Cyberoam

Unified Threat Management

White Paper

Pharming Prevention

Cyberoam prevents Sophisticated pharming attacks

Pharming the next generation of phishing attack, also makes the use of social engineering to obtain access credentials such as usernames and passwords of the Internet users. A deceptive Internet threat, it is potentially more sinister than phishing because it circumvents the need to entice users into responding to spam email messages. A pharming attack occurs on a broader front by misdirecting users from legitimate websites to similar looking mirror sites that have been designed to look and feel like the original.

What is Pharming?

Pharming exploits DNS server vulnerabilities, allowing the hacker to acquire domain names of sites and redirecting the site traffic to a mirror site.

These bogus websites collect sensitive personal user information such as account IDs, usernames, passwords and credit card details and send it across to the pharmer all without the user's knowledge.

Statistics from the SANS Internet Storm Center (ISC) show that at least 1,300 web sites were compromised by pharming exploits in early March 2005. As per the warning issued by the ISC, the attacks corrupted the Domain Name System (DNS) Servers, causing legitimate requests to .com sites being misdirected to websites controlled by the pharmers.1
Pharming : The Line of Attack

Since pharming does not rely on the victim taking an action that leads to information theft, it is much more difficult to identify and thus far more effective.

There are two types of pharming attacks. One, that is carried out at the network level corrupts the Domain Name System (DNS) servers while the other alters the PC's host file at the individual level.

- DNS Poisoning is the corruption of Internet server's Domain Name System table by replacing the legitimate DNS entries with fraudulent ones. The DNS translates web and e-mail addresses into a unique IP address. If a DNS directory is "poisoned" - altered to contain the false “Domain name to IP Address” information - users can be silently shuttled to a bogus website even if they type in the correct URL. At this point, apart from information theft, a Trojan, worm or spyware or other malware can be installed on the user's computer to carry out keylogging for the purposes of identity theft.
- Alterations to the PC's host file through emailed viruses like the Banker Trojan accomplishes the same goal as DNS poisoning. Since the web browser checks the local host file first and the data in the local host file overrides the information contained in the DNS serves the pharmer can mislead the users to fake sites designed to make them reveal their personal and financial credentials.

Cyberoam Pharming Prevention

Cyberoam offers highly effective, blended protection from pharming attacks.

Spyware Blocker

Cyberoam takes a blended approach to preventing spyware which can be a precursor to pharming attacks - from entering the network. Spyware Blocker prevents inbound and outbound traffic to sites like P2P and other known spyware carriers. WebCat, Cyberoam site database, has a constantly updated spyware category with comprehensive listing of such sites, ensuring reliable access prevention. The category is updated through a series of measures that ensure comprehensive listing.

Prevents Spam Entry

Cyberoam's pre-integrated Anti-Spam analyses mail content and marks spam with policy-based action of quarantine, tag and deletion options. This prevents virus and Trojan carrying mail from entering the network. In addition, Cyberoam blocks or limits access to hotmail, yahoo and other webmails, delivering further protection.

Prevents Virus Entry

Cyberoam's state-of-the art Anti-Virus solution prevents entry of email viruses and Trojans in addition to web viruses that are used to corrupt the host file in the user's PC.

Prevents DNS Poisoning

Cyberoam offers pharming protection, by directing users to the original site despite a corrupt host file or DNS poisoning, through effective HTTP proxy. Cyberoam DNS Interceptor acts as a transparent DNS server, overriding the request to go to the fake site and directs the user to the original site with the help of its own DNS cache.

In case of fresh requests where the domain name match is not available over the Cyberoam DNS cache, a request is sent to the original DNS servers, thereby ignoring the fake domain name matching.

Building upon the success of phishing, the new breed of pharming attacks has armed fraudsters to reach a wider customer base with very little effort and relatively low detection rates. It is therefore vital that organizations secure themselves early on against such scams. Through its blended approach, using its existing features like Spyware Blocker, Anti-Spam and Anti-virus solutions, Cyberoam delivers dependable protection against pharming attacks with no extra cost involved for this security.

Sources

1.isc.sans.org