COMPUTERWORLD
Security

Researchers unleash DNS attack code

HD Moore unveils two exploits for Dan Kaminsky's critical Internet routing bug

July 24, 2008 (Computerworld) Just days after details of a critical bug in the Domain Name System (DNS) software went public, researchers released attack code that can silently redirect users to unintended sites.

HD Moore, the creator of the Metasploit penetration testing framework, and a hacker who goes by the alias "I)ruid," published the attack code in two parts yesterday and today to several security mailing lists and to the Computer Academic Underground Web site.

The two exploits do essentially the same thing, said Andrew Storms, director of security operations at nCircle Network Security Inc.; both poison a DNS server's cache, and therefore can, at least temporarily, replace the legitimate addresses in that cache with bogus destinations. Users steering to what they believe are valid sites could, if they pull the routing information from a victimized DNS server, be sent instead to a fake site such as a phony banking site, where they could be easily duped into divulging confidential information.

Yesterday's exploit, explained Storms, lets an attacker poison a DNS server's cache with a single malicious entry, but today's attack code allows a hacker to poison large quantities of domains with one fell swoop. "This second exploit has the potential for a much larger impact," said Storms, "and could result in potentially thousands of fake addresses inserted into a DNS server's cache.

HD Moore, however, noted that the single entry exploit of Tuesday gives attackers more anonymity, while today's exploit requires hackers to have a real DNS server. "That means they'll be less anonymous," Moore said, adding that it would be possible to trace the DNS requests back to the fake server operated by the attacker, then have it taken offline by, for instance, the host provider.

"Both [kinds of attacks] will be difficult to detect," Storm said. "It will probably take an end user to raise the flag when they go to their banking site, for example, and then report, 'Hey, this just doesn't look quite right.'" Digging through the enormous amount of data generated by a DNS server -- hundreds of thousands of results in an hour at a company like nCircle, said Storms -- is simply impossible.

The DNS cache-poisoning bug exploited by Moore's and I)ruid's attack code was first announced earlier this month by Dan Kaminsky, director of penetration testing at Seattle-based IOActive Inc. The bug, which Kaminsky uncovered earlier this year, was patched that same day by several major vendors, including Cisco Systems Inc., Internet Systems Consortium Inc. and Microsoft Corp.

Although Kaminsky declined to publicly disclose technical information, he briefed several fellow security researchers after he was criticized for overstating the seriousness of the threat. Those researchers recanted, and said Kaminsky's research was on target.

Monday, however, a German hacker went public with his guesses about the bug's details. His speculation was confirmed later in the day by Matasano Security, a consultancy that included at least one researcher who had been briefed on the bug by Kaminsky.

That was when Moore and I)ruid started working on the attack code, Moore said today. "We were keeping an eye on it before, but we didn't really start until Monday," he said. "There have been tools available to check to see if you needed to patch [the DNS software], but there wasn't any way to actually see if you could actually do this attack."

The exploits have been added to the Metasploit framework, said Moore, but at the moment can be launched only from systems running Linux. He said that work on exploits able to run from Mac OS X and other operating systems would start soon, but that the attack code would not be tweaked for Windows. Because of the way the exploits are written, they "would never work on Windows."

That doesn't mean Windows users are safe, however. Although the current exploits can't be launched by attackers from a Windows PC, end users running Windows are at risk if they don't apply this month's DNS patches.

Storms didn't dismiss the possibility of attacks now that exploit code is available, but downplayed the threat because of all the attention the bug has received. "I think the likelihood of a mass attack is limited," said Storms, "because a whole lot more people understand how DNS works than did several weeks ago."

Users should patch now, said Storms, even if they're not operating a DNS server. "It's important that you look at the Microsoft patch now," he said, referring to the fix Microsoft issued two weeks ago for every version of Windows except Vista.

"Anytime you can change [entries on a] DNS server, you run into a lot of other issues, including drive-by Web attacks," warned Moore.