US Security Group Suspects Chinese Military Is Behind Hacking Attacks

A secretive **Chinese military** unit is believed to be behind a series of **hacking attacks**, a U.S. computer security company said, prompting a strong denial by China and accusations that it was in fact the victim of U.S. hacking.

The company, **Mandiant**, identified the **People's Liberation Army**'s Shanghai-based **Unit 61398** as the most likely driving force behind the **hacking**. Mandiant said it believed the unit had carried out "sustained" attacks on a wide range of industries.

"The nature of Unit 61398's work is considered by China to be a state secret; however, we believe it engages in harmful 'Computer Network Operations'," Mandiant said in a report released in the United States on Monday.

"It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively," it said.

China's Defense Ministry issued a flat denial of the accusations and called them "unprofessional." It said hacking attacks are a global problem and that China is one of world's biggest victims of cyber assaults.

"The Chinese army has never supported any hacking activity," the Defense Ministry said in a brief, faxed statement to Reuters. "Statements about the Chinese army engaging in **cyber attacks** are unprofessional and not in line with facts."

Video: Is this China's hacking headquarters?

Exposing cyber espionage:
61398 is located in Shanghai's Pudong district, China's

financial and banking hub, and is staffed by perhaps thousands of people proficient in English as well as computer programming and network operations, Mandiant said in its report.

The unit had stolen “hundreds of terabytes of data from at least 141 organizations across a diverse set of industries beginning as early as 2006”, it said.

Most of the victims were located in the United States, with smaller numbers in Canada and Britain. The information stolen ranged from details on mergers and acquisitions to the emails of senior employees, the company said.

The 12-story building, which houses the unit, sits in an unassuming residential area and is surrounded by a wall adorned with military propaganda photos and slogans; outside the gate, a sign warns members of the public they are in a restricted military area and should not take pictures.

There were no obvious signs of extra security on Tuesday.

The Chinese Foreign Ministry said the government firmly opposed hacking, adding that it doubted the evidence provided in the U.S. security group’s report.

“Hacking attacks are transnational and anonymous. Determining their origins are extremely difficult. We don’t know how the evidence in this so-called report can be tenable,” spokesman Hong Lei told a daily news briefing.

“Arbitrary criticism based on rudimentary data is irresponsible, unprofessional and not helpful in resolving the issue.”

Hong cited a Chinese study which pointed to the United States as being behind hacking in China.

“Of the above mentioned **Internet hacking attacks**, attacks originating from the United States rank first.”

“Economic Cyber Espionage”
Some experts said they doubted Chinese government denials.

“The **PLA** plays a key role in China’s multi-faceted security strategy, so it makes sense that its resources would be used to facilitate economic cyber espionage that helps the Chinese economy,” said Dmitri Alperovitch, chief technology officer and co-founder of CrowdStrike, one of Mandiant’s competitors.

Though privately held and little known to the general public, **Mandiant** is one of a handful of U.S. **cyber-security** companies that specialize in attempting to detect, prevent and trace the most advanced hacking attacks, instead of the garden-variety viruses and criminal intrusions that befoul corporate networks on a daily basis.

But Mandiant does not promote its analysis in public and only rarely issues topical papers about changes in techniques or behaviors.

It has never before given the apparent proper names of suspected hackers or directly tied them to a military branch of the Chinese government, giving the new report special resonance.

The company published details of the attack programs and dummy websites used to infiltrate **U.S.** companies, typically via deceptive emails.

U.S. officials have complained in the past to China about sanctioned trade-secret theft, but have had a limited public record to point to.

Mandiant said it knew the PLA would shift tactics and programs in response to its report but concluded that the disclosure was worth it because of the scale of the harm and the ability of **China** to issue denials in the past and duck accountability.

The company traced Unit 61398’s presence on the Internet—including registration data for a question-and-answer session with a Chinese professor and numeric Internet

addresses within a block assigned to the PLA unit—and concluded that it was a major contributor to operations against the U.S. companies.

Members of Congress and intelligence authorities in the United States have publicized the same general conclusions: that **economic espionage** is an official mission of the PLA and other elements of the **Chinese government**, and that hacking is a primary method.

In November 2011, the U.S. National Counterintelligence Executive publicly decried China in particular as the biggest known thief of U.S. trade secrets.

The Mandiant report comes a week after President Barack Obama issued a long-awaited executive order aimed at getting the private owners of power plants and other critical infrastructure to share data on attacks with officials and to begin to follow consensus best practices on **security**.

Both Democrats and Republicans have said more powerful legislation is needed, citing Chinese penetration not just of the largest companies but of operations essential to a functioning country, including those comprising the electric grid.

Additional reporting by Michael Martina and Koh Gui Qing in Beijing, Carlos Barria in Shanghai and Jim Finkle in Boston; editing by Robert Birsel and Sanjeev Miglani.