WIRED

Details of DNS Flaw Leaked; Exploit Expected by End of Today

By Kim Zetter July 22, 2008 | 5:15:06 PMCategories: Cybersecurity, Glitches and Bugs, Hacks and Cracks

Despite Dan Kaminsky's efforts to keep a lid on the details of the critical DNS vulnerability he found, someone at the security firm Matasano leaked the information on its blog yesterday, then quickly pulled the post down. But not before others had grabbed the information and reposted it elsewhere, leading Kaminsky to post an urgent 0-day message on his blog reading, "Patch. Today. Now. Yes, stay late."

Hackers are furiously working on an exploit to attack the vulnerability. HD Moore, creator of the Metasploit tool, says one should be available by the end of the day.

Earlier this month, Kaminsky, a penetration tester with IOActive, went public with information about a serious and fundamental security vulnerability in the Domain Name System that would allow attackers to easily impersonate any website -- banking sites, Google, Gmail and other web mail websites -- to attack unsuspecting users.

Kaminsky announced the vulnerability after working quietly for months with a number of vendors that make DNS software to create a fix for the flaw and patch their software. On July 8, Kaminsky held a press conference announcing a massive multivendor patch among those vendors, and urged everyone who owns a DNS server to update their software.

But Kaminsky broke one of the fundamental rules of disclosure in announcing the bug. He failed to provide details about the flaw so system administrators could understand what it was and determine if it was serious enough to warrant an upgrade to their systems.

Kaminsky promised to reveal those details next month in a presentation he plans to give at the Black Hat security conference in Las Vegas. But he said he wanted to give administrators a 30-day head start to get their systems patched before he provided details that could allow hackers to create an exploit to attack the systems.

Kaminsky asked researchers not to speculate about the bug details in the meantime and to trust that it was a serious issue. Some did as he asked. But many security researchers took his coyness as a challenge to uncover the details Kaminsky was holding back.

Halvar Flake, a German security researcher, was the first to publish details that correctly speculated on the bug, though Kaminsky told Threat Level that others figured out the bug many days before Flake published his findings. Flake's post also didn't provide all of the correct details about the bug. But Matasano took care of that issue when it spilled the beans in a post that has garnered heavy criticism from other security researchers who accuse Matasano of irresponsible disclosure and of trying to get publicity by stealing attention from Kaminsky's Black Hat talk next month.

The disclosure was bound to happen, however, since Kaminsky had been forced to provide details of the bug privately to numerous people who balked at patching their systems without knowing the exact nature of the bug. In the absence of these details, some system administrators and security researchers had accused Kaminsky of rehashing an old, known vulnerability in DNS to gain notoriety.

Matasano's founder, Thomas Ptacek, had been one of the researchers who doubted Kaminsky's findings, but he recanted after Kaminsky disclosed details of the bug to him in private. Ptacek wasn't the employee whose name appeared at the bottom of the Matasano post disclosing the information, but the founder apologized today for disclosing the information. In the message he said the company had written the post in anticipation of publishing it as soon as Kaminsky or someone else spilled the details, implying that the early publication had been unintentional.

The DNS flaw that Kaminsky discovered allows a hacker to conduct a "cache poisoning attack" that could be accomplished in about ten seconds, allowing an attacker to fool a DNS server into redirecting web surfers to malicious web sites.

DNS servers do the job of translating a web site's name to its address on the internet -- for example, translating www.amazon.com to 207.171.160.0 -- so a browser can bring up the web site for a user. A cache poisoning attack allows a hacker to subvert a DNS server to surreptitiously translate a website's name to a different address instead of the real address, so that when a user types in "www.amazon.com," his browser is directed to a malicious site instead, where an attacker can download malware to the user's computer or steal user names and passwords that the user enters at the fake site (such as e-mail log-in information), similar to the way phishing attacks work.

"It's a really bad bug that really impacts every web site you use and your readers use," Kaminsky said. "It impacts whether or not readers are even going to see the article you're about to write."

Kaminsky told Threat Level he's not interested right now in slinging mud with Matasano and others over how the information has been disclosed. He just wants people to patch their systems.

He also says he's happy that administrators have had some time, though not as much as he'd hoped, to get their systems patched before the information went public.

"We got thirteen days of a patch being out without the bug being public," he said. "That's unprecedented. I'm pretty proud of at least thirteen days. I would have liked thirty, but I got thirteen."