

Chinese spy team hacks Forbes.com: security firms

February 10 2015



US cyber security firms say that a Chinese espionage team hacked Forbes magazine to hunt defense contractors, financial firms, and other unsuspecting prey visiting the popular news website

US cyber security firms on Tuesday said that a Chinese espionage team hacked Forbes magazine to hunt defense contractors, financial firms, and other unsuspecting prey visiting the popular news website.

Invincea and iSight Partners detailed what they described as a "watering hole" campaign late last year that took advantage of Forbes.com and other legitimate websites.

"A Chinese advanced persistent threat compromised Forbes.com to set up a watering hole style web-based drive-by attack against US defense and financial services [firms](#) in late November 2014," Invincea said in a report posted at its website.

The "brazen attack" took advantage of Adobe Flash and Internet Explorer vulnerabilities which have since been patched, according to Invincea.

Watering hole attacks typically involve hackers breaking into websites popular with their desired targets and then booby-trapping venues with viruses to infect visitors.

The cyber espionage campaign focused on Forbes.com appeared to last only a few days, but the security firms said deeper investigation could determine it went on for a longer period of time.

iSight believed that the culprits behind the attack were Chinese cyber espionage agents it called Codoso Team but also referred to as Sunshop Group.

The group has been linked to previous cyber spying campaigns against US government; military; defense industrial; think tanks covering foreign affairs; financial services; energy firms, and political dissidents, according to security researchers.

Rather than spreading malicious code to the machines of the millions of people who visited Forbes.com, the hackers appeared to be after select targets such as defense and [financial services](#) firms, according to iSight.

Further investigation reportedly revealed a set of websites being used by Codoso to target dissident groups.

Given that Forbes.com is ranked the 61st most popular website in the United States and the 168th most popular in the world, the reach of the espionage campaign could be vast, [security researchers](#) said.

© 2015 AFP

Citation: Chinese spy team hacks Forbes.com: security firms (2015, February 10) retrieved 10 April 2024 from <https://phys.org/news/2015-02-chinese-spy-team-hacks-forbescom.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>
--