A look at Mandiant, allegations on China hacking

February 19 2013, by Anne Flaherty

(AP)—A private technology security firm on Tuesday described in extraordinary detail efforts it blamed on a Chinese military unit to hack into 141 businesses, mostly inside the U.S., and steal commercial secrets. China denies the claim. Here's a look at the company, Mandiant, and why its report is significant.

What is Mandiant?

Headquartered in suburban Alexandria, Virginia, Mandiant was started in 2004 by Kevin Mandia, a retired Air Force officer who carved out a lucrative niche investigating computer crimes. Mandiant says it can detect and trace even quiet intrusions, such as the theft of employee passwords or trade secrets that a company otherwise might not be aware is happening.

Mandiant was most recently noted for its work in helping The New York Times trace an attack on its employees' computers to China, following a Times investigation into China's Premier Wen Jiabao. The newspaper publicly acknowledged Mandiant's role in the case.

Are there other companies like Mandiant? Why not just call the FBI?

There are other companies that specialize in cybercrime response and forensics, including CrowdStrike, Kroll Advisory Solutions, and Stroz Friedberg in New York. Others specialize in establishing and testing a company's computer defenses and monitoring traffic to detect hackers or

suspicious behavior.

Companies can be reluctant to call the FBI. Businesses don't want to hand over their most sensitive information—including computers and proprietary data—to the government and would rather maintain control of the investigation. Many companies are less concerned about tracing the origin of an attack than resuming business to make money. They also don't want their vulnerabilities discussed in a courtroom or leaked to news organizations or shareholders, which can happen if the government were involved. Companies like Mandiant have a big financial incentive—and signed confidentiality promises—to keep names of clients secret.

What did Mandiant's report say? Why is it important?

Mandiant alleges that it has traced a massive hacking campaign on U.S. businesses to a drab, white 12-story office building outside Shanghai run by "Unit 61398" of the People's Liberation Army. The report contains some of the most extensive and detailed accusations on China's cybersnooping publicly available, including a timeline and details of malware used.

The U.S. government, including its intelligence agencies, almost certainly has similar and even more detailed information but it's regarded as highly classified. Being a private company, Mandiant doesn't have to keep its information secret, although it hasn't released the names of the companies attacked.

Why did Mandiant publish its findings?

Mandiant says it was time to call out China for its systematic hacking and that releasing as many details as possible will help security professionals. It acknowledged in a statement that releasing the

information was risky because it said the Chinese will change tactics now that some of its techniques are known. Mandiant also said it expects itself to be targeted, beyond what it described as an unsophisticated effort in April to trick some employees into installing malicious software disguised as a draft press release. "We expect reprisals from China as well as an onslaught of criticism," Mandiant wrote.

Mandiant has an obvious commercial interest in releasing the information, too. The company said its existing customers were already warned about and protected against the techniques it discovered, and it offered a free software tool to companies and organizations to detect suspicious activity.

It puts Mandiant front-and-center at a critical time on a national debate about cybersecurity. Its founder testified earlier this month to the House Intelligence Committee on hacking threats. Last week, President Barack Obama signed an executive order aimed at improving government cooperation with industry, and Congress is weighing various legislative proposals on the matter.