A new brand of cybersecurity: hacking the hackers

December 6 2012, by Ken Dilanian

As head of the FBI's cyber crimes division, Shawn Henry often had to deal with exasperated company executives after his agents informed them that their networks had been hacked and their secrets pilfered.

"By whom?" the company officials would ask. "What have they taken? Where did it go?"

"Sorry," Henry's agents had to reply, "that's classified."

Even though the FBI in many cases had evidence the attacker had been backed by a foreign intelligence agency, agents couldn't disclose it because the U.S. government believed doing so could compromise top-secret sources and methods.

Henry, 50, decided this year that such a dichotomy shouldn't put companies at such a disadvantage. So after 24 years of service, he left the FBI to become president of CrowdStrike, an Internet security startup in Irvine, Calif.

His new mission: to make life difficult for hackers trying to attack American institutions.

CrowdStrike is at the forefront of a new business model for cyber security, one that identifies sophisticated foreign attackers trying to steal U.S. intellectual property and uses the attackers' own techniques and vulnerabilities to thwart them.

The firm is marketing itself as a private cyber intelligence agency, staking out networks to catch infiltrators, assembling dossiers on hackers and fooling intruders into stealing bogus data.

In the process, the firm has waded into a debate about how far companies should go in defending themselves from cyber attack.

"The traditional way of trying to defend your network is just not going to cut it. You have to do something different," said Irving Lachow, who directs the Program on Technology and National Security at the Center for a New American Security.

"One way is to engage the adversary. CrowdStrike represents a new breed of company that is focused on doing exactly that," he said.

When somebody is shooting at you, "you don't ask, 'Is that a 9-millimeter or a .45?' " said CrowdStrike Chief Executive George Kurtz. "You ask: 'Who is shooting at me, and why are they shooting at me?' "

The attackers often breach company networks using a tactic known as spear phishing, a practice that gets an employee to download a malware file by disguising it, for example, in an email purporting to be from someone the worker knows. Firewalls and anti-virus software are almost useless against such techniques.

So CrowdStrike uses decoys to lure hackers into a controlled environment so investigators can watch and trace the attack. Sometimes the company feeds hackers false information, as in a case recently when a client was entering negotiations in China and expected to be hacked.

CrowdStrike, which employs Chinese linguists and former U.S. government cyber warriors, also has identified Chinese hackers using clues in their malware. It then profiles them - complete with real names and photos - using information gathered from a variety of sources.

That has helped the company, for example, identify a Chinese hacker who targets financial institutions and tends to seek merger and acquisition information. The company assigned the hacker a code name, Capital Panda, in the profile.

Profiles enable a more targeted defense by helping CrowdStrike know when an attacker is likely to strike, how he communicates, what malware he uses and how he tries to take the stolen data.

Kurtz, a former chief technology officer at security firm McAfee Inc., started CrowdStrike in February with fellow McAfee alumnus Dmitri Alperovitch and $26 million in financing from private equity firm Warburg Pincus.

Alperovitch rose to prominence last year when he wrote a white paper on what he called Operation Shady Rat, a series of state-sponsored cyber penetrations of more than 70 government agencies, companies and institutions. He didn't say publicly the intrusions came from China, but that was obvious to other experts.

China denies engaging in cyber espionage. U.S. intelligence officials said hackers sponsored by China and, to a lesser extent, Russia, are responsible for what Gen. Keith B. Alexander, director of the National Security Agency, has called "the greatest transfer of wealth in history" by siphoning bid documents, formulas, business plans and other intellectual property from Western companies.

The U.S. government's response has been confined to raising the issue politely in diplomatic discussions. CrowdStrike's confrontational approach is more satisfying to those damaged by cyber economic espionage.

The company is not without critics, who worry how far companies might go down the road of cyber vigilantism.

This year, Michael Hayden, former director of both the CIA and the NSA, raised the specter of a "digital Blackwater," a paid mercenary battling cyber attackers on behalf of corporations. CrowdStrike rejects any comparison to the notorious private security company that got into trouble when its employees killed 17 civilians in Iraq in 2007.

But some find the comparison apt - and troubling.

"You don't want the Internet to resemble Somalia," said one cyber expert who did not want to be identified because it could jeopardize his friendships with CrowdStrike's founders.

Some experts believe CrowdStrike and other companies should be able to "hack back" by, for example, disabling servers that host cyber attacks, whether they are in the U.S. or abroad.

The Justice Department said hacking back may be illegal under the Computer Fraud and Abuse Act, a 1996 law that prohibits accessing a computer without authorization. Many lawyers liken it to the principle that a person can't legally break into his neighbor's house, even if he sees his stolen television in the neighbor's living room.

"We will not break the law, but there's a lot organizations can do behind their own firewall on their own networks to make life difficult for the adversary," Henry said.

Others, including Stewart Baker, former NSA general counsel, said the law does allow hacking back in self-defense. A company that saw its stolen data on a foreign server was allowed to retrieve it, Baker argued.

In the post 9/11 world, airline passengers would almost certainly tackle and restrain an unruly passenger who rushed the cockpit, and they wouldn't be charged with assault and kidnapping even though they technically had committed those offenses, said Steven Chabinsky, who retired this year as the FBI's top cyber lawyer and became CrowdStrike's chief risk officer.

But it's different when you are breaking into someone else's property, said Daimon Geopfert, a former Air Force cybercrimes investigator who now heads cybersecurity services for consulting firm McGladrey in Chicago.

Often, he said, servers that host cyber attacks belong to innocent third parties that have themselves been hacked. "It's not only legally wrong, it's morally wrong," he said.

Critics also worry that to the extent CrowdStrike runs offensive operations against hackers controlled by the Russian or the Chinese governments, it risks creating an international incident.

"Why isn't it an international incident when China steals our intellectual property?" Alperovitch said. "If the government would say, 'We're actually going to stand up to China,' that would be great; we'd go back to doing defense only. But they are not saying that."

(c)2012 Tribune Co.
Distributed by MCT Information Services

Citation: A new brand of cybersecurity: hacking the hackers (2012, December 6) retrieved 23 May 2024 from https://phys.org/news/2012-12-brand-cybersecurity-hacking-hackers.html