The Red Hen restaurant that refused to serve Sarah Sanders was hit by a cyberattack

29/06/2018

Having your business suddenly in the political spotlight can have several adverse consequences, including gaining the attention of online fraudsters.

The Red Hen Restaurant in Lexington, Virgina, which recently made news refusing to serve White House Press Secretary Sarah Huckabee Sanders, is being targeted in a cyberattack according to a researcher. The scammers have apparently taken over parts of the Red Hen's website in order to use its sudden popularity to drive traffic to their own web sites, which sell things like discount Viagra.

The scammers likely weren’t trying to take a political stand, and instead hoped to capitalize on heightened internet traffic to the website because of the headlines, said Chris Boyd, lead

malware intelligence analyst at security software company Malwarebytes, who wrote a blog post about what he found on the site. Even so, Boyd suggested that users might want to stay away from the site, as the compromise could mean the site is open to other kinds of attacks that could harm end-users.

An ancient tactic

Malicious advertisers often take advantage of small-business websites inundated with a sudden spike of traffic, using a specific type of search engine optimization known as “spamdexing.”

“If someone was going to do this for a political reason, there would have been something more splashy, like a website defacement, and they wouldn’t have gone down this road of a more malicious, hidden SEO spam tactic,” Boyd said. This type of attack isn’t used often anymore because modern search engine security protects most websites against it, he explained.

The attack includes injecting spam into search engine results, which in the Red Hen’s case are directing readers back to online sales sites for erectile dysfunction drugs like Viagra or for Japanese sports car fans, depending on the region people are visiting from, said Boyd. He said spamdexing is an “absolutely ancient” hacking tactic, and for the restaurant’s site included several compromises, starting with “keyword stuffing,” which involves putting words related to specific content — like Viagra — into the text of articles on the website, even if they make little sense.

The attack on the website also included “scraper sites,” which made small changes to the website to get ad-based revenue driven back to a malicious site, and “hidden text,” a technique where malicious advertisers fill the background of a website

with text that is the same color as the page's background, in an effort to boost online links and ranking to their own sites.

A call to the Red Hen was not immediately returned. Boyd recommended avoiding a visit to the website until it's fixed. "Generally speaking, any website that has been compromised runs the risk of getting turned into an infection portal," he said.