Hackers booby-trap foreign policy group websites

May 16 2012

Photo illustration. Internet security researchers warned that foreign policy and human rights websites are being booby-trapped by hackers in what appears to be cyber espionage.

Internet security researchers warned that foreign policy and human rights websites are being booby-trapped by hackers in what appears to be cyber espionage.

As of Monday websites for Amnesty International Hong Kong, the Cambodian Ministry of Foreign Affairs and the US Center for Defense Information (CDI) remained rigged to slip "hostile" code onto visitors' computers, according to Shadowserver Foundation devoted to tracking and reporting Internet threats.

"These attackers are not spreading malware through strategically

compromised websites to make friends," Shadowserver researchers Steven Adair and Ned Moran warned in a blog post.

"They are aiming to expand their access and steal data."

Data typically sought included messages, intellectual property, research, and business intelligence such as contracts and negotiations, according to security specialists.

"The CDI website is currently serving up a malicious Flash exploit that ties back to attackers known to engage in cyber espionage," the researchers said.

"This threat group appears to be interested in targets with a tie to foreign policy and defense activities."

In recent weeks, Shadowserver has seen an array of "strategic Web compromises" taking advantage of flaws in Oracle Java and Adobe Flash programs.

The tactic is referred to as a "drive-by" attack by computer security specialists because people's computers are secretly infected simply by visiting a reputable website unaware that it has been booby-trapped by hackers.

A website for the International Institute of Counter-Terrorism at the Interdisciplinary Center in Herzliya, Israel, was listed among those compromised by hackers.

Shadowserver said that it began looking into the hacks after researchers at Websense reported last week that the main page of Amnesty International United Kingdom had been rigged with drive-by malware.

There are indications that a website for the American Research Center in Egypt was briefly compromised last week in a manner similar to the CDI page hack, according to Shadowserver.

Earlier this month the Centre for European Policy Studies website at ceps.eu was similarly compromised, according to the volunteer-based Internet security group.

Shadowserver referred to the hacks as "advance persistent threats," a term used in the industry to refer to cyber espionage by groups such as governments.

"Many of these attackers are quite skilled at moving laterally within an organization and will take advantage of any entry point they have into a network," the researchers said.

"Cyber espionage attacks are not a fabricated issue and are not going away any time soon."