EXHIBIT 5

2014-02-24 - Poisoned YouTube ads serve Caphaw banking trojan - SC Magazine

Wednesday, March 19, 2014
3:57 PM

Poisoned YouTube ads serve Caphaw banking trojan

YouTube's ad network was compromised to host the Styx exploit kit, researchers found.

Recent YouTube visitors should be extra vigilant after ads on the website were found to be poisoned.

According to researchers at Bromium Labs, who blogged about the threat on Friday, YouTube's ad network was compromised to host the Styx exploit kit.

The kit, which in recent news was pegged as compromising online retailer Hasbro.com, was leveraged to spread a nasty banking trojan, called Caphaw, to users.

The Styx exploit kit spread the malware by taking advantage of a Java vulnerability (CVE-2013-2460), which was patched last year.

“We noticed the malware tries to detect the version of Java installed and based on the version, it sends out different URLs to ensure that the exploit is compatible with the Java versions,” the blog post said. “This is a signature of the Styx Exploit kit.”

After working with Google (which owns YouTube) to address the issue, Bromium Labs updated its blog post on Sunday to reveal the “root cause” of the infections.

“Google has confirmed that a rogue advertiser was behind this malvertisment. Google has taken this campaign off and is beefing up internal procedures to prevent such events from occurring again,” the blog post said.

The Caphaw malware that infected YouTube visitors is a variant of banking trojan Shylock, and was used in a campaign last fall which targeted customers of 24 banks around the world.

In that campaign, Caphaw was also believed to have been delivered as part of a crimeware kit that exploited vulnerable versions of Java.