

Top FBI cyber-cop joins spy thwarting startup

April 19 2012



Veteran FBI cyber security expert Shawn Henry, pictured here in December 2010, said he is fighting the enemy on a new front by joining a startup out to protect firms from online spies.

Veteran FBI cyber security expert Shawn Henry said he is fighting the enemy on a new front by joining a startup out to protect firms from online spies.

After 24 years of working for the FBI, Henry has switched to the private sector as the head of a CrowdStrike division specializing in [cyber attack](#) incident responses and identifying adversaries.

"I've been saying that the private sector could be filling the Internet security void that the government hasn't been filling," Henry told AFP on Wednesday.

"Now I can do something," he continued. "CrowdStrike was going to do everything I said we should be doing."

Former McAfee [chief technical officer](#) George Kurtz and Dmitri Alperovitch, who has researched major cyber [espionage](#) operations, had operated CrowdStrike in "stealth mode" until early this year.

The startup got \$26 million in backing from global [private equity firm](#) Warburg Pincus.

Relentless waves of cyber attacks that appeared to be the work of states inspired the researchers come up with a different way of taking on the threat.

"Most companies are focused on detecting [malware](#), and there are millions of pieces of that, with new ones coming all the time," Kurtz told AFP in a recent interview.

"It really is akin to focusing on the bullets in the gun as opposed to the shooter... We think most companies have an adversary problem, not a malware problem."

CrowdStrike is building tools to figure out who is behind attacks, how they move after invading systems and what they are out to steal or accomplish, according to the researchers.

"You can't know how best to fight a war without knowing who the enemy is, and it is the same thing in [cyber space](#)," Alperovitch said, describing China and Russia as the most prominent threats.

CrowdStrike plans to have a security product to market in the second half of this year.

"At the end of the day it is another guy sitting at a keyboard somewhere going after your data," Alperovitch said. "You don't have a malware problem, you have a people problem."

The idea of using intelligence to understand and "mitigate adversaries" resonated with Henry.

"You can't just build a wall higher and higher," he said, referring to computer security that relies on software barriers to stop viruses or intruders.

"We are focusing on identifying them inside the network and making the cost of intrusion much higher."

Former FBI executive director Henry coordinated responses by federal and local police to cyber threats.

(c) 2012 AFP

Citation: Top FBI cyber-cop joins spy thwarting startup (2012, April 19) retrieved 20 April 2024 from <https://phys.org/news/2012-04-fbi-cyber-cop-spy-thwarting-startup.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--