Tool Turns Any JavaScript-Enabled Browser into a Malicious Drone

March 27 2007

A new tool too dangerous to give away can turn any PC - Windows, Mac, Linux - or any device with a browser into a site attacker.

The tool, called Jikto, is a Web application scanner that searches for cross-site scripting vulnerabilities. Billy Hoffman, a security researcher with SPI Dynamics, demonstrated what the tool could do at the ShmooCon hacker convention March 24. Namely, Jikto, which is written in JavaScript, can surreptitiously latch onto a browser that has JavaScript enabled.

After silently inserting itself to run inside any browser - be it that of a PC, a cell phone - Jikto can then search sites for cross-site scripting vulnerabilities and report its findings to a third party without the user of the infected browser being aware.

It can also replicate itself onto sites containing cross-site scripting vulnerabilities and then spread via latching onto visiting browsers, Hoffman told eWEEK in an interview.

This is something that JavaScript wasn't supposed to be able to do, but unfortunately, Hoffman said, it can.

JavaScript was originally Netscape's version of the ECMAScript standard, a scripting language based on the concept of prototype-based programming.

Now controlled by the Mozilla Foundation, JavaScript is best known for its client-side use in Web sites.

In that context, a major use of JavaScript is to write functions that are embedded in HTML pages and which interact with the DOM (Document Object Model) of the page to do things that HTML can't do on its own: create pop-up windows, validate Web form input values or change images as a mouse cursor moves over them, for example.

Web application vulnerability scanners have been around some seven years. Most have been software installed on a PC.

Jikto, because it's written in JavaScript, doesn't need to be grounded on a client, Hoffman said.

"Your browser just visits a page. If it contains JavaScript, it can start scanning other sites for vulnerabilities," he said.

The ShmooCon audience, which contained members of Microsoft's Internet Explorer team and representatives from Mozilla - the makers of the FireFox browser - were "kind of shocked" to learn what the evil one can do with JavaScript, Hoffman said.

That's good, the security researcher said - "By getting them interested, we can use that to - heighten the awareness of the dangers of Web site vulnerabilities ."

As it is, over the past few years, security researchers have seen attackers doing much more with Web site vulnerabilities, particularly with cross-site scripting vulnerabilities, where attackers can inject JavaScript into a site, he said.

For example, instead of typing a message or a question on an online

guestbook or forum, an attacker could insert JavaScript. The malicious HTML then downloads to a browser.

Examples of recent JavaScript exploits have included the Windows Live Italy search engine getting hit by a link bomb earlier in March, with some 95 percent of search results on "hot" keywords leading to malware and exploit sites.

Symantec reported that encrypted JavaScript was redirecting visitors. Other recent JavaScript exploits include the Yamanner virus that struck Yahoo's Webmail system and the Samy worm attack that targeted users of MySpace, Hoffman pointed out.

"We've seen - worm attacks - before, but infecting desktop applications," he said.

The Web appeals to attackers because it's ubiquitous, thus making a much more efficient delivery vehicle, Hoffman said: It will carry an attack to Windows, Linux, Mac, cell phones, smart phones or anything that understands JavaScript.

"I could write a piece of malware to only infect Windows or Linux users, or write it in JavaScript and have it infect everybody."

"JavaScript is kind of limited in what it's supposed to do," Hoffman told eWEEK. "But in the last few years people have found all kinds of neat tricks you can do with JavaScript."

Hoffman had originally intended to publicly release Jikto at ShmooCon, but said he reversed himself at the behest of SPI Dynamics officials, due to the damage attackers could do with the tool.

"We tend to use this as an educational process, to show look, this is

where we are now with how bad things can be," he said.

Education is certainly needed, Hoffman said, given that most developers he knows are two and a half to three years behind on security.

"I wanted to get everyone cooked up and say, 'Here's all the things we're seeing it do in the wild.'"

While some security professionals have noted the rising number of cross-site scripting attacks, only recently have those attacks become "really, really dangerous," Hoffman said.

Outside the security industry, the awareness of the dangers are low. "We need to start taking Web vulnerabilities seriously," he said.

The question is, who can patch a browser to be immune to an attack such as Hoffman demonstrated with Jikto? No one, Hoffman said, because "there isn't anything fundamentally wrong with IE or Firefox."

Nor is the problem with JavaScript. The problem is that JavaScript is simply capable of doing things that can be subverted, Hoffman said.

"Some of its capabilities allow it to be used this way," he said. "It's like I have this crowbar, which I can use to break into a car, but it's also good for a lot of - positive - things as well. JavaScript isn't evil or bad inherently. It's just you can do things with it people didn't intend for you to do."

As it is, big Internet players including Google, eBay, PayPal, Yahoo and the Mozilla Foundation have found themselves used as cross-site scripting platforms due to vulnerabilities.

Just as they have addressed it, so too must smaller companies, Hoffman

said.

"Google and Yahoo and eBay and PayPal, they throw millions a year, if not tens of millions, at Web security, at designing applications securely from the start," he said. "And even they make mistakes. But the big guys take this seriously. Small to medium companies with Web presence … should take it seriously. If - the big guys are - making mistakes, and they're pretty smart, chances are you're making mistakes too."

The fact that SDI Dynamics refrained from releasing the code should be no comfort. If Hoffman knows about the ability to use JavaScript maliciously in this way, as he demonstrated with Jikto, others certainly do as well.

"I'm not that smart a guy," he said. "If I'm talking about it at a conference, you better believe somebody else has figured it out. Those people have not told people about it" because they're likely quietly exploiting JavaScript in this way, he said. "They're likely selling - such code as - exploits, using to find vulnerabilities, or all sorts of things."

Jikto is more a proof of concept code sampling than a tool per se, Hoffman said.

"It's fairly easy for someone to reproduce my work. It's proof of concept code, maybe 900 lines of code total. Most of that was comments to myself and spacing. It wasn't that sophisticated a concept."Maybe not, but it did serve to show that "everybody has to get rid of cross-site scripting vulnerabilities," Hoffman said. "People who think it's not a problem should look to Google's" susceptibility, he said.

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

Citation: Tool Turns Any JavaScript-Enabled Browser into a Malicious Drone (2007, March 27) retrieved 9 April 2024 from
https://phys.org/news/2007-03-tool-javascript-enabled-browser-malicious-drone.html