

Publication Date: 8/7/2005

Site Defacements

Author

Lew Newlin is CTO of [SiteRecon](#), a provider of internet [email monitoring](#) and [web site monitoring](#) services for business.

Abstract

Site defacements are the fastest-growing area of computer incident. Strategies and actions that can be deployed so you do not become site defacement victim.

Article

A valid fear every webmaster faces is the defacement of their site. According to the Computer Security Institute (CSI), 2005 Computer Crime and Security Survey, web site defacements are the "fastest-growing" area of incident. A check of Zone-H.org seems to validate the finding with a display of over 750 sites defacement for a single date (8/15/2005).

To address defacements, it is first important to understand how defacements occur and what can be done to prevent them. Generally, sites can be vulnerable due to undisclosed vulnerabilities in vendor software, a missing security patch, misconfiguration, and/or bad site programming. Any of these vulnerabilities could permit an attacker to gain access that would allow defacement.

While not much can be done concerning undisclosed vendor vulnerabilities, the other causes are correctable. When vendor security patches are released, install them quickly. When patches are released, many attackers are reverse engineering the patch to discover the vulnerability being addressed. It is not uncommon to find exploit code published on the internet within 48 hours of a patch's release.

Verify your server and site configurations. Specific areas of concern are normally FTP upload rights, site publishing rights, server login privileges, open ports and passwords. Delete or seriously restrict the ability of people to anonymously upload files. Check for the use of default passwords and for ones that can be easily guessed. Double check your systems open ports and the publishing rights of your web server software. Numerous companies offer free products or free initial vulnerability scans that can confirm your system settings. Using the search engine term "free vulnerability scanning" will yield dozens of companies and products.

Check your site code to verify errors and unintended data are being dealt with correctly. Regardless of what a visitor does, input should be validated and all errors should return a graceful message. A few areas to check: are your pages vulnerable to buffer overruns due to incorrect data being entered; are your pages vulnerable to SQL or scripting code injection; does your error messages reveal sensitive information such as connection strings, passwords, or system information?

Establish a schedule and process to monitor system changes, configurations, and code. While researching this article, I noticed a Zone-H posting that a Microsoft United Kingdom site was defaced. While the attacker did not publish how the attack was executed, it is safe to assume configuration played a large role. Software features change with each patch applied, mistakes happen and code changes.

The CSI report points out that the dollar losses caused by web site defacements are actually very low in relation to losses suffered by viruses and the theft of proprietary information. The report goes on to state that "losses (such as the lost future sales due to negative media coverage following a breach)" were not largely represented in the cost figures. I believe that most victims of site defacements will agree that embarrassment far outweighs the dollar loss suffered.

When considering defacement strategies, web site monitoring services should also be considered. Many monitoring services offer the ability to check for the existence of keywords or page changes. While monitoring

services will not prevent defacements, site monitoring will at least alert you of the event. Hopefully, before you suffer negative media coverage.

Copyright 2005, Information Solutions, Inc., All rights reserved.