Ask any security professional to name the most commonly exploited services and chances are the Domain Name Service (DNS) will be near the top of the list.

Security Wire Weekly: Kaminsky at Black Hat 2008

Listen to clips of Kaminsky's Black Hat 2008 presentation in Las Vegas.

This seemingly simple service, responsible for translating between human-friendly domain names (e.g. searchsecurity.techtarget.com) and machine-friendly Internet Protocol (IP) addresses (e.g. 65.214.43.37) has always been an attractive target for those seeking to do harm since it plays a critical role in the Internet's infrastructure. If DNS is compromised, Internet traffic can be redirected at will: powerful stuff for purveyors of malware and phishing attacks.

At the 2008 Black Hat briefings, security researcher Dan Kaminsky revealed the details of a "new" flaw in DNS (or, more accurately, the new combination of two old flaws in an effective vulnerability cocktail).

It's worth noting that Dan followed the responsible disclosure process; he informed major DNS software vendors of his discovery months before his Black Hat presentation. However, as often happens with major vulnerabilities, some details about the DNS flaw leaked in advance of Black Hat, leading to a whirlwind of speculation and panic as white hats scrambled to patch their servers before the black hats developed exploit code. As I write this, there is already DNS exploit code in the wild.

Kaminsky's DNS exploit explained
So how does Dan's attack work? It's based upon two well-known vulnerabilities in DNS: transaction ID guessing and referral records. When a server makes a DNS request, it identifies the request using a unique transaction ID that enables the server to validate responses and ensure that they're from the correct query.

The problem is the transaction ID range is limited to 65,535 possibilities, making a guessing attack possible. If an attacker knows a DNS query is being issued, he can attempt to forge a response to that query with a random transaction ID. In that case, he has a 1 in 65,535 chance of getting it right.

The second problem involves the ability of a DNS server to include more information in a response packet than a single DNS entry. For example, an attacker who owns a DNS server for a site called evilmalware.com could respond to queries for that domain with not only the IP address for evilmalware.com, but also include some additional information: "By the way, SearchSecurity.com is located at 1.2.3.4" (where 1.2.3.4 is a site under the control of the hacker, and, by no means the real SearchSecurity.com). This was solved long ago with the concept of bailiwicks. Basically, DNS clients now know to only accept responses that answer questions that they asked and to discard any extraneous information packaged with the requested address.

Either of these vulnerabilities by itself isn't really a big deal: they've both been documented for years. Odds like 1:65,535 aren't very appealing to hackers and all current versions of DNS support bailiwick protection. The intriguing twist in Kaminsky's attack is the way he combines the two. First, he points out that there's no limit on the number of incorrect transaction IDs you can guess, so it's basically a race between the hacker and the legitimate server. If an attacker can send 100 false responses before the legitimate server replies (a feat which Kaminsky claims is possible), the 1:65,535 odds can be improved to a much more favorable 1:655.

At this point, you may be asking yourself, what's the big deal? If a malicious hacker wins the race, he or she is only able to poison the DNS for that specific query. That's where the true danger of Kaminsky's attack comes into play. His second significant contribution is noting that, although bailiwicks apply for most DNS response data, they don't apply for referrals to other DNS servers. So, an attacker could respond to the evilmalware.com query with a response stating, effectively, "I don't know, but you can find it at searchsecurity.techtarget.com, which is located at 1.2.3.4." In accomplishing this, it's possible to direct traffic to arbitrary locations of an attacker's choice.

Patching the DNS flaw
Fortunately, Kaminsky also describes a response and has spent the last several months furiously spreading the news among DNS server vendors. The answer is to use source port randomization. This removes the currently predictable nature of DNS source ports and replaces it with a randomized selection technique. Now, the attacker needs to guess not only the correct transaction ID, but also the correct UDP port to flood with replies. This will result in a much more unwieldy
1:163,840,000 success rate, rendering the attack useless.

Security managers reading this should immediately determine whether the DNS servers covering their enterprises are vulnerable to the attack and, if they are, patch them immediately. As of today, patches are available for all major operating systems through normal support channels. To test servers for the vulnerability, Kaminsky provides a nifty DNS Checker tool that sends a bunch of queries to his own DNS server and then analyzes them for the use of predictable source ports.

**Protect remote connections from DNS flaw**

Once an organization has patched its own DNS servers, there's still more work to do. Users operating within the friendly confines of the corporate infrastructure are protected, but it's important to remember that this isn't the only place that users access the Internet. They work from home and travel, taking advantage of Internet access (and DNS services) offered by various commercial ISPs, hotels, restaurants, airports and other Wi-Fi hotspots.

That said, so far the DNS vulnerability has been a case study in security awareness and prompt patching. At Dan's talk, he cited statistics that more than 80% of DNS servers worldwide are already patched, including many of those used by major providers.

This means steps must be taken to protect enterprise users when they're away from the office. While it might be tempting to point them at the DNS Checker tool, that's not really a practical solution, since it requires both remembering to run the check and possessing the technical ability to interpret the results.

A better strategy is to ensure employees use the VPN to connect back to the enterprise infrastructure. Be sure that the configuration isn't using split tunneling and that the VPN pushes DNS configuration. This ensures that remote users will use their enterprise's DNS servers, rather than relying upon those provided by the access site. For the truly paranoid, configure the VPN client with a hard-coded IP address, eliminating the client's reliance on the local network's DNS server to find a path home.

Overall, Kaminsky outlined an extremely serious threat to the security of the Internet. Our shared infrastructure depends upon the proper functioning of DNS and a mutual trust that it properly resolves names. If you haven't already checked the patch status of your servers, do so immediately. Once the remaining 20% of servers are patched, we'll be safe from DNS exploits -- at least until Kaminsky's next Black Hat presentation!

**About the author:**

Mike Chapple, CISA, CISSP, is an IT security professional with the University of Notre Dame. He previously served as an information security researcher with the National Security Agency and the U.S. Air Force. Mike is a frequent contributor to SearchSecurity, a technical editor for Information Security magazine and the author of several information security titles, including the CISSP Prep Guide and Information Security Illuminated. He also answers your questions on network security.

Rate this Tip

To rate tips, you must be a member of SearchSecurity.com. Register now to start rating these tips. Log in if you are already a member.
RELATED CONTENT

- **Network Security Tactics**
  Directory services and beyond: The future of LDAP
  Screencast: Catching network traffic with Wireshark
  Enterprise role management: Trends and best practices
  Using Nessus Attack Scripting Language (NASL) to find application vulnerabilities
  Screencast: Recovering lost data with WinHex
  How to build security into a virtualized server environment
  How to install and configure Nessus
  How to run a Nessus system scan
  Nessus: Vulnerability scanning in the enterprise

- **Emerging Information Security Threats**
  Windows Vista security 'rendered useless' by researchers
  Hacking techniques compromise Windows Vista heap
  Kaminsky: DNS flaw capable of attacks on many fronts
  Hoffman to demonstrate new hacking techniques
  Black Hat Las Vegas 2008: News, podcasts and videos
  DNS flaw handling leaves Kaminsky pleased
  DNS exploit code released by Metasploit founder
  Apple iPhone mail, Safari prone to spoofing
  Noted reverse engineer outs DNS flaw details.
  How can 'DRAM remanence' compromise encryption keys?

- **Security News Makers**
  Hoffman to demonstrate new hacking techniques
  DNS flaw handling leaves Kaminsky pleased
  Valuable lesson emerges from DNS flaw handling
  Citrix executive named Sourcefire CEO
  How can organizations secure implanted microchips and RFID tags?
  Face-Off: Is vulnerability research ethical?
  RSA's Coviello: Security professionals must spark innovation
  Thompson calls for marriage of data and security management
  Microsoft’s Mundie: Let’s talk privacy
  RSA Conference 2008: Special news coverage

RELATED GLOSSARY TERMS

Terms from Whatis.com – the technology online dictionary
DNS rebinding attack (SearchSecurity.com)
- drive-by pharming (SearchSecurity.com)
- JavaScript hijacking (SearchSecurity.com)
- man in the browser (SearchSecurity.com)
- phlashing (SearchSecurity.com)
- polymorphic malware (SearchSecurity.com)

RELATED RESOURCES
- 2020software.com, trial software downloads for accounting software, ERP software, CRM software and business software systems
- Search Bitpipe.com for the latest white papers and business webcasts
- Whatis.com, the online computer dictionary

DISCLAIMER: Our Tips Exchange is a forum for you to share technical advice and expertise with your peers and to learn from other enterprise IT professionals. TechTarget provides the infrastructure to facilitate this sharing of information. However, we cannot guarantee the accuracy or validity of the material submitted. You agree that your use of the Ask The Expert services and your reliance on any questions, answers, information or other materials received through this Web site is at your own risk.