Microsoft gets busy on fix for IE watering hole attack

January 1 2013, by Nancy Owano

(Phys.org)—Microsoft has published a security advisory about a vulnerability in Internet Explorer 6, 7, and 8. "We are only aware of a very small number of targeted attacks at this time," a Microsoft team blog said. The company acknowledged the vulnerability in its Microsoft Security Advisory (2794220) published on Saturday. Reports about the problem pointed to affected users who had visited the Council of Foreign Relations (CFR) website. According to network security company FireEye, "we can also confirm that the CFR website was also hosting the malicious content as early as Friday, December 21."

CFR is described as a nonpartisan think tank focused on American foreign policy and international affairs. FireEye said the initial JavaScript hosting the exploit only served the exploit to browsers with an

OS language as either U.S. English, Chinese (China), Chinese (Taiwan), Japanese, Korean, or Russian.

Microsoft described the nature of the vulnerability as a "remote code execution vulnerability that exists in the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user within Internet Explorer. An attacker could host a specially crafted website that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view the website."

Outside Microsoft, security bloggers are referring to the attack on the CFR website as a "watering hole attack." In this type of activity, the attackers identify specific targets and scout out which sites they frequently visit. Attackers then plant malware on them. As Kaspersky Lab's *Threatpost* similarly explains, it is "where a website frequented by topically connected subjects is infected with malware hoping to snare those site visitors in drive-by attacks."

Symantec views the metaphor of a watering hole fitting, as "the attack is similar to a predator waiting at a watering hole in a desert. The predator knows that victims will eventually have to come to the watering hole, so rather than go hunting, he waits for his victims to come to him. Similarly, attackers find a Web site that caters to a particular audience, which includes the target the attackers are interested in. Having identified this website, the attackers hack into it using a variety of means. The attackers then inject an exploit onto public pages of the website that they hope will be visited by their ultimate target. Any visitor susceptible to the exploit is compromised and a back door Trojan is installed onto their computer."

Microsoft has responded with mitigations and workarounds. The

company said the IE team is working on a security update but in the interim it recommended that IE8 customers block the current attacks by disabling Javascript, which will prevent the vulnerability from being triggered initially, and disabling Flash, which will prevent ActionScript-based heap spray from preparing memory such that the freed object contains exploit code. Microsoft said also that "disabling the ms-help protocol handler and ensuring that Java6 is not allowed to run will block the ASLR bypass and the associated ROP chain." Microsoft is working on a Fix-It protection tool as well as security update.

Users of IE9 and 10 are not susceptible to the attacks. "We want to reiterate the IE9 and IE10 are not affected and that we currently see only very targeted attacks," Microsoft stated.

More information: technet.microsoft.com/en-us/se … ity/advisory/2794220