Symantec | Website Security Solutions

WEBSITE SECURITY

SIX THINGS THAT CAN KILL YOUR WEBSITE
AND HOW TO STOP THEM

Whitepaper Report

Published April 2013

Symantec | Website Security Solutions

Your website is your shop front, your brand on display and an essential sales and marketing tool. You spent a lot of money building it and attracting visitors. It is business critical: it would be a disaster if that shop front were smashed, your reputation was tarnished and visitors stopped coming. This is why website security is so important.

In addition, people are still wary about doing business online. Trust and security should be core parts of your website strategy alongside design, hosting, SEO and marketing. Yet, companies often don't pay enough attention to these factors with potentially disastrous consequences.

This white paper lists six threats to your website and what you can do to prevent them.

1. Website malware

Website servers can be attacked by malware just like desktop PCs. Compromising legitimate websites and using them to infect visitors is an increasingly popular tactic for online criminals: in 2012, Symantec saw a three-fold increase in this type of web attack[1].

What's worse is that site owners often don't know that their site has been compromised until it is blacklisted by search engines or customers start complaining about infections they picked up on the site. The damage to your traffic and your customers' trust can be huge.

Criminals can buy ready-made malware, such as the popular Sakura toolkit, which they install on someone else's website. It scans visitors' computers for known vulnerabilities and picks the most effective exploit to infect them[2].

[1] Symantec ISTR 18

[2] Symantec Attack Signatures: Sakura Exploit Toolkit
http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=25761

Online advertisement for a malware toolkit

But how do the criminals break into the website in the first place? Again there are toolkits and documentation that make it easy to spot and exploit vulnerable systems. For example, the LizaMoon toolkit used a SQL injection technique to infect millions of websites[3].

Other techniques exploit vulnerabilities in content management systems, website hosting software or server operating systems.

Recommendations:

- Keep your website server software up to date with the very latest patches and security updates.
- Control access to key systems and use strong passwords or two-factor authentication.
- Get daily Anti-Malware Website Scans and Vulnerability Assessment with Symantec's Secure Site Pro, Secure Site EV, and Secure Site Pro EV SSL Certificates.

2. Malvertising

Criminals can also sneak malware infections onto legitimate ad-funded sites using malicious advertising or 'malvertising'. Last year, more than 10 billion ad impressions were compromised in this way[4].

This form of attack is insidious because the website owner often has little control over which ads are served on their site or where they come from, and conventional site scanning may miss an infected ad if it's not visible during the scan. Criminals can actually buy ad space using commercial ad networks or they can subvert or hack existing adverts to inject their infections.

Just accessing the page with a corrupt ad on is enough to risk an infection; people don't actually need to click on the ad to activate it. Without good anti-malware protection on their PC, they run the risk of a silent infection. But if the infection is detected, they may (reasonably) think that the site that triggered it is dangerous and they will definitely think less of the company behind that site.

Recommendations:

- Use reputable advertising networks.
- Where possible, limit adverts' ability to run code (e.g. use static images or plain text).
- Consider Symantec AdVantage, a cloud-hosted security tool designed to block malvertising with real-time monitoring and the ability to trace malware back to its source.

[3] CNNMoney: LizaMoon attack infects millions of websites: http://money.cnn.com/2011/04/01/technology/lizamoon/index.htm

[4] Online Trust Alliance, accessed 12 March 2013, https://otalliance.org/resources/malvertising.html

3. Search engine blacklisting

Search engines such as Google and Bing scan websites for malware and, if they find any on your site, your site could be blacklisted. This means that they stop listing the site, stop sending traffic to it and, depending on a visitor's browser, they may also display a warning about the infection before the visitor goes to your site, even if they enter the address directly.

Blacklisting could have a devastating effect on your site traffic and your brand reputation, undermining a lot of expensive search engine optimisation. Even if you rectify the problem, it can take time for search engines to reinstate your site.

The other reason for a search engine to blacklist your site is if you break their guidelines (or in an attempt to 'play' their system for a higher position in search results. Google publishes helpful guidelines about good and bad practices, including details of behaviour that will get you blacklisted[5].

Google is reported to block 6,000 sites a day[6]. Even big names like TechCrunch and the New York Times have been blacklisted because they were found to be inadvertently running infected ads [7].

Recommendations:

- Protect your site against malvertising and malware (see previous sections).
- Avoid dubious search engine optimisation techniques.
- Sign up for Google and Bing webmaster tools to get email warnings if your site is blacklisted.

4. Security warnings and expired certificates

Imagine that you're a consumer and you're ready to buy something but as you click on the checkout button, your browser gives you a security warning because of an out of date SSL certificate. The odds that you will complete the transaction now are pretty low. Indeed, you'd think twice about coming back to the site in future. Similarly, if you use SSL certificates to protect online applications and services and they expire, user confidence in your service will take a nosedive.

TheVerge.com

[5] Google Webmaster Guidelines: http://support.google.com/webmasters/bin/answer.py?hl=en&answer=35769

[6] http://mobile.businessweek.com/articles/2012-05-07/protect-your-companys-website-from-malware

[7] 'Google Flags Ad Network Isocket for Alleged Malware; chrome blocks TechCrunch, Cult of Mac, others (Updated)', The Next Web, accessed 12 March 2013, http://thenextweb.com/google/2013/01/15/google-flags-ad-network-isocket-for-alleged-malware-chrome-blocks-techcrunch-cult-of-mac-others/

Consequences of Unexpected SSL Expirations and Browser Warnings

Companies with more than a handful of certificates and servers face a serious management challenge. Who is responsible for buying and renewing certificates? How are records kept? How do you prevent 'rogue' purchasing? How do you manage the processes to ensure that certificates are renewed in good time?

Centralising certificate management is not only good practice but it is also essential if you want to avoid accidental expiries or last-minute rush renewals.

- Audit your certificates across the whole organisation so you know what you have, who supplies them and when they expire.
- Consolidate certificates under a single management umbrella.
- Symantec® Managed PKI for SSL gives you a cloud-hosted certificate discovery and management toolkit. (It also includes daily malware scans of your public-facing sites.)
- Set up alerts and diary notes to remind you in good time before certificates expire. Symantec will also give you a named account manager who will help you with all of these processes.

5. Brand impersonation (phishing)

Criminals use well-known names and brands to trick people into disclosing confidential information or installing malware. Often, they use fake websites to fool people. The best-known example of this kind of attack, known as ‘phishing’, is when a fraudster uses a fake bank site to lure customers into revealing bank or credit card details and passwords.

A more recent development has seen scammers use social media to lure people to fake websites where they disclose information, such as social media website passwords, in the hope of some reward such as free vouchers or a free phone.

Typical social media scam

Fake website with bogus survey

Fake websites and brand hijacking make it essential for reputable companies to protect and highlight the authenticity of their real sites. Extended Validation SSL certificates display a green background and the name of the company on the address bar to confirm the true identity of the site. The extended validation and authentication process includes detailed checks into the ownership of the site, making it harder to fake.

Many leading companies, including Twitter and Facebook, demonstrate that their sites are secure by implementing SSL from login to logoff (this is also known as Always-on SSL). This means that every page on the site is encrypted, not just check-out pages and other pages where people enter sensitive information. The benefit of Always-on SSL is that the reassurance that comes with an Extended Validation certificate is always on display meaning that customers can trust a site from the very first click.

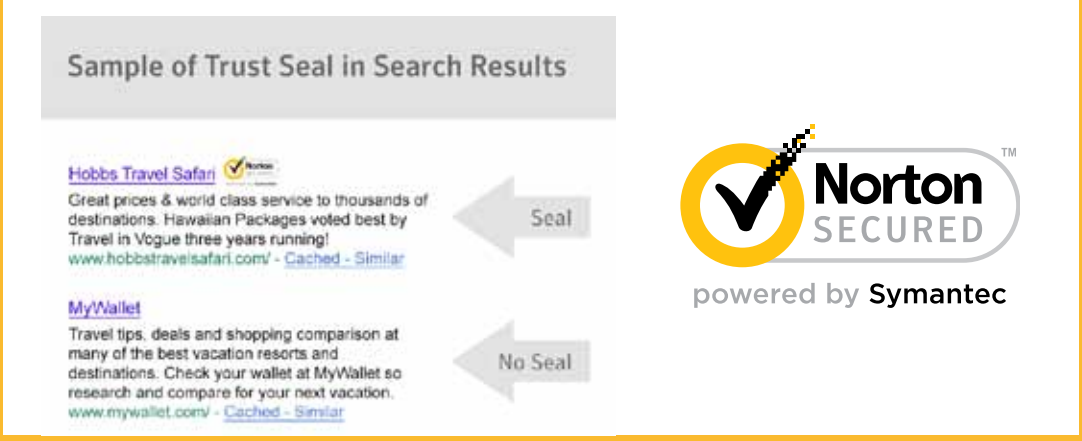
Recommendations

- Use Extended Validation (EV) SSL Certificates to authenticate your site and reassure customers that they are not using a phishing site.
- Consider implementing Always-on SSL using Symantec Secure Site with EV SSL Certificates which provides a clearly visible reassurance that a user's interaction with your site is secure and encrypted.

6. Customer security concerns

With so much criminality and so many security concerns, it's not surprising that people are wary when using websites and look for reassurance that they are safe. In addition, there is a lot of competition for your visitors' attention. There are 634 million websites[8] and people evaluate websites very quickly: the average page visit lasts a little less than a minute[9] and the first ten seconds are critical. So, providing visible reassurance is very important.

Trust marks, such as the Norton™ Secured Seal show people that you take security seriously. They also demonstrate that your site is scanned regularly for malware and other vulnerabilities. This reassurance means that 94% of respondents in a recent survey were more likely to continue an online purchase when they saw it[10].



Confidence begins before a visitor even reaches your site. Of course not being blacklisted by a search engine is essential but Symantec Seal-in-Search™ gives people visible proof that your site is safe in the results page of a search engine. Like the Norton Secured Seal, Symantec Seal-in-Search™ is included with all Symantec SSL certificates

Recommendation

- Display visible signs that your site is secure, scanned and trustworthy, both on the site and, if possible, in search engines.

[8] Netcraft December 2012 Web Server Survey: http://news.netcraft.com/archives/2012/12/04/december-2012-web-server-survey.html.

[9] Jakob Nielsen's Alertbox: How Long do users stay on web pages, September 12, 2011: http://www.nngroup.com/articles/how-long-do-users-stay-on-web-pages/.

[10] Symantec U.S. Online Consumer Study, February 2011.

Choose the right partner

With so much at stake, it has never been more important to choose a well-known, reputable security partner. Symantec already secures more than one million web servers worldwide[11]. It takes a holistic view of your website's security that goes beyond SSL certificates to embrace encryption, certificate management, malware and vulnerability scanning, trust marks and more. It sets high standards for its own security, for example with KPMG-audited authentication processes and military-grade data centers for its SSL infrastructure. If you're looking for trust, security and confidence for your website, Symantec is the right partner.

[11] Includes Symantec subsidiaries, affiliates, and resellers.