Is Mandiant a 'Digital Blackwater'?

ANNE FLAHERTY, Associated Press

WASHINGTON (AP) — When Kevin Mandia, a retired military cybercrime investigator, decided to expose China as a primary threat to U.S. computer networks, he didn't have to consult with American diplomats in Beijing or declassify tactics to safely reveal government secrets.

He pulled together a 76-page report [1] based on seven years of his company's work and produced the most detailed public account yet of how, he says, the Chinese government has been rummaging through the networks of major U.S. companies.

It wasn't news to Mandia's commercial competitors, or the federal government, that systematic attacks could be traced back to a nondescript office building outside Shanghai that he believes was run by the Chinese army. What was remarkable was that the extraordinary details — code names of hackers, one's affection for Harry Potter and how they stole sensitive trade secrets and passwords — came from a private security company without the official backing of the U.S. military or intelligence agencies that are responsible for protecting the nation from a cyberattack.

The report, embraced by stakeholders in both government and industry, represented a notable alignment of interests in Washington: The Obama administration has pressed for new evidence of Chinese hacking that it can leverage in diplomatic talks — without revealing secrets about its own hacking investigations — and Mandiant [2] makes headlines with its sensational revelations.

The report also shows the balance of power in America's cyberwar has shifted into the hands of the $30 billion-a-year computer security industry.

"We probably kicked the hornet's nest," Mandia, 42, said in an interview at the Alexandria, Va., headquarters of Mandiant. But "tolerance is just dwindling. People are tired of the status quo of being hacked with impunity, where there's no risk or repercussion."

China has disputed Mandiant's allegations.

Mandiant, which took in some $100 million in business last year — up 60 percent from the year before — is part of a lucrative and exploding market that goes beyond antivirus software and firewalls. These "digital forensics" outfits can tell a business whether its systems have been breached and — if the company pays extra — who attacked it.

Mandiant's staff is stocked with retired intelligence and law enforcement agents who specialize in computer forensics and promise their clients confidentiality and control over the investigation. In turn, they get unfettered access to the crime scene and resources to fix the problem (Mandiant won't say exactly how much it charges, but it's estimated to average around $400 an hour).

The growing reliance on contractors like Mandiant has been compared to that enjoyed by the military and State Department contractor formerly known as Blackwater, which provided physical security to diplomats and other VIPs during the Iraq war. Officials inside and outside government say that's not a bad thing; contractors can often act more quickly than the government and without as much red tape. There are also serious privacy concerns: Most U.S. citizens don't want the government to access their bank accounts, for example, even if China is attacking their bank.

"The government doesn't have the capacity," said Shawn Henry, a former FBI executive assistant director who works for a Mandiant competitor, CrowdStrike. "There are a lot of people working hard. But the structures aren't there."

Michael DuBose, another former senior Justice Department official who works at a different Mandiant competitor, Kroll Advisory Solutions, added: "I think there's a recognition that the government can't stand at the entry point of the Internet to the United States and shield it from all bad things coming in."

Since Mandiant released its report this week, government officials and lawmakers have publicly embraced its findings. Sen. Dianne Feinstein, the Democratic chairwoman of the Senate Intelligence Committee, hailed Mandiant for exposing China as a problem. She called its report "sobering" and said she hoped it would spur an international agreement to protect companies from cyber-espionage.

"It's a forcing function in the private sector, and frankly ... it's a forcing function with the government," said retired Air Force Gen. Michael Hayden, the former director of the CIA and the National Security Agency who now works for the Chertoff Group, a security consulting firm.

Mandiant's report raises questions, too, about the extent to which private companies are in control of defending the nation's most crucial networks, like power companies and water treatment plants. Another question is what rules of engagement private companies might rely on. When does a company strike back?

Mandia and his competitors said they are beholden to U.S. and international laws, which prohibit the type of intrusive acts they accuse China of taking. Mandia also says his clients aren't interested in starting a cyberwar with foreign hackers, in part because they are so vulnerable.

"The only time (hacking back) would really work is if we got all the bad guys out of our networks in the first place," he said. "Then you can start playing that game." Still, publishing the hacking report was itself an offensive shot across China's bow.

Mandia said he started his company in 2004 after years in the private sector because there was no company focused on investigating intrusions. With a master's degree in forensic science from George Washington University, he became Mandiant's sole employee and, two years later, got a cash infusion from a college friend. Now, he oversees some 330 employees and the field is growing rapidly. He says he used to see maybe three major incidents a month when he started his business; now he estimates there can be anywhere from 30 to 100 incidents a month.

Mandia is hardly alone. A former co-worker, Stuart McClure, recently started his own company, called Cylance. He received $15 billion in venture capital funds for his business, which he says is distinctive because of its focus on prevention. McClure said in general he sees the future of cyberdefense residing in the private sector, with its deeper pockets and less red tape.

"With a commercial entity, you can get more creative," McClure said.

As for any problems they might cause in diplomatic or security circles for the federal government, Mandia and his competitors say that's not really on their radar, although he's hiring attorneys to help him monitor changing U.S. policies and regulations. But as a tech guy, he says he's focused on stopping intrusions.

"We're security guys," Mandia said. "We're not diplomats."

—

Online:

Mandiant: http://www.mandiant.com [2]

The report: http://intelreport.mandiant.com/ [1]

Source URL (retrieved on *10/20/2014 - 1:22am*):
http://www.wirelessdesignmag.com/news/2013/02/mandiant-digital-blackwater?qt-blogs=0

Links:
[1] http://intelreport.mandiant.com/
[2] http://www.mandiant.com