COMPUTERWORLD
THE VOICE OF IT MANAGEMENT

How CAPTCHA got trashed

The wiggly words are now most useful for malware authors

Steven J. Vaughan-Nichols 15/07/2008 09:02:49

CAPTCHA used to be an easy and useful way for Web administrators to authenticate users. Now it's an easy and useful way for malware authors and spammers to do their dirty work.

CAPTCHA -- Completely Automated Public Turing Test to Tell Computers and Humans Apart -- was a good idea in its day. You presented users with an obfuscated string of characters and then had them decode and type the string in to get an e-mail account, a social networking account or comment access on an online forum. Not much fuss (though users justifiably complained that the difference between 1 (one) and l (the lower-case letter l) can be hard to see in many fonts) and certainly no muss from a Web administrator's point of view.

So it was that CAPTCHA went from relatively obscure security measure perfected in 2000 by researchers at Carnegie Mellon University to deployment by most of the major Web e-mail sites and many other Web sites by 2007. Sites such as Yahoo Mail, Google's Gmail and Microsoft's Hotmail all used -- and, for that matter, continue to use -- CAPTCHA to make sure that only human beings, not bots, could get accounts or make postings.

Those days are long gone.

By January 2008, Yahoo Mail's CAPTCHA had been cracked. Gmail was ripped open in April. Hotmail's top got popped during the same month.

And then things got bad.

There are now programs available online (no, we will not tell you where) that automate CAPTCHA attacks. You don't need to have any cracking skills. All you need is a desire to spread spam, make anonymous online attacks against your enemies, propagate malware or, in general, be an online jerk.

It's not just free e-mail sites that can be made to suffer, though.

John Nagle, founder of SiteTruth, a site that tries to identify bogus businesses and their Web sites, wrote in late May on Techdirt that while spam on the popular online classified ad service Craigslist "has been a minor nuisance for years ... this year, the spammers started winning and are taking over."

Craigslist tried "to stop spamming by checking for duplicate submissions," Nagle explained. "They check for excessive posts from a single IP address. They require users to register with a valid e-mail address. They added a CAPTCHA to stop automated posting tools. And users can flag postings they recognize as spam."

According to Nagle, growing sophisticated, "Several commercial products are now available to overcome those little obstacles to bulk posting. A tool called CL Auto Posting Tool is one such product. It not only posts to Craigslist automatically, it has built-in strategies to overcome each Craigslist anti-spam mechanism." It's not the only one. There are, he added, "other desktop software products [such as] AdBomber and Ad Master. For spammers preferring a service-oriented approach, there's ItsYourPost." The result? "The defenses of Craigslist have been overrun. Some categories on Craigslist have become over 90 per cent spam. The personals sections were the first to go, then the services categories, and more recently, the job postings."

Of course, you don't have to pay anything. There are now free CAPTCHA crackers available online.

Craigslist is fighting back. The organization is now using phone verification for some ads. Crackers, in return, are working on a way to break Craigslist's phone defenses. With combat costs mounting, it's hard to see how Craigslist, which has always been a free service, can continue to survive with its no-visible-means-of-revenue model.

It's not, as the Craigslist situation shows, that malicious e-mail is the only problem coming from broken CAPTCHA security. Paul Wood, senior analyst at MessageLabs, a UK-based e-mail security company, says, "MessageLabs have already begun to see examples of spammers exploiting other techniques once they have bypassed the CAPTCHA of Google and Hotmail -- for example, using Google Docs to create spam content and including the link in the spam e-mail messages, evading traditional antispam techniques that rely on identifying known spam domains in URLs."

Social network users are also vulnerable to attack from CAPTCHA-compromised sites, says Stephan Chenette, manager of security research at Websense Security Labs.

"The newer generation doesn't use e-mail to communicate," Chenette explains. "Instead, they use social networks, and they're not too concerned about revealing their personal information on social networks or blogs where they post instead of sending e-mail. What happens is that an attacker creates a public blog of his own or sets up an account; he can then use these to publish malicious links. By exploiting the trust of the people on that community, he uses them to spread botnets and the like."

Because social networks offer such an "enormous attack surface" and "their users don't think of themselves as being vulnerable in the same way experienced e-mail or IM users are," they're especially easy to exploit, says Chenette.

Another new attack vector is coming from CAPTCHA's collapse: the quick creation of fake Web sites. According to Chenette, these sites get their content from legitimate Web sites by copying and pasting to maximize their search engine optimization and reputation to quickly gain an audience.

"Reputation is all the rage for malicious attackers. From a search engine perspective, the content is what matters. Malicious attackers will pull sites' contents and embed it in their site, and that gives them a high search-engine ranking, which gives them a higher reputation," says Chenette. "We've been seeing that quite a lot recently. Of course, search engine poisoning is quite old, but now reputation sites [such as Digg] that use CAPTCHA are being targeted."

So with all these problems, all these new ways to attack users both by e-mail and on social networks and blogs, is there any hope for CAPTCHA?

No, not really.

"I think my view on this now is that time is definitely running out for current CAPTCHA systems; already they are not as effective as they once were," says Wood. "It's already becoming more difficult for real customers to use them successfully, and they continue to come under increasing pressure from spammers."

Chenette goes further: "CAPTCHA has been broken for the last year and a half. The technology has really not progressed. They've got a little bit harder but the hackers have made programs that can easily break them. This works both with print and audio CAPTCHA. All of these have been broken in one way or the other."

Chenette says it's a "fundamental problem with no simple answer." After all, "harder CAPTCHA solutions mean harder problems for people as well." And he believes that "the idea behind CAPTCHA may need to be part of a solution."

Chenette doesn't expect that a one-size-fits-all solution will emerge, however. "Each site will have to choose its own answer. Financial sector sites, for example, will be more difficult than a free social-networking site," he notes.

Wood expects to see CAPTCHA replaced soon. "I would expect to see some sites introducing new techniques to replace the existing CAPTCHA models, maybe as early as the beginning of next year, perhaps involving 3-D spatial perception, such as the one created by SpamFizzle," he says.

And if that fails in its turn, well, there's always CAPTCHAs like the one used by Quantum Random Bit Generator Service.

Computerworld Buyer's Guide - Vendors Matched to this Article

Dimension Data , **Trend Micro** , **GFI** , **SonicWALL** , **Secure Computing** , **MessageLabs** , **CA**

More about Websense, Google, Microsoft, Mellon, MessageLabs, Yahoo, Carnegie Mellon University, Quantum

Login or register to post comments