

## Cyber spies try probing U.S. drone plans

China-based hackers for months have been targeting federal agencies and contractors through infected emails apparently to spy on the Pentagon's drone strategy and other intelligence matters, according to Internet security researchers.

The reported espionage employed a tactic known as spear-phishing where infiltrators, operating under the guise of a legitimate sender, email specific victims a virus-laden file or link. In this case, the hackers used email addresses from military and other government organizations, Jaime Blasco, manager of AlienVault Labs, said Tuesday.

Some emails went to employees at U.S. military contractors, he said, but declined to discuss any information related to specific victims.

The lab traced samples of the malicious software to network addresses in China, AlienVault disclosed last month.

Blasco has since discovered from the same spies separate malware that is capable of overriding Pentagon smart card credentials, known as the Common Access Card, to get into protected resources, he said Tuesday. In addition, the intruders have been pursuing other government organizations with information of interest to Chinese intelligence operations -- including the General Services Administration, the U.S. government's buying arm, and the Central Tibetan Administration.

"After studying all these attacks and all the methods used, we can conclude that they are likely the same group behind all these attacks," Blasco said.

The Chinese government is believed to sponsor cyber strikes on U.S. assets regularly, with the Office of the Director of National Intelligence reporting in November 2011 that "Chinese actors are the world's most active and persistent perpetrators of economic espionage."

The thinking is that the authors of the virus are snooping on the U.S. government's plans for remotely piloted aircraft by infiltrating the computers of the aircrafts' designers. "In most of the campaigns the malware dropped displays some document or media attractive to the victim," Blasco reported last month. One server consistently sent viruses showing drone images labeled as Defense Department media; computer-generated drone renderings; and Boeing Co. drone prototypes. The campaign appears to have been running since at least September.

This particular malware, called Sykipot, works by injecting itself into a victim's browser or email account and then following orders from the hacker's command-and-control server, Blasco said. The intruder is capable of ordering the virus to extract documents or insert phony materials, for example. As of December 2011, only a couple of thousand server programs were running these files online and nearly 80 percent of them were located in China, he said.

The outsiders apparently tried to hide their footsteps by redirecting commands through hacked U.S. servers. "If someone is seeing that traffic, for instance the security team of the victim organization, it will look less suspicious," he said.

"We shouldn't jump to assumptions but whoever is behind Sykipot is massively collecting information from targeted victims that covers dozens of industries," Blasco wrote in December. There are several clues pointing to China. At least six Chinese network locations, or IP addresses, were hosting the command-and-control servers, he found. In addition, one of the tools the authors used to package the email campaigns contained message errors in Chinese. Also, all the documentation to set up the framework for running the server software is written in Mandarin. And most of the Web addresses displaying the images were registered on Xinnet, a Chinese domain name seller.

This is not the first time cybersecurity researchers have uncovered evidence of a single operative undertaking aggressive surveillance of military contractors. In 2011, McAfee investigators **reported** that during a targeted five-year operation, one specific entity penetrated the computers of 72 global organizations, including six federal agencies, 13 defense contractors and two computer security companies.

Pentagon officials were not immediately able to comment.

A GSA spokesman said in a statement, "like every federal agency, we're constantly on the lookout for new attacks against our systems. We've successfully used best-in-class techniques and safeguards to prevent inappropriate access to our systems and continually educate our employees to be on the watch for phishing scams."

---