Crooks have new chances as websites grow more complex

May 20 2010, By Steve Johnson

Cyber crooks are increasingly targeting the growing array of Web applications -- everything from interactive maps to stock tickers -- potentially giving them access to the credit card and Social Security numbers of people using those sites.

Despite the increased security threat, experts say, some Silicon Valley companies and others that make the software enabling many of these online features aren't responding quickly to fix the flaws.

"It's a wild, wild world out there," said Mandeep Khera, chief marketing officer at Santa Clara, Calif.-based Cenzic, which sells software to help ward off hackers. Despite a growing effort to beef up security on the Internet, he added, "consumers need to be aware of how vulnerable most of these websites are."

Hoping to attract the public, businesses and others on the Web in recent years have added more and more applications. This includes multimedia players, document readers, auction features, reservation systems, video games, calendars, stock tickers, currency converters and e-commerce payment systems.

But to make those features work requires layers of sophisticated software. And keeping all that code free of the cracks that crooks can infiltrate isn't easy, according to Tom Cross, manager of IBM's X-Force Advanced Research unit, which monitors cyber threats, "The reality is that the more complicated this code gets, the more potential for vulnerabilities there is," he said. "We're also seeing an increased sophistication in the people committing these kinds of crimes."

In March, Miami computer hacker Albert Gonzalez was sentenced to 25 years in prison for orchestrating one of the nation's largest credit- and debit-card thefts, which he and his cohorts carried out after identifying vulnerabilities in various businesses' websites.

In January, Google revealed that a series of cyber attacks originating from China had pilfered its intellectual property and targeted about 30 other Silicon Valley companies.

In July last year, Twitter acknowledged that a French hacker who broke into its site had accessed sensitive company documents and, reportedly, the accounts of President Barack Obama.

"Every 1.3 seconds a new Web page is getting infected," according to a recent report by Dasient, an Internet security firm in Palo Alto, Calif. "Users who interact on the Web ... are therefore at great risk."

"It's pretty bad out there now," agreed Jeremiah Grossman, chief technology officer of Santa Clara-based WhiteHat Security, which helps website operators spot vulnerabilities. But given how fast applications are being added to the Internet, he predicted, "it's likely to get worse."

The danger is acute for consumers, experts add, because just visiting a site can leave them exposed to a cyber attack.

Much of the software incorporated into Web applications comes from big corporations. But the speed with which they fix the problems varies greatly, according to a study in February by IBM's X-Force group.

By the end of 2009, the report said, Oracle left 38 percent of such flaws without patches, Google 25 percent and Apple 22 percent. Hewlett-Packard, Adobe Systems, Cisco Systems and Mozilla failed to provide patches for just 5 percent or less of what it called "their critical and high vulnerabilities."

Oracle declined to discuss the study, and Apple did not respond to a Mercury News request for comment. But Google issued a statement disputing the study's accuracy, saying "a sizable number of flaws" the report claimed hadn't been fixed actually were. "Google contributes substantial resources and expertise not only to improving the security of our own products but also to enhancing the security of the broader web," the statement added.

Several security experts said such differences of opinion can happen because not everyone agrees on what constitutes a vulnerability. Moreover, they said, many website operators use their own customized software and often aren't aware of the weaknesses lurking in their applications.

Even when holes are identified, those responsible for sealing them may be reluctant to do so because of the cost. Some flaws can be patched for a few thousand dollars, experts said. But to design, test and widely disseminate a complicated fix for a major glitch, "you are talking in the millions of dollars," said Francis deSouza, a senior vice president at Symantec of Mountain View, Calif., which provides information security services.

Another problem, experts said, is that colleges and universities do not routinely teach software engineering students how to keep crooks from compromising their code. Plus, the wide variety of software used for Web applications makes it difficult to establish uniform protections for the public.

"It's like editing a book with people of all different grammar styles," said Rob Lee, a faculty fellow at the SANS Institute, a Maryland-based cybersecurity education organization. "Are you going to catch every mistake? It's a challenge, but it's one that needs to be taken on."

PATCHING VULNERABLE WEB APPLICATIONS:

An IBM report in February found wide variations in how some Silicon Valley companies responded to security holes in their software. Here are the percentages of "critical and high vulnerabilities" that it said were left without a security patch at the end of 2009.

- Oracle: 38 percent

- Google: 25 percent

- Apple: 22 percent

- HP: 5 percent

- Adobe: 4 percent

- Cisco: 1 percent

- Mozilla: 0 percent

Source: IBM X-Force 2009 Trend and Risk Report

STAYING SAFE ONLINE:

Once credit card or other personal information is shared with a website, keeping that from hackers can be difficult, given the vulnerabilities of many web applications. Here are some steps consumers can take:

• Don't click on any Web ads or pop-ups

• Update to the latest version of your browser

• Use a virtual credit card that expires after one use. These are available from credit card companies and banks.

• Check with your credit card company about shopping sites you're considering using.

• Ask the site's webmaster how the site is secured.

Citation: Crooks have new chances as websites grow more complex (2010, May 20) retrieved 24 April 2024 from https://phys.org/news/2010-05-crooks-chances-websites-complex.html