Published on *InfoWorld* (http://www.infoworld.com)

The new cyber defense: Hack the attackers

By InfoWorld Tech Watch
Created *2012-04-24 03:00AM*

As the ecology of online attacks has evolved, so have defenders' methods. In 2009, the then-classified Comprehensive National Cyber Initiative -- the U.S. government's cybersecurity strategy -- espoused the concept of offense informing defense [1]. The maxim suggested that defenders needed to use data from actual attacks to help them create specific defenses to protect critical infrastructure and corporate networks. In the past two years, security professionals have increasingly embraced the concept but have generally not ventured outside their own firewalls.

Now, some security experts are recommending that companies take it farther and that defenders should go on the attack. At the SOURCE Boston security conference last week, for example, Iftach Ian Amit, an independent security consultant who claims to have conducted several offensive operations, told attendees that companies need to consider counterintelligence operations.

"We can be much more active" in defending our network, he said. "Counter intel is fair game.... Everything around is yours; you better know everything that goes on out there."

While attackers do reconnaissance and information gathering on their corporate targets, most companies are taking a passive stance and waiting for an attack, he said. Like medieval defenders of a castle, today's companies are sitting behind their digital walls with only a narrow view of what's happening outside their network. Instead, companies must collect intelligence and act to blunt attacks before they happen, Amit said. They should do their own research on attackers, figure out which ones are behind any probes targeted their networks and conduct limited attacks in return.

"You want to find out who's leaking data? Put data that looks interesting inside an organization, and see where it ends up," he said. "It works. Trust me, we've done this numerous times. It's fun."

The concept is not necessarily new. In 2009, two researchers argued that some groups be allowed to act on behalf of victims to shut down botnets [2]. Microsoft has, to some extent, done just that with its MARS (Microsoft Active Response for Security) program, which has taken legal measures against four botnets in the past two years [3]. At the RSA Security Conference in February, Greg Hoglund, the founder of HBGary, recommended that companies develop the capability to gather intelligence on threats and to take a more active approach to detecting attackers in their network.

Amit stressed that companies should consult with their lawyers to make sure that they are abiding by all laws. However, companies need lawyers who will seek creative legal solutions to the problems, Amit said. "Get a real lawyer, not one who will tell you, 'No, you can't do that,'" he said. "Get a lawyer who will tell you, 'You can't do it like this, but if we put a server over there, then, yeah, you can do that.'"

Amit, who operates out of Israel, has infiltrated communities of adversaries targeting his clients to gather intelligence. In one case, he replaced their remote access trojan with another one that would allow him to remotely access any computer with the software on it. In another case, his client replaced a program that creates fully undetectable malware with a version that would send defenders the signature of any code created with the program.

In the end, defenders have to be careful not to cause collateral damage, but they should not shy away from an offensive approach, he said.

"It is attack and defense; it is conflict," Amit said. "You can't be too naive."

This story, "The new cyber defense: Hack the attackers [4]," was originally published at InfoWorld.com [5]. Get the first word on what the important tech news really means with the InfoWorld Tech Watch blog [6]. For the latest developments in business technology news, follow InfoWorld.com on Twitter [7].

Correction: *In this article as originally posted, Greg Hoglund's statements at the RSA Security Conference could be misconstrued. He only recommended that companies develop more active intelligence and monitoring operations. The story has been amended.*

Cyber Crime Intrusion Detection Malware Security Management

Source URL (retrieved on *2012-04-25 07:03AM*): http://www.infoworld.com/t/security-management/the-new-cyber-defense-hack-the-attackers-191553

Links:
[1] http://csis.org/publication/twenty-important-controls-effective-cyber-defense-and-fisma-compliance
[2] http://www.csoonline.com/article/495520/cyberwar-is-offense-the-new-defense-
[3] http://www.infoworld.com/t/cyber-crime/botnet-whack-mole-just-might-work-189741
[4] https://www.infoworld.com/t/security-management/the-new-cyber-defense-hack-the-attackers-191553?source=footer
[5] http://www.infoworld.com/?source=footer
[6] http://www.infoworld.com/blogs/infoworld-tech-watch?source=footer
[7] http://twitter.com/infoworld