SALTED HASH- TOP SECURITY NEWS
By Steve Ragan

NEWS

FireEye: Forbes.com served malicious ads to visitors

Researchers say ads were pushing visitors to Neutrino and Angler exploits

CSO | Sep 22, 2015 5:00 AM PT

In a blog post, researchers from FireEye have outlined a malvertising campaign that was running on Forbes.com earlier this month, which led visitors to landing pages ran by the Neutrino and Angler exploit kits.

The attacks were triggered on a handful of articles, but the logs released by FireEye show that none of them were current.

Once the article was loaded, calls to the ad itself would load a JS file, which contained an iframe that redirected the user to the selected exploit kit.

MORE ON CSO: What is wrong with this picture? The NEW clean desk test

At first, the Neutrino kit was the primary source of delivered malware (after exploiting Flash vulnerabilities), but additional investigation discovered the Angler exploit kit being used as well.

"By abusing ad platforms – particularly ad platforms that enable Real Time Bidding," FireEye's researchers explained, "attackers can selectively target where the malicious content gets displayed."

"When these ads are served by mainstream websites, the potential for mass infection increases significantly, leaving users and enterprises at risk."

FireEye worked with Forbes and their ad partners, and the malicious ads have been gone since September 15, seven days after they were first detected.

Earlier this month, researchers at Malwarebytes discovered a malvertising campaign using the Angler exploit kit targeting a number of high-profile websites such as eBay (in the UK), Drudge Report, Legacy.com, and Answers.com.

Just this week, the same gang targeted Realtor.com visitors and once again they used the Angler exploit kit as the delivery platform. In each case, the campaign targeted computers with Ransomware or generic malware designed for ad fraud.

The gang behind both incidents leveraged a number of large ad networks, including DoubleClick, AppNexus, ExoClick, and engage:BDR. As is the case with most malvertising, the on-demand platforms are the better target for crooks, because they can target people for little upfront investment and gain access to a steady stream of consistent traffic on the larger websites.

Steve Ragan — *Senior Staff Writer*

Insider: How a good CSO confronts inevitable bad news ›

View Comments