



The risks borne by one are shared by all: web site compromises

Having your company web site hacked or 'compromised' can be a costly experience for your organisation. There are immediate costs in responding to the compromise itself (and this includes the actual cost of recovery, as well as the loss of revenue during the outage), but the greater damage to your business may only become apparent over time – customers ceded to a competitor as a result of the loss of trust in your service may never return.

The stakes have never been higher. Criminals increasingly recognise the advantage of directly attacking and compromising legitimate web sites, those used every day by the public – web sites like yours.

Criminals exploit the inherent trust consumers and the public have in known brands, whether they are public or private organisations - the greater the popularity of a particular brand, the more attractive a target their web site presents.

The risk of being targeted is rising, but you can defend against the attackers – a basic understanding of attacks and knowledge of the right security tools may be all it takes to keep your site out of the hands of criminals.

How common are web site compromises?

Quantifying the number of web site compromises can be difficult. For obvious reasons companies who are not legally bound to disclose successful attacks may not report them as there are rarely beneficial reasons to do so.

In a recent report, internet security company WebSense identified that during Q3-Q4 2008 “77% of web sites with malicious code are legitimate sites that have been compromised”¹, while 70% of the top 100 web sites (as rated by WebSense) either hosted, or contained a redirect to malware².

Figure 1 shows trends in website compromises as seen by AusCERT from 2005 to 2009. Another source for quantifying defacement attacks is the Zone-H website, which provides an archive of over three million³ defaced websites.

¹ Websense Security Labs State of Internet Security, Q3 – Q4 2008, p2. Available from http://securitylabs.websense.com/content/Assets/WSL_ReportQ3Q4FNL.PDF

² Software designed to perform unwanted or malicious activity eg viruses, spyware, keyloggers

³ Zone-H website, <http://www.zone-h.org>

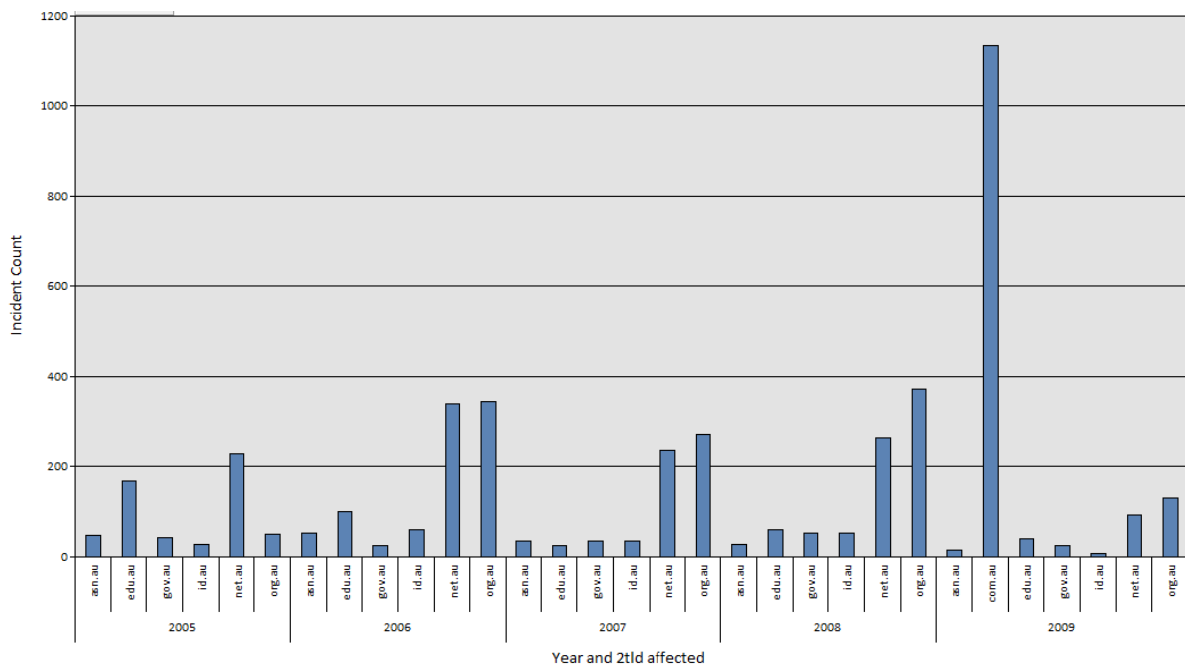


Figure 1

Who's affected by web site compromises?

This is a problem that affects every industry; it is not limited to small businesses and personal web pages. It affects the websites of governments, private enterprise, and educational institutions.

Hacking web sites for fun and profit – attacker motivation

Motivations for hacking websites range from the juvenile to the professional, and are often opportunistic in nature. Some of the more common motivations, inferred from the observable results of the compromise are:

Politics and ego

In attacks where politics or ego gratification is the motivation, content is usually modified to display political messages or graphics; in many cases the attacker will leave their tag (or pseudonym) on the site and attackers will often submit evidence of the attack to sites like Zone-H so a record can be kept and to publicise the attack in the wider security community.

Financially motivated

Financially motivated attacks often cause a visitor to be redirected, usually without their knowledge, to another web site which then attempts to install malware on a user's computer. This is not always the case however, as the attackers may operate the compromised web site for phishing and other similar attacks where user data is captured for later use in criminal activities. AusCERT has seen a surge in the sophistication of these attacks and the determination and resources of the attackers who carry them out.

Hosting of digital contraband

Another reason for attacking legitimate websites is to gain a non-attributable server to host illegal material like child pornography, pirated software and movies. A compromised web

server may also be used as a distribution point for malware used by the hacker community.

Other motivations

There are of course, many other motivations for compromising websites. For example, unethical individuals working in the field of competitive intelligence may compromise a web site to use it as a staging area for deeper attacks into a network, or disgruntled current or former employees may seek revenge by attacking the system to embarrass the company.

Types of vulnerabilities exploited

There are many ways to attack a web site, and most of the techniques involve exploiting a level of trust in one or more directions. For example, when a web site trusts a user to only provide it with information that it expects to see, a rogue user may be able to run code on the web server or cause data to be displayed from unrelated sites and add, modify or destroy information in associated databases.

Attacks which exploit a level of trust include the following:

SQL injection –

This attack occurs when a user is able to pass commands that access or modify information in a database to a web site, which passes the commands directly to the database without checking that the content contains only expected text such as, upper and lower case alphanumeric characters.

Remote file inclusion (RFI) -

This is an attack in which a user is able to pass an arbitrary remote website location as an argument to a script running on the web server, causing the web server to retrieve the file, and execute it. Depending on the permissions granted to the web server, this type of attack may lead to complete compromise of the system on which the web server is running.

Cross Site Scripting (XSS) –

This attack, also makes use of input validation errors, allowing a user to pass script commands to a web server, the server echoes the input provided by the attacker without first checking to see that it is non malicious. While many see this as a nuisance rather than a serious threat, code reuse between the front and back end of a web server may allow an attacker to run script commands on a system within the corporate network.

Cross Site Request Forgery (CSRF/XSRF) –

XSRF can be quite complex – these attacks allow a website, or possibly html content in emails to silently perform actions on another website. For example, if your website developer is logged into your company's website and visits a malicious website then it may be possible for the malicious website to perform actions on your company website by making use of the open session. This process is shown in Figure 2.

Cross Site Request Forgery (XSRF) Example

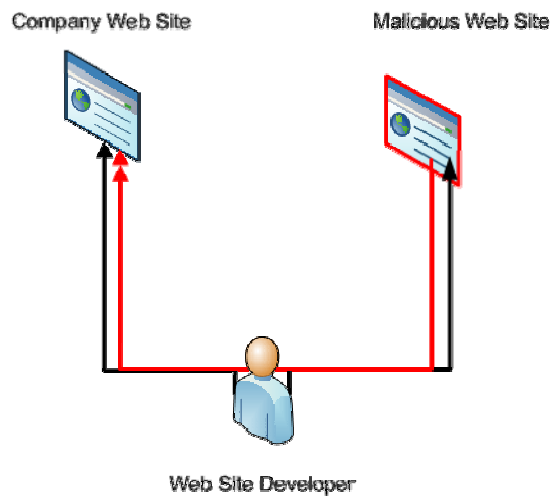


Figure 2

Stolen accounts

Finally, attackers often make use of usernames and passwords obtained by some other means – often a password stealing Trojan program existing on a user's machine. These credentials are then used to connect to web servers and alter existing content or upload new content.

Steps you can take to reduce your risk

Secure Coding and Hosting

Following secure coding practices is the best way to reduce the risk of web site compromise. The Open Web Application Security Project (OWASP) ⁴ offers guidance for many popular languages. If your organisation outsources any of its web development, talk to the developer about their experience in developing secure web sites.

Secure hosting of your web site is also something to consider. There are positives and negatives for in-house versus external hosting. Consider the purpose and popularity of the web site, staff experience, ease of management, how security is managed, costs of responding to attacks, and liability as factors in the decision making process.

Reverse Proxy/Web Application Gateway

A reverse proxy or web application gateway can be used to filter requests for the web sites they protect. Reverse proxies can be dedicated appliances or software implementations. Often, reverse proxies will perform deeper inspection of communications to look for dangerous data and perform virus detection.

⁴ OWASP <http://www.owasp.org>

Penetration Tests

Performing penetration testing using freely available tools is a good way to identify the obvious vulnerabilities in your web applications. It may also be desirable to have a third party test for vulnerabilities, which can yield better results than a simple automated scan. Penetration testers are often highly skilled, but choose your provider with care. Talk to others in your industry to identify possible testers, and the experiences of your peers. Remember however, that the results of a penetration test will only be useful if they are acted upon.

Review your logs

Despite taking measures to reduce the risk of compromise, there are no guarantees of a successful defence. Regularly reviewing logs on web servers should still be carried out, looking for successful or unsuccessful attacks that may have bypassed other countermeasures. This will help you to better adapt your countermeasures to the threats you face.

Conclusion

Web site attacks pose a serious risk to the reputation of organisations and the security of computers that connect to them. Organisations need to look beyond their own direct risks and ask themselves whether they are prepared to expose potential customers and the public to unnecessary security risks such as identity theft and fraud.

While attacks are commonplace, most can be prevented through secure coding practices and adequate ongoing security management.⁵

⁵ First published in 'Business Data Strategy' magazine, eZine and www.bdstrategy.com.au.