CrowdStrike Falcon Traces Attacks Back To Hackers

darkreading.com/attacks-and-breaches/crowdstrike-falcon-traces-attacks-back-to-hackers/d/d-id/1110402

Mathew J. Schwartz June 17, 2013

(click image for larger view)
The Syrian Electronic Army: 9 Things We Know

Who's launching online attacks against your network? How can you better detect those attacks and -- if an attack turns out to be successful -- identify what was stolen? Enabling businesses to answer those questions is the premise of a cloud-based service announced Tuesday by security startup CrowdStrike. Dubbed Falcon, the big-data "active defense platform" is designed to identify intrusions in real time, attribute attacks – correlate with a known group of attackers – and help businesses block attacks or even engage in counterintelligence or deception by feeding attackers fake information.

"This is the real-time damage assessment that no one is doing today," said Dmitri Alperovitch, the co-founder and CTO of CrowdStrike, speaking by phone. "It shows you who the adversary is, what did they do [on your network], what did they take, which commands did they execute?" The service works in part by running a small (400 KB) "sensor" on

Windows 7 and Mac OS X systems, bolstered by DNS, email and API sensors on servers, to track the types of attacks that are being launched. CrowdStrike then correlates attack information with intelligence that the company gathers on attack groups.

[NSA whistleblower's accusations deepen. Read Snowden Says U.S. Hacking Chinese Civilians Since 2009.]

As highlighted by successful spear-phishing attacks against everyone from security giant RSA to the White House, stopping every last information security attack might be impossible. So-called advanced persistent threat (APT) groups often use fake emails and attachments to infect targeted PCs and steal data, oftentimes without end users or security teams being aware. Once attackers infect a single PC, unless they're detected, they can lurk in corporate networks indefinitely: telecommunications giant Nortel was compromised for 10 years, defense contractor QinetiQ for three years.

Such attacks are cheap to build and inexpensive to launch. Even if only one attack out of every 100 or 1,000 attempts succeeds, that might equal success for attackers. Given that reality, CrowdStrike's play is to help businesses identify not just when they've been attacked, but also who stole the information, what they stole and why they targeted the business in the first place -- what's their bigger goal?

"The problem you've had for the past six to seven years is the emergence of targeted attackers, and for them, it doesn't mater how many layers of defense you put in place; what they want is you," said Alperovitch. "They want money, national secrets, intellectual property, and they're going to worm their way in, because the return on that investment is gigantic."

Could defenders gain an edge by better understanding their attackers? "From an adversary perspective, we really focus on the targeted attackers," said Alperovitch. "We're tracking lots of nation-state-sponsored groups that are working to penetrate companies," he said, and "understanding their campaigns, and tradecraft, as well as who they're targeting."

CrowdStrike has grouped attackers into "adversary groups" -- to date, about 48 in total -- named for country characteristics: "pandas" for groups operating from China; "cats" as in Persian cats for Iran; "bears" for Russia; "saints" for Georgia; and "tigers" for India. "Some in the community refer to the adversary by the malware detection name from a specific antivirus vendor, e.g. Hydraq," said Adam Meyers, director of intelligence at CrowdStrike, in a blog post, referring to the name of the malware used in the so-called Aurora attacks against Google. "This is sometimes useful, but when the adversary is using a malware that is detected as Generic.Downloader.234, you have a much harder time communicating," Meyers said.

CrowdStrike recommends that businesses use its intelligence on online adversaries to identify and focus on the attackers they're most likely to face. "For example, if you're in the financial service industry, you'll care about Big Panda, which is going after financial services

firms, but not Karma Panda that's going after dissident groups," said Alperovitch. "If you're trying to go after everyone and defend against everything, you're really defending against nothing."

For instance, one group that CrowdStrike has been tracking -- dubbed Anchor Panda -- has launched 124 attacks over the past six months, many of which appear to be aimed in part at building out deep-sea capabilities. Adam Meyers, head of intelligence for Crowdstrike, recently told *The New Yorker* that the information being targeted by the group bears more than a passing resemblance to China's five-year plan for modernizing its infrastructure.

Once businesses have identified the group behind an attack, or used new intelligence to identify previously unidentified attacks that were successful as well as what was stolen, what happens next? According to Alperovitch, "if you want to work with the government, we can help with that as well, on our services side," which is headed by Shawn Henry, whose prior job was serving as the executive assistant director of the FBI's criminal, cyber, response and services branch. "Or you take the attribution and take legal action against that individual or the company," he said. "A lot of companies are multinationals, so you can actually sue them in the United States -- or in a jurisdiction of your choosing overseas, and get criminal damages or injunctive relief for stolen information."

Alperovitch said that when it comes to responding to hack attacks, there can be strength in numbers: "If you're one company going up against China, you're going to be afraid of retaliation, of your business being shut out of China. But if you're in a band of 20 or 30 Fortune 100 companies, China can't really retaliate; it needs them all."

"Ultimately we'll only solve this problem together, not individually trying to build castles to protect ourselves," said Alperovitch. "That model hasn't worked in the physical world in over 400 years, and certainly not in cyber space."