligence agencies and private security firms that track many of the 20 or so other Chinese groups every day say those groups appear to be contractors with links to the unit.

And the Chinese Ministry of Foreign Affairs said Tuesday that the allegations were “unprofessional.”

“Making unfounded accusations based on preliminary results is both irresponsible and unprofessional, and is not helpful for the resolution of the relevant problem,” said Hong Lei, a ministry spokesman. “China resolutely opposes hacking actions and has established relevant laws and regulations and taken strict law enforcement measures to defend against online hacking activities.”

While the unit’s existence and operations are considered a Chinese state secret, Representative Mike Rogers of Michigan, the Republican chairman of the House Intelligence Committee, said in an interview that the Mandiant report was “completely consistent with the type of activity the Intelligence Committee has been seeing for some time.”

The White House said it was “aware” of the Mandiant report, and Tommy Vietor, the spokesman for the National Security Council, said, “We have repeatedly raised our concerns at the highest levels about cybertheft with senior Chinese officials, including in the military, and we will continue to do so.”

The United States government is planning to begin a more aggressive defense against Chinese hacking groups, starting on Tuesday. Under a directive signed by President Obama last week, the government plans to share with American Internet providers information it has gathered about the unique digital signatures of the largest of the groups, including Comment Crew and others emanating from near where Unit 61398 is based.

But the government warnings will not explicitly link those groups, or the giant computer servers they use, to the Chinese army. The question of whether to publicly name the unit and accuse it of widespread theft is the subject of ongoing debate.

“There are huge diplomatic sensitivities here,” said one intelligence official, with frustration in his voice.

But Obama administration officials say they are planning to tell China’s new leaders in coming weeks that the volume and sophistication of the attacks have become so intense that they threaten the fundamental relationship between Washington and Beijing.

The United States government also has cyberwarriors. Working with Israel, the United States has used malicious software called Stuxnet to disrupt Iran’s uranium enrichment program. But government officials insist they operate under strict, if classified, rules that bar using offensive weapons for nonmilitary purposes or stealing corporate data.

The United States finds itself in something of an asymmetrical digital war with China. “In the cold war, we were focused every day on the nuclear command centers around Moscow,” one senior defense official said recently. “Today, it’s fair to say that we worry as much about the computer servers in Shanghai.”

A Shadowy Unit

Unit 61398 — formally, the 2nd Bureau of the People’s Liberation Army’s General Staff Department’s 3rd Department — exists almost nowhere in official Chinese military descriptions. Yet intelligence analysts who have studied the group say it is the central element of Chinese computer espionage. The unit was described in 2011 as the “premier entity targeting the United States and Canada, most likely focusing on political, economic, and military-related intelligence” by the Project 2049 Institute, a nongovernmental organization in Virginia that studies security and policy issues in Asia.

While the Obama administration has never publicly discussed the Chinese unit’s activities, a secret State Department cable written the day before Barack Obama was elected president in November 2008 described at length American concerns about the group’s attacks on government sites. (At the time American intelligence agencies called the unit “Byzantine Candor,” a code word dropped after the cable was published by WikiLeaks.)

The Defense Department and the State Department were particular targets, the cable said, describing how the group’s intruders send e-mails, called “spearphishing” attacks, that placed malware on target computers once the recipient clicked on them. From there, they were inside the systems.

American officials say that a combination of diplomatic concerns and the desire to follow the unit's activities have kept the government from going public. But Mandiant's report is forcing the issue into public view.

For more than six years, Mandiant tracked the actions of Comment Crew, so named for the attackers' penchant for embedding hidden code or comments into Web pages. Based on the digital crumbs the group left behind — its attackers have been known to use the same malware, Web domains, Internet protocol addresses, hacking tools and techniques across attacks — Mandiant followed 141 attacks by the group, which it called "A.P.T. 1" for Advanced Persistent Threat 1.

"But those are only the ones we could easily identify," said Mr. Mandia. Other security experts estimate that the group is responsible for thousands of attacks.

As Mandiant mapped the Internet protocol addresses and other bits of digital evidence, it all led back to the edges of Pudong district of Shanghai, right around the Unit 61398 headquarters. The group's report, along with 3,000 addresses and other indicators that can be used to identify the source of attacks, concludes "the totality of the evidence" leads to the conclusion that "A.P.T. 1 is Unit 61398."

Mandiant discovered that two sets of I.P. addresses used in the attacks were registered in the same neighborhood as Unit 61398's building.

"It's where more than 90 percent of the attacks we followed come from," said Mr. Mandia.

The only other possibility, the report concludes with a touch of sarcasm, is that "a secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multiyear enterprise-scale computer espionage campaign right outside of Unit 61398's gates."

The most fascinating elements of the Mandiant report follow the keystroke-by-keystroke actions of several of the hackers who the firm believes work for the P.L.A. Mandiant tracked their activities from inside the computer systems of American companies they were invading. The companies had given Mandiant investigators full access to rid them of the Chinese spies.

One of the most visible hackers it followed is UglyGorilla, who first appeared on a Chinese military forum in January 2004, asking whether China has a "similar force" to the "cyber army" being set up by the American military.

By 2007 UglyGorilla was turning out a suite of malware with what the report called a "clearly identifiable signature." Another hacker, called "DOTA" by Mandiant, created e-mail accounts that were used to plant malware. That hacker was tracked frequently using a password that appeared to be based on his military unit's designation. DOTA and UglyGorilla both used the same I.P. addresses linked back to Unit 61398's neighborhood.

Mandiant discovered several cases in which attackers logged into their Facebook and Twitter accounts to get around China's firewall that blocks ordinary citizen's access, making it easier to track down their real identities.

Mandiant also discovered an internal China Telecom memo discussing the state-owned telecom company's decision to install high-speed fiber-optic lines for Unit 61398's headquarters.

China's defense ministry has denied that it is responsible for initiating attacks. "It is unprofessional and groundless to accuse the Chinese military of launching cyberattacks without any conclusive evidence," it said last month, one of the statements that prompted Mandiant to make public its evidence.

Escalating Attacks

Mandiant believes Unit 61398 conducted sporadic attacks on American corporate and government computer networks; the earliest it found was in 2006. Two years ago the numbers spiked. Mandiant discovered some of the intrusions were long-running. On average the group would stay inside a network, stealing data and passwords, for a year; in one case it had access for four years and 10 months.

Mandiant has watched the group as it has stolen technology blueprints, manufacturing processes, clinical trial results, pricing documents, negotiation strategies and other proprietary information from more than 100 of its clients, mostly in the United States. Mandiant identified attacks on 20 industries, from military contractors to chemical plants, mining companies and satellite and telecommunications corporations.

Mandiant's report does not name the victims, who usually insist on anonymity. A 2009 attack on Coca-Cola coincided with the beverage giant's failed attempt to acquire the China Huiyuan Juice Group for $2.4 billion, according to people with knowledge of the results of the company's investigation.

As Coca-Cola executives were negotiating what would have been the largest foreign purchase of a Chinese company, Comment Crew was busy rummaging through their computers in an apparent effort to learn more about Coca-Cola's negotiation strategy.

The attack on Coca-Cola began, like hundreds before it, with a seemingly innocuous e-mail to an executive that was, in fact, a spearphishing attack. When the executive clicked on a malicious link in the e-mail, it gave the attackers a foothold inside Coca-Cola's network. From inside, they sent confidential company files through a maze of computers back to Shanghai, on a weekly basis, unnoticed.

Two years later, Comment Crew was one of at least three Chinese-based groups to mount a similar attack on RSA, the computer security company owned by EMC, a large technology company. It is best known for its SecurID token, carried by employees at United States intelligence agencies, military contractors and many major companies. (The New York Times also uses the firm's tokens to allow access to its e-mail and production systems remotely.) RSA has offered to replace SecurID tokens for customers and said it had added new layers of security to its products.

As in the Coca-Cola case, the attack began with a targeted, cleverly fashioned poisoned e-mail to an RSA employee. Two months later, hackers breached Lockheed Martin, the nation's largest defense contractor, partly by using the information they gleaned from the RSA attack.

Mandiant is not the only private firm tracking Comment Crew. In 2011, Joe Stewart, a Dell SecureWorks researcher, was analyzing malware used in the RSA attack when he discovered that the attackers had used a hacker tool to mask their true location.

When he reverse-engineered the tool, he found that the vast majority of stolen data had been transferred to the same range of I.P. addresses that Mandiant later identified in Shanghai.

Dell SecureWorks says it believed Comment Crew includes the same group of attackers behind Operation Shady RAT, an extensive computer espionage campaign uncovered in 2011 in which more than 70 organizations over a five-year period, including the United Nations, government agencies in the United States, Canada, South Korea, Taiwan and Vietnam were targeted.

Infrastructure at Risk

What most worries American investigators is that the latest set of attacks believed coming from Unit 61398 focus not just on stealing information, but obtaining the ability to manipulate American critical infrastructure: the power grids and other utilities.

Staff at Digital Bond, a small security firm that specializes in those industrial-control computers, said that last June Comment Crew unsuccessfully attacked it. A part-time employee at Digital Bond received an e-mail that appeared to come from his boss, Dale Peterson. The e-mail, in perfect English, discussed security weaknesses in critical infrastructure systems, and asked the employee to click a link to a document for more information. Mr. Peterson caught the e-mail and shared it with other researchers, who found the link contained a remote-access tool that would have given the attackers control over the employee's computer and potentially given them a front-row seat to confidential information about Digital Bond's clients, which include a major water project, a power plant and a mining company.

Jaime Blasco, a security researcher at AlienVault, analyzed the computer servers used in the attack, which led him to other victims, including the Chertoff Group. That firm, headed by the former secretary of the Department of Homeland Security, Michael Chertoff, has run simulations of an extensive digital attack on the United States. Other attacks were made on a contractor for the National Geospatial-Intelligence Agency, and the National Electrical Manufacturers Association, a lobbying group that represents companies that make components for power grids. Those organizations confirmed they were attacked but have said they prevented attackers from gaining access to their network.

Mr. Blasco said that, based on the forensics, all the victims had been hit by Comment Crew. But the most troubling attack to date, security experts say, was a successful invasion of the Canadian arm of Telvent. The company, now owned by Schneider Electric, designs software that gives oil and gas pipeline companies and power grid operators remote access to valves, switches and security systems.

Telvent keeps detailed blueprints on more than half of all the oil and gas pipelines in North and South America, and has access to their systems. In September, Telvent Canada told customers that attackers had broken into its systems and taken project files. That access was immediately cut, so that the intruders could not take command of the systems.

Martin Hanna, a Schneider Electric spokesman, did not return requests for comment, but security researchers who studied the malware used in the attack, including Mr. Stewart at Dell SecureWorks and Mr. Blasco at AlienVault, confirmed that the perpetrators were the Comment Crew.

“This is terrifying because — forget about the country — if someone hired me and told me they wanted to have the offensive capability to take out as many critical systems as possible, I would be going after the vendors and do things like what happened to Telvent,“ Mr. Peterson of Digital Bond said. “It’s the holy grail.”

Mr. Obama alluded to this concern in the State of the Union speech, without mentioning China or any other nation. “We know foreign countries and companies swipe our corporate secrets,” he said. “Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air-traffic control systems. We cannot look back years from now and wonder why we did nothing.”

Mr. Obama faces a vexing choice: In a sprawling, vital relationship with China, is it worth a major confrontation between the world’s largest and second largest economy over computer hacking?

A few years ago, administration officials say, the theft of intellectual property was an annoyance, resulting in the loss of billions of dollars of revenue. But clearly something has changed. The mounting evidence of state sponsorship, the increasing boldness of Unit 61398, and the growing threat to American infrastructure are leading officials to conclude that a far stronger response is necessary.

“Right now there is no incentive for the Chinese to stop doing this,” said Mr. Rogers, the House intelligence chairman. “If we don’t create a high price, it’s only going to keep accelerating.”

A version of this article appears in print on February 19, 2013, on Page A1 of the New York edition with the headline: China’s Army Seen as Tied To Hacking Against U.S.

© 2018 The New York Times Company