Energy Watering Hole Attack Used LightsOut Exploit Kit

By Dennis Fisher

Published: 2014-03-13 · Archived: 2026-04-02 11:37:42 UTC

A recent watering-hole attack targeted firms in the energy sector and led victims to a separate site that used the LightsOut exploit kit to compromise their machines.

A recent watering-hole attack targeted firms in the energy sector using a compromised site belonging to a law firm that works with energy companies and led victims to a separate site that used the LightsOut exploit kit to compromise their machines.

The attack, which was active during late February according to researchers at Zscaler, follows a familiar pattern seen in many other such attacks. It began with the compromise of a law firm's site at 39essex[.]com and when users hit the site, they were redirected to a third-party site, which hosted the exploit kit. When victims visited the second compromised site hosting the kit, it performed a number of diagnostic tests on the user's browser to see what sort of exploits should be delivered.

The kit checks to see whether Java is running, whether the user is running Internet Explorer and what version of Adobe Reader is installed. Once that information is gathered, the LightsOut exploit kit goes to work, firing exploits against the user's machine.

"Ultimately, a payload is delivered from the LightsOut Exploit kit, which attempts to drop a malicious JAR file exploiting CVE-2013-2465. At the time of research, the binary file was no longer available, which suggests that the attack window has now closed for this particular watering hole. However, other security sources tell us that the site used in the attack is also a known HAVEX RAT CnC," Chris Mannon of Zscaler wrote in an analysis of the attack.

This most recent attack shares a lot of traits with one that ran last fall, and also targeted firms in the energy and oil sector. In that watering hole attack, the attackers were using Java, IE and Firefox exploits and the malware delivered was used to record system configurations and data on the clipboard and from the keyboard.

The researchers at Zscaler said that the similarities between the two attacks is likely not a coincidence.

"It would seem that the attackers responsible for this threat are back for more," Mannon said.

Image from Flickr photos of Joe Stump.
