SECURITY darkREADING
Protect The Business Enable Access

# Security Teams Need Better Intel, More Offense

**Adversaries go through five steps to prepare and execute an attack, but defenders only react to the last two steps. It's time for defenders to add intelligence gathering, counter intel, and even offense to the game, security experts say**

By Robert Lemos, Contributing Writer
Dark Reading, Darkreading

Apr 24, 2012 | 08:37 PM
URL - http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/232900905/security-teams-need-better-intel-more-offense.html

The recipe for a cyberattack is straightforward: Attackers gather intelligence on the target's systems, research vulnerabilities, exploit those weaknesses, gain control of the systems, and conduct post-exploitation operations.

Yet for the first three parts of attackers' operations, most defenders do nothing. Only after attackers act on a corporate network -- the fourth step -- does a victim's security team becomes aware of the attack. In a presentation at the SOURCE Boston security conference last week, independent security consultant Iftach Ian Amit told attendees that defenders need to do better.

"We are basically just waiting to be attacked," he said.

Increasingly, security experts are recommending that companies become more aggressive in gathering information on their attackers. Companies need to gather or buy intelligence on adversaries and should consider more active counter intelligence operations, Amit said. Rather than hunker down behind the firewall, like defenders of a medieval castle, security analysts should explore the landscape. To match attackers' first steps, defenders should model their organization's threats, gather intelligence, and correlate the data to pinpoint possible threats, he said.

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

The case for more active defense has gained adherents over the past few years. In 2009, the then-classified Comprehensive National Cyber Initiative -- the U.S. government's cybersecurity strategy -- reportedly relied heavily on the concept of a defense that adapts to the offense. Rather than focusing on all vulnerabilities equally, for example, defenders can use data from actual attacks to help them create specific defenses to protect critical infrastructure and corporate networks.

Support for more active responses to attacks has grown as well. In 2009, two researchers presenting at the Conference on Cyber Warfare in Tallin, Estonia, argued that some groups be allowed to shutter botnets on behalf of the victims. With the Microsoft Active Response for Security (MARS) program, Microsoft has essentially done just that -- shutting down four botnets in the past two years and showing that offensive actions can help protect defenders.

***[Microsoft's Zeus botnet case demonstrates the risks and challenges associated with takedowns when multiple groups are tracking the same botnet. See Botnet Takedowns Can Incur Collateral Damage.]***

While many companies are satisfied with keeping a passive defense, others chafe at the constant stream of attacks and their inability to attack back, said Ken Silva, senior vice president for cyber strategy at information technology contractor ManTech International.

"I will tell you that companies today are getting very frustrated with the continuous landscape of compromise," Silva said. "They feel incredibly helpless, so they are looking for the next thing they can do ... The measures that companies will take to defend themselves is going to escalate."

Silva does not condone attacking the attacker, however. Active intelligence-gathering, yes. But targeting attackers can easily backfire, he warned. If attackers are staging attacks from another company's servers, for example, defenders who attack back can damage an innocent party's server and are putting themselves in legal jeopardy.

"There are a lot of risks on a number of levels," Silva said.

The legal pitfalls can be serious, acknowledged consultant Amit. He stressed that companies should consult with their lawyers to make sure that they are abiding by all laws. However, companies need lawyers that 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.'"

Operating out of Israel, Amit has infiltrated communities of adversaries targeting his clients to gather intelligence, he told attendees at SOURCE Boston. In one case, he replaced a remote access Trojan with a compromised version that could allow defenders to track they users of the software. 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.

The need for such tactics are relatively rare, says Phil Lin, director of product marketing for FireEye, a maker of products to detect advanced threats. Counter intelligence does not mean that defenders need to attack back. Instead, they can employ other tactics, such as honeypots and threat intelligence to better understand attackers.

Yet even Lin can understand the frustration of defenders unable to permanently stop attackers' activities.

"It is definitely fair to say that customers and enterprises are very frustrated with the current state of cybersecurity," he said. "But what people choose to do about that frustration is the point in question."

*Have a comment on this story? Please click "Add Your Comment" below. If you'd like to contact* Dark Reading's *editors directly, send us a message.*

Print