Chinese Hacking Group Codoso Team Uses Forbes.com As Watering Hole

By Ericka Chickowski, Contributing Writer

Published: 2015-02-10 · Archived: 2026-04-06 00:39:33 UTC

Another day, another cyberespionage campaign attributed to a Chinese hacking group. Today's newly identified hacking push is a watering hole attack against Forbes and other targets last November that's been attributed by iSIGHT Partners and Invincea to likely be the handiwork of a long-running group they call Codoso Team, but which has also been named as Sunshop Group. The campaign was made possible by a zero-day attack that strung together a now-patched Adobe vulnerability with a bypass vulnerability in Microsoft's ASLR technology for Internet Explorer that the company patched today.

Research evidence only showed the attack to occur over a couple of days, but in addition to some highly targeted web properties it infected the Thought of the Day widget on Forbes.com with the intent to perform drive-by-download attacks via the Flash vulnerability. In spite of the mainstream appeal via Forbes, which is ranked by Alexa as the 61st most popular website on the Internet, the targets of this attack were fairly narrow. Attackers seemed to be going after defense sector firms, Chinese dissident groups and other political target, as well as certain financial targets and other commercial targets in pharmaceutical and energy sectors that could benefit the Chinese economy.

"So what's really interesting about this is it separates a lot of cyber espionage activity from say criminal activity. These guys don't typically just put drive-bys anywhere," says John Hultquist, senior manager of cyber espionage threat intelligence for iSIGHT. "They don't want anybody's information. What they want is information associated with the requirements that they have. Usually those requirements are gathering intelligence on intellectual property, gathering strategic intelligence, gathering information on say dissidents or security issues that they're working."

First publicly identified as the Sunshop Group by FireEye in 2013, Codoso Team has been on security research radars since 2010 as it perpetrated numerous targeted attacks using zero-day vulnerabilities.

"You may remember in 2010 the prize was actually awarded to a noted Chinese dissident," says Hultquist. "Shortly after that these operators went in, popped the website, and used that website to serve up exploits to visitors, again a very targeted concept. Since then they don't only operate this way or through this manner, they're also carrying out targeted spearphishing attacks."

It also shares attack techniques with Deep Panda, which like Codoso, leans heavily on the use of the Derusbi malware to carry out attacks. While they may be sharing resources, iSIGHT believes them to be two distinct gangs.

According to Anup Ghosh, CEO at Invincea, his team first noticed activity around the Forbes.com site through a defense firm customer. Typically used to tracking broad malvertising campaigns using similar media sites, his

team was surprised to see the attack only going after specific customer types, primarily in the defense sector. He also says the attack was unique through the use of chained zero-day exploits. Not only was it attacking a Flash zero-day, but it was also leveraging a zero-day in ASLR to bypass that mitigation technique.

"Effectively in modern operating systems and browsers there is a layer of technology that Microsoft has added to the mix that really makes it much more difficult for a particular exploit to figure out what address base it's operating in. So it makes it more difficult or nearly impossible to execute a buffer overflow," explains Patrick McBride, vice president at iSIGHT. "In this case the team was able to exploit that ASLR, get outside of that box, if you will, and then directly exploit the flash vulnerability. "

About the Author

Ericka Chickowski specializes in coverage of information technology and business innovation. She has focused on information security for the better part of a decade and regularly writes about the security industry as a contributor to Dark Reading.
