Global Information Assurance Certification Paper

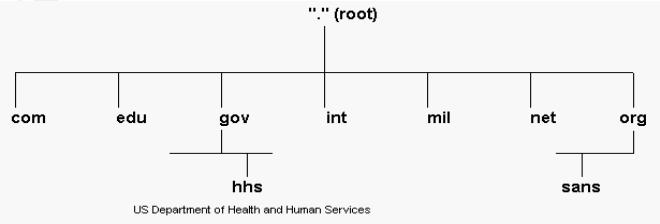
Has your domain been hijacked lately?

It happens more than you hear about. Just lately, many companies have suffered through the surprise, and frustration of having their web and e-mail servers sitting idly by, while all of the internet traffic intended for their network, ends up elsewhere. This is known as domain hijacking. And companies such as Microsoft, Adobe, Nike, Yahoo, and RSA Security, to just name a few, have all suffered through the agony of having their domains hijacked.

DNS Basics

To understand domain hijacking, first we must understand the basics of DNS.[1] DNS (Domain Name Service), is a distributed database that maps domain names, or host names to IP addresses. This is much better than the old way of entering all hosts and IP addresses into a locally stored hosts table manually. Dennis Fisher points out in his article in eWeek February 5th, 2001 titled, "DNS proves to be weak link in Internet Chain,"[2] "That more than 80% of the DNS servers on the internet use BIND (Berkley Internet Name Domain) open source software, to handle the DNS databases, and queries." Unfortunately, BIND was not real secure in its early releases, but with BIND v9 most of the major vulnerabilities have been corrected.

DNS uses a hierarchical inverted tree structure, with a root node and seven subdomain nodes below. These subdomain nodes, which are domains themselves, are the top-level domains and are controlled by ICANN, the Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit, international corporation that was formed in September 1998 to take over global responsibility for Internet Protocol (IP) address space allocation, protocol parameter assignment, Domain Name System (DNS) management, and root server system management functions. These services were previously performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. IANA is now a part of ICANN. Network Solutions Inc. (NSI), is one of the more popular accredited Internet Domain Name registrar's under ICANN.



The 7 top level domains are: .com (commercial), .edu (education), .gov (US governmental), .int (international), .mil (military), .net (network providers e.g. ISP's), and .org (organizations).[3] Then there are subdomains that branch off from the parent domain, e.g. sans.org, or hhs.gov.

When a host tries to go to a site on the internet, it needs to resolve a URL (Universal Resources Locator), e.g. http://www.sans.org, it first queries its local host file, and then will ask the DNS server for help. If the local DNS server has this information, it will return the IP address to the requesting host, e.g. 167.216.133.33. If the local DNS server does not know, it will issue a recursive query, which will search the tree of DNS servers until it finds an authoritative DNS server that has this information.[1] Once the host gets the IP address of the URL, it contacts that host directly by IP address.

Domain Hijacking

Domain hijacking is when incorrect IP addresses get entered into the DNS database, thereby pointing traffic destined for one domain to any domain the hacker chooses. There are several techniques used to hijack domains.

1. DNS Spoofing: There is the technique of fooling the DNS server by spoofing the DNS responses, and making the DNS server "think" it is talking to a trusted server. For example, the spoofing host will then send a command to change the IP address of www.sans.org to www.hackers.net in the DNS server's local database. Because it has fooled the DNS server into believing it is a trusted host, the DNS server allows this update. Now, all traffic that queries this DNS server destined for www.sans.org, will get redirected to www.hackers.net.

2. Cache Poisoning: Is another technique used to hijack DNS information. DNS servers cache all local zone files, and information for all zones the DNS server is authoritative for, and also the history of all recursive queries it's done. The time it holds this information in cache is called the Time To Live, or TTL. It caches this data to help speed up the time it takes the DNS server to respond to a query. The cache gets poisoned when the DNS server gets an incorrect mapping with a high TTL, which allows it to first change the "real" IP address it holds in cache, with a false IP address, and then give out that incorrect information.

3. E-mail Spoofing: Is another very successful technique used to hijack DNS information. DNS names are registered with ICANN, and these transactions are usually done via e-mail. The authentication of the request is usually verified by the return mail address. If that return address is spoofed, and it is confirmed, then the update occurs, causing incorrect IP address information to get stored into the root DNS servers. It is confirmed by sending a confirmation e-mail out to the return address. This e-mail is hijacked by the intruder, who then floods the correct e-mail address to hide this change.[4,5,6]

4. Hack the DNS server: Make sure your DNS server is well protected, because another way to hijack a domain is to hack into the DNS server itself and make the changes directly. This can also be accomplished by getting direct physical access to the DNS server.

5. Human Error: There is always the honest mistake of an administrator entering the information into the DNS servers incorrectly.

Case-in-Point

- As mentioned earlier, there have recently been several high profile companies that have had their domains hijacked. Most notably is the case of Microsoft. This after the embarrassment of the recent security breach of the Microsoft network, causing the potential loss of some of their source code. And Microsoft has now suffered through more problems with users having a difficult time trying to access their network. According to an article by Charles Babcock, from Interactive Week, titled "Microsoft Repels More Attacks,"[7] Charles says their problems started Wednesday January 24, 2001, "when a technician erroneously updated Microsoft's Domain Name Service servers in a move that prevented users from accessing the www.microsoft.com, and www.msn.com sites, for approximately 22.5 hours." And again on January 29, 2001, Microsoft had web, and e-mail servers sitting idly by. According to Microsoft CIO Rick Devenuti, "Someone attempted to block legitimate access to our Web properties by flooding our network routers with large volumes of bogus requests." Charles Babcock then goes on to say, "This attack was the first of its kind, however, to bring down Web sites by targeting, not the Web servers, but the routers sitting in front of them." Michael Warfield, a senior researcher for the X-Force anti-virus team at Internet Security Systems said, "Microsoft was vulnerable to such an attack because it had positioned a set of routers serving its entire site on one network segment. The technician's mistake illustrated to the world that Microsoft had inadvertently created "a single point of failure", and someone found "a big, juicy target" too tempting to resist."

- Another of the high profile cases involved Nike Corporation. In the article "Nike Blames NSI for site hijacking,"[8] Ann Harrison points out "that the hijacking of Nike's Web site sparked an international argument over whether the footwear company or Internet domain-name registrar NSI, should bear responsibility for the temporary theft of Nike.com. The Nike hijack occurred June 21, 2000 when a group calling itself S-11 redirected traffic from Nike.com to servers at a Scotland-based Web-hosting company in a slap at both Nike and the World Economic Forum. Greg Lloyd Smith, director of FirstNET Online in Edinburgh, Scotland, said, "The wayward Nike traffic swamped his company's Web servers and impaired service to its real customers." After unsuccessfully trying to bill Nike for use of his servers, Smith said he's preparing to sue the company, for allegedly neglecting to secure its Internet domain. Nike, in turn, said the responsibility lies with NSI. "Changes to Nike's domain status are supposed to be made only via NSI's encrypted and password-protected security system," said Nike spokeswoman Corby Casler. "But NSI used a spoofed piece

of e-mail from the S-11 group as authorization to change Nike's registry information without requiring a password," she says. The impact on Nike product sales made through Nike.com was minimal during the hijacking, which lasted from six to 24 hours."

- Adobe.com is another of the recent hijacking cases. In the article "Adobe.com Falls Prey to Domain Hijacker,"[9] Brian McWilliams says: "An attacker hijacked Adobe.com from its owner, Adobe Systems Inc., disrupting the big software firm's Web servers and e-mail service. Adobe Systems Vice President of Information Systems Gerrard Rutter confirmed that an as-yet unidentified attacker was able to perform an unauthorized modification of the domain record for adobe.com. The attacker apparently tricked Network Solutions Inc. into transferring the domain record for adobe.com to Paycenter, an ICANN-accredited registrar in China. Besides altering the domain's contact information, the name servers for the address were also modified. The DNS changes caused connections to www.adobe.comto bring up Paycenter's homepage. In addition, Rutter said "Adobe employees were unable to receive e-mail from outside the corporate network for most of the day.""

- RSA Security was another victim of Domain hijacking. In the article "Something Old, Something New: DNS Hijacking,"[10] Mark Joseph Edwards says: "In the case of RSA Security's Web site hijack, someone diverted traffic to a fake Web page after gaining access to an upstream DNS server out of RSA Security's direct control. The intruder accessed the DNS server and temporarily modified its DNS records so those queries destined for RSA Security's Web site would divert to the fake RSA Security Web Site. It's that simple. People thought they had landed on the real RSA Security site when, in fact, they simply landed on a spoofed sited at another IP address."

Summary

These are but just a few of the higher profile documented cases of DNS hijacking. In light of the seemingly simple techniques hackers have used to carry out their evil ways, there are a few things out there that are going to make their lives a little tougher. In the article "Registrar Examines Domain Hijacking Defenses,"[6] by Steven Bonisteel, he points out: "There are three ways to request a change through NSI. Simple e-mail, where the only verification is the "mail-from" address, the second technique uses an encrypted password, or the third way is to use PGP, with a public/private key encryption."
One more of the emerging technologies to help in this area is DNSSec. In the article "DNS security upgrade promises a safer Net,"[11] by Carolyn Duffy Marsan, she talks in depth about: "The new security mechanism, dubbed DNSSec, plugs a hole in the Internet's Domain Name System that hackers have exploited to spoof Web sites. DNSSec prevents these attacks by allowing Web sites to verify their domain names and corresponding IP addresses using digital signatures and public-key encryption. DNSSec is included in BIND v9."

So, in short, there are promising new technologies that will ultimately tighten up the entire DNS structure to make it much more secure and reliable.

References

[1] Mockapetris, P. "Domain Names – Implementation and Specification." RFC 1035 November, 1987 URL: http://www.ietf.org/rfc/rfc1035.txt?number=1035 (2/14/01)

[2] Fisher, Dennis "DNS proves to be weak link in Internet chain" Feb 5, 2001 URL: http://www.zdnet.com/eweek/stories/general/0,11011,2681845,00.html (2/14/01)

[3] Postel J. "Domain Name System Structure and Delegation" RFC 1591 March, 1994 URL: http://www.ietf.org/rfc/rfc1591.txt?number=1591 (2/14/01)

[4] Seifried, Kurt "DNS spoofing/registering/etc" Dec 31 1999 URL: http://archives.neohapsis.com/archives/bugtraq/1999-q4/0545.html (2/14/01)

[5] Vision, Max "Internic Domain Hijacking - "It Happens"" February 10, 2000 URL: http://www.whitehats.com/papers/internic/ (2/14/01)

[6] Bonisteel, Steven "Registrar Examines Domain Hijacking Defenses" June 6, 2000 URL: http://www.info-sec.com/internet/00/internet_060700a_j.shtml (2/14/01)

[7] Babcock, Charles "Microsoft Repels More Attacks" January 29, 2001 URL: http://www.zdnet.com/filters/printerfriendly/0,6061,2679418-35.html (2/14/01)

[8] Harrison, Ann "Nike blames NSI for site hijacking" July 4, 2000 URL: http://www.cnn.com/2000/TECH/computing/07/04/nike.v.nsi.idg/index.html (2/14/01)

[9] McWilliams, Brian "Adobe.com Falls Prey to Domain Hijacker" October 19, 2000 URL: http://www.internetnews.com/wd-news/article/0,,10_489731,00.html (2/14/01)

[10] Edwards, Mark Joseph "Something Old, Something New: DNS Hijacking" Feb 16, 2000 URL: http://www.ntsecurity.net/Articles/Print.cfm?ArticleID=8170 (2/14/01)

[11] Marsan, Carolyn Duffy "DNS security upgrade promises a safer Net" Oct 17, 2000 URL: http://www.cnn.com/2000/TECH/computing/10/17/dns.security.upgrade.idg/index.html (2/14/01)