

Compromised Websites
An Owner's Perspective
February 2012



Compromised Websites: An Owner's Perspective

Overview

Compromised (stolen or hacked) websites continue to be an attractive target for cybercriminals who benefit primarily from the misuse of reputable domains. Cybercriminals are also able to make use of resources like processing power, bandwidth, and the hosting available via compromised web servers.

In order to better understand the compromise process, illicit usage, and recovery of hacked websites, StopBadware and Commtouch surveyed over 600 website owners and administrators whose sites had been compromised. This document reviews the survey and its results, and includes tips to help website owners prevent their sites from being hacked or compromised.

Commtouch provides a range of email security, Web filtering and antivirus solutions to protect end-users, enterprises and service providers from badware. StopBadware works to educate and assist webmasters to prevent their sites from being hacked and to restore infected sites to normal operation.

Introduction

COMPROMISED WEBSITES: A VALUABLE PRIZE

Most current Internet security suites include tools for Web security. These usually depend on databases of sites known to contain malware, phishing or spam products. These databases also contain known clean sites as well as reputation mechanisms that allow the rating of unknown sites. Compromising a known clean site therefore gives a cybercriminal a platform to perpetrate any number of activities with the reassurance that the site is less likely to be blocked by Web security software.

In addition, the hacker gets free hosting and all the associated resources, such as bandwidth and computing power. For these reasons, a compromised site is a useful tool for criminals who propagate badware. Malicious actors frequently work hard to find exploits that allow hundreds or thousands of sites running the same software to be compromised simultaneously.

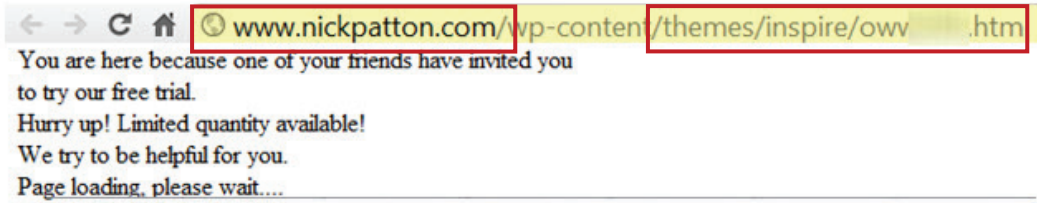
EXAMPLE: REDIRECTION VIA COMPROMISED SITE

In a recent spam outbreak, compromised sites were used extensively to redirect users to the destination URL selling "enhancers" (products that promise to increase sexual performance). Once a site was compromised, a simple HTML file was placed in the "themes" directory, and this URL was emailed to millions of addresses. The HTML file included simple redirect code and a plain message. The homepage of one of these sites is shown below. In this case, the site continued to function normally and there

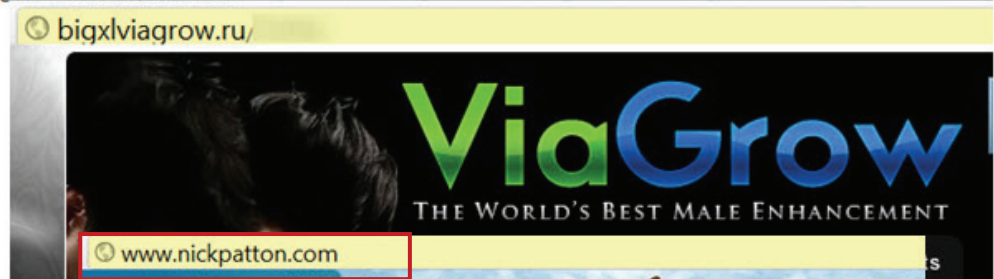
Compromised Websites: An Owner's Perspective

was no immediate indication to the website owner that the site was assisting in the distribution of spam advertising.

Compromised site with redirect code and message hidden in "themes" folder



Destination site selling "enhancers"



Fully functional Homepage of compromised site



Source: Commtouch

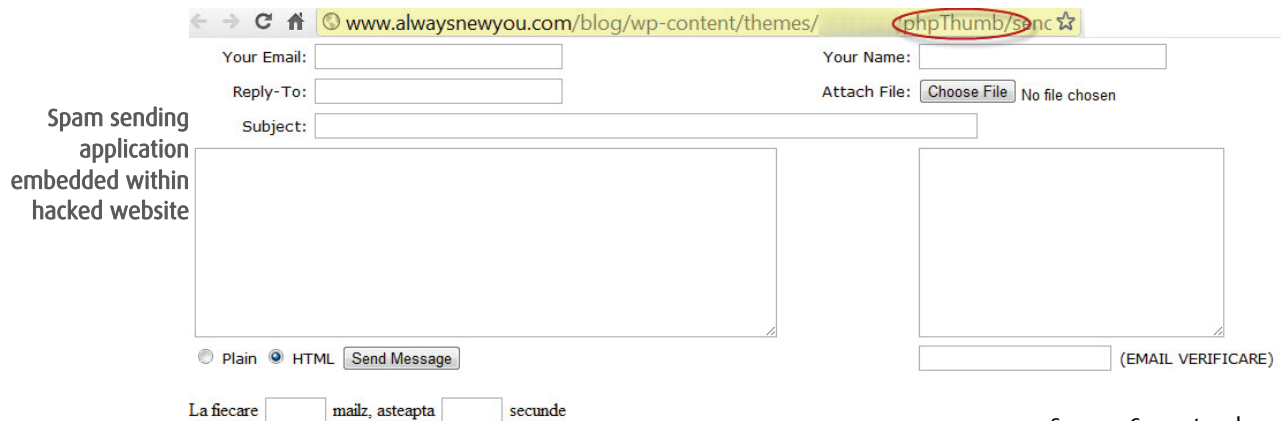
EXAMPLE: EXPLOITING AN IMAGE MANAGER

Thousands of sites use a script called "phpThumb" to manage the images on their webpages. The script allows page designers to fix image sizes, add watermarks and perform other image-related actions when pages are generated. phpThumb also includes a vulnerability (already documented over 5 years ago) that allows attackers to run any code they wish on the target website.

In one attack, masses of spam and phishing emails were sent from sites that were hacked using the phpThumb vulnerability. The attackers installed an email-sending application on the web server – usually in the phpThumb directory. The inserted code (sendme.php) provides a neat and easy-to-use spam/phishing sending application, as shown below. The sites continued to function normally.

As with other such compromises, the good reputation of the domain is abused in this way to send spam and phishing emails.

Compromised Websites: An Owner's Perspective



Surveying compromised websites

The continued use of compromised websites, as illustrated in the examples above, raises several questions:

- What website software is targeted?
- How are the websites compromised?
- What are the compromised websites used for?
- How do website owners become aware of the compromise?
- How do website owners regain control of their sites?
- Did the hosting providers assist affected website owners?
- How did the experience change website owners' attitudes toward their hosting providers?

"This has happened once before and I think it is due to not changing the FTP password often enough."

Website Owner

To better understand these issues, Commtouch and StopBadware initiated a public survey of website owners whose sites had been compromised. The survey was publicized on LinkedIn, Twitter, Facebook, the StopBadware website and blog, StopBadware's community forum, StopBadware emails to website owners who had requested independent review of their sites, and the Commtouch Blog. The results presented below summarize over 600 responses received between November 2011 and January 2012.

COMMENTS

Respondents to the survey were eager to expand on their experiences – many of the comments are displayed throughout the report.

"My websites keep getting compromised even though I am diligent about staying on the latest version of my products. My hosting provider keeps telling me this is not their problem. Is this normal?"

Website Owner

Compromised Websites: An Owner's Perspective

WHICH WEBSITE SOFTWARE IS TARGETED?

Do website hackers target specific website software? Is there a particular Content Management System (CMS) that is more vulnerable than others? The answers received seem to identify WordPress (28%) as a strong favorite for cybercriminals. On the other hand, WordPress is the most commonly used CMS, so statistically it was expected to feature prominently. In addition, WordPress has an extensive plugin culture – and in many cases, security flaws within these plugins are the attack vectors in site compromises.

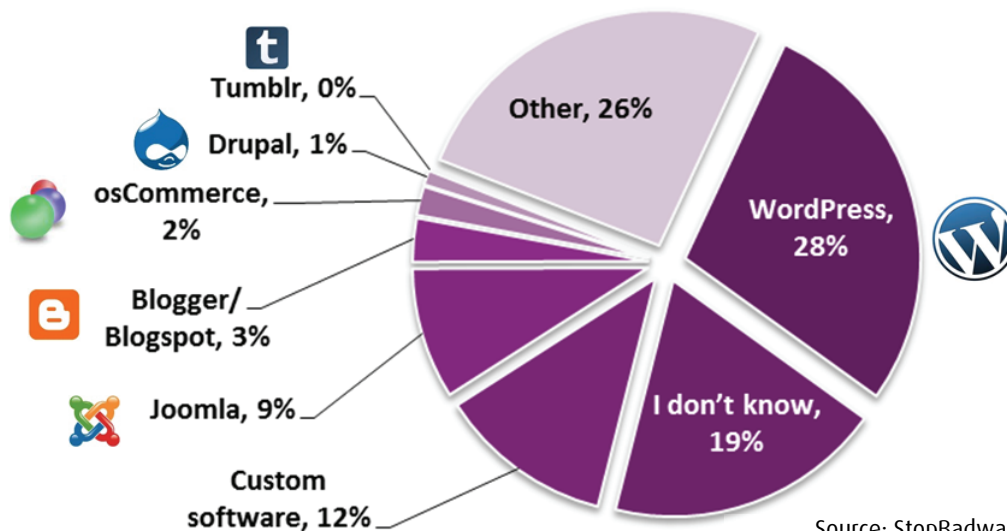
Respondents who listed “Other” described their use of: numerous proprietary systems, ZenPhoto, vBulletin, and Movable Type (predecessor of WordPress). Notably, nearly 20% of respondents didn't know what CMS was used in their websites.

“My problem seemed to be caused by a rogue WordPress plugin. I contacted the author of the plugin but he refused to believe that his plugin was the problem - even though his own website was also hacked in the same way!”

Website Owner

Which software do you use to run your website?

- WordPress
- I don't know
- Custom software
- Joomla
- Blogger/ Blogspot
- osCommerce
- Drupal
- Tumblr
- Other



Source: StopBadware, Commtouch

Correlating the percentages in the pie chart with CMS penetration data from w3techs.com paints WordPress in a better light. Although WordPress represents 54% of known CMSs, it only featured in 28% of the hacks. Joomla, Blogspot and osCommerce on the other hand show direct correlations to their installed base.

Compromised Websites: An Owner's Perspective

HOW ARE WEBSITES COMPROMISED?

Malicious hackers are a devious bunch – always looking for new flaws, exploits and social engineering tricks that will allow them to compromise a website. With this in mind, it comes as no surprise that most website owners (63%) simply don't know how their sites were compromised.

20% of respondents admitted that their failure to update website software and/or plugins had likely left them open to attack. Those who chose more than one option in their responses most commonly combined stolen credentials with recent public computer or WiFi access – so the blog update from the library PC or airport lounge may have been to blame.

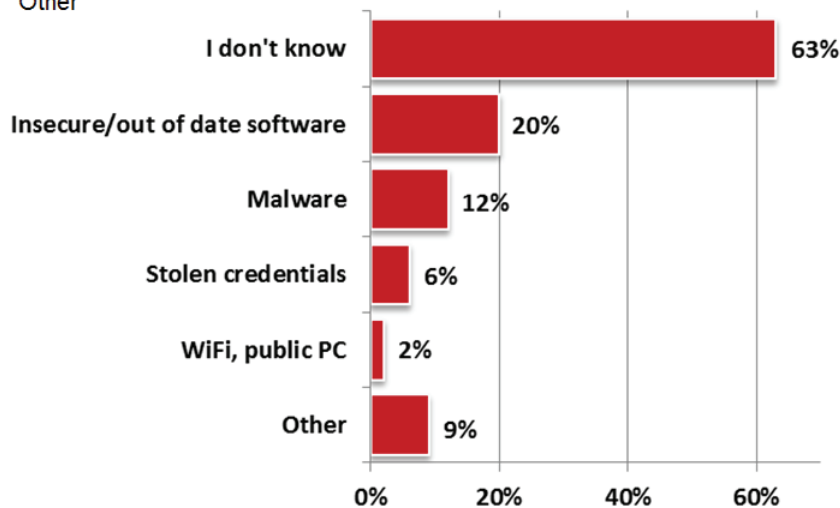
Some website owners who responded "other" were convinced that their site had been compromised as part of an attack on the entire shared server where the site was hosted.

"I am running a business, where Internet presence is at its utmost importance. I have ignored the need to update to the latest security patch....and surely paid the price."

Website Owner

How was your site compromised? (more than one response allowed)

- I don't know
- Hackers exploited out of date or insecure software on my site
- A computer that is used to update the website was infected with a computer virus or other malware
- My credentials (username/password) or those of a colleague were used to access the site
- I used a public computer or public WiFi network to make changes to the site or post a blog (e.g.: Internet café)
- Other



Source: StopBadware, Commtouch

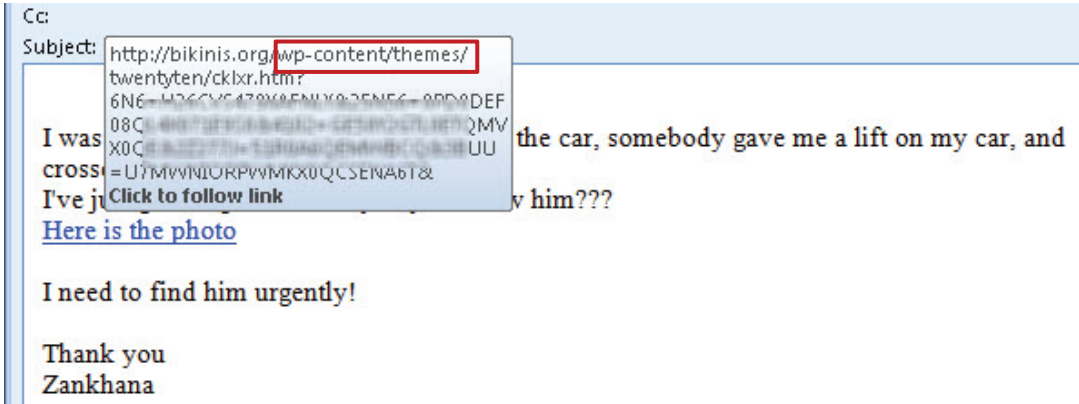
Compromised Websites: An Owner's Perspective

WHAT ARE THE COMPROMISED WEBSITES USED FOR?

As described in the introduction, the compromised website provides a useful platform for a range of illicit activities. These activities include:

- Hosting malware – this may take the form of complex scripts that infect any visiting PC. Alternatively, well-crafted emails may have convinced a recipient to download a malware file that is hosted on the compromised site. In the example below, the malware script is hidden in a WordPress themes subdirectory.

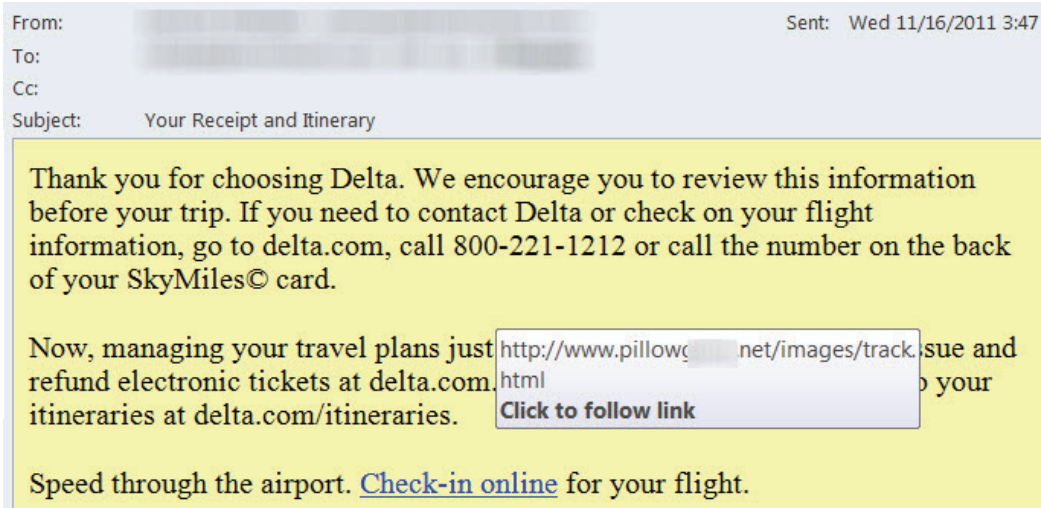
Phony distress email with a link to malware hidden in the themes directory of "bikinis.org"



The screenshot shows an email header with the subject line: `http://bikinis.org/wp-content/themes/twentyten/cklxr.htm?6N6-H26CVF472V8FNUY83EN5C-8DD0DEF08C-887283088810-6E8D0C718E72MVX0C8-822770-138040CEW4B10838UU=U7MVVNIORPVMKX0QCSENA6T&`. A red box highlights the path `wp-content/themes/`. The email body contains the text: "I was crossed by him???", "I've just seen a photo of the car, somebody gave me a lift on my car, and here is the photo", and "I need to find him urgently!". The sender is identified as "Thank you Zankhana".

- URL redirect – thousands of compromised sites may perform simple redirects to a few "master" URLs. This is accomplished with a few lines of HTML code hidden in the compromised site, forcing the site to act as a "front door" to the badware. The master URLs contain spam product pages or malware. In the example below, "track.html" includes a redirect to the malicious destination URL.

Phony airline itinerary email with a link to a compromised site. The file "track.html" redirects to a site hosting malware



The screenshot shows an email header with the subject line: "Your Receipt and Itinerary". The email body contains the text: "Thank you for choosing Delta. We encourage you to review this information before your trip. If you need to contact Delta or check on your flight information, go to delta.com, call 800-221-1212 or call the number on the back of your SkyMiles© card." and "Now, managing your travel plans just got easier. You can now issue and refund electronic tickets at delta.com, check in for your itineraries at delta.com/itineraries." A blue box highlights the URL `http://www.pillowtalk.com/images/track.html`. The email also includes the text: "Speed through the airport. Check-in online for your flight."

- Hosting phishing, spam pages, pornography – one or two static pages on the compromised site may advertise spam products (pharmaceuticals, replicas, enhancers, etc.), act as phishing pages for banks, PayPal, Gmail, etc., or offer explicit (sometimes illegal) content.

Compromised Websites: An Owner's Perspective

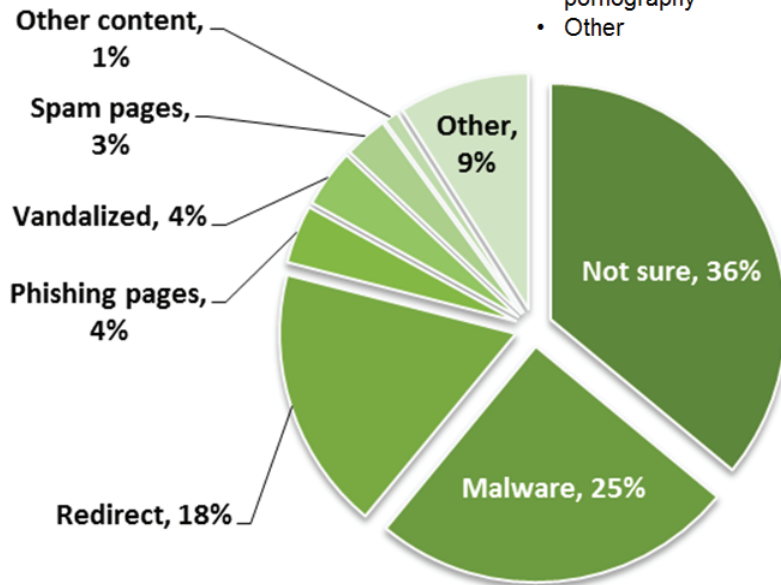
- Vandalism – the aim of the compromise might be to embarrass the site owner or, alternatively, to make some political point – generally known as “hacktivism.” Some respondents reported vandalism by their competitors.
- Other content or activity – some fairly complex forms of site misuse have been recorded. The spam-sending script described in the introduction is one example.

“My site was attacked by my competitor in the same field.”
Website Owner

The results of the survey reveal that many website owners (36%) who became aware of a compromise did not know what their site was (mis)used for. The remaining 64% observed the complete range of activities described above; the largest group (25%) believed their sites were used to host malware. Other responses indicated that compromised sites were used to redirect to malicious URLs, spread malware to other legitimate websites, and host links for SEO poisoning purposes.

How was your site used after it was compromised?

- Not sure - I was just told it was compromised
- Used to host or deliver malware
- Used to redirect to another site
- Used to host phishing pages
- Pages on the site were vandalized
- Used to host spam-product pages (e.g.; online pharmacy)
- Used to host other content such as pornography
- Other



Source: StopBadware, Commtouch

Compromised Websites: An Owner's Perspective

HOW DO WEBSITE OWNERS BECOME AWARE OF THE COMPROMISE?

In rare cases of site vandalism, the malicious actors make it plainly obvious to the site owner (and the rest of the world) that the site has been compromised (see example below).

Vandalized website



Source: Commtouch

In most cases, though, attackers need the resources and reputation of the site to do their dirty work and therefore do not make the compromise obvious. So how are website owners to know that there is a problem? It turns out that in nearly half of the cases, owners were alerted by a browser, search engine or other warning when they tried to visit their own sites. A sample screen from Google's Chrome browser is shown below.

Google Chrome warning message



Source: Commtouch

Alternatively, colleagues, friends, web hosting providers, or security organizations (such as StopBadware) let the owner know there was something amiss. This group collectively accounts for 35% of the notifications, but may in fact be larger. Of the

Compromised Websites: An Owner's Perspective

10% of respondents who answered "other," many indicated that they too were informed by a third party.

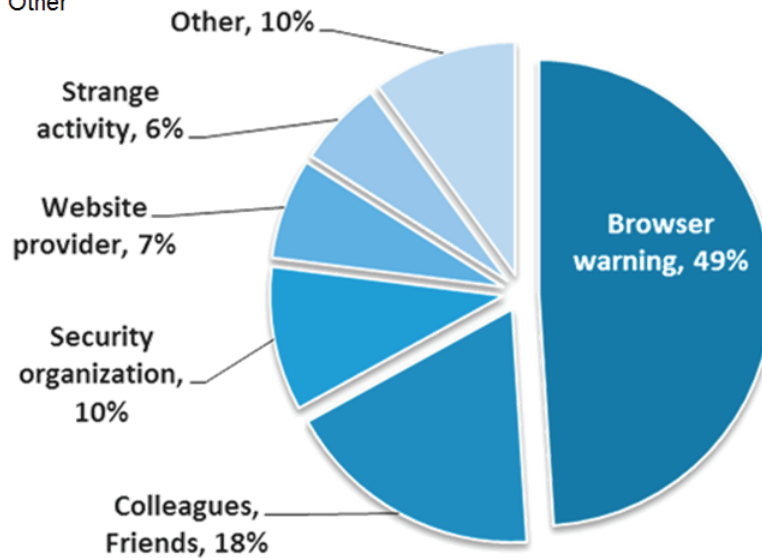
Notably, only 6% of website owners were able to detect an issue based on strange or increased activity within their sites. This statistic reinforces the theory that malicious actors try to keep compromises under the radar. The longer a compromise goes unnoticed, the longer a bad actor is able to use a legitimate site for nefarious purposes. A further small percentage of site owners became aware of the problem after being locked out of some Web services or waking up to vandalized sites.

"Finding a way to lift a [warning] from Google is not straightforward."

Website Owner

How were you made aware of the compromise ?

- I saw a warning while trying to visit my website (e.g. "This site may harm your computer" or "Reported attack site")
- Colleagues, friends, or website visitors told me
- Notified by a security company/organization
- Notified by my website provider/Web hosting company
- I noticed strange activity or increased activity on my site.
- Other



Source: StopBadware, Commtouch

HOW DO WEBSITE OWNERS REGAIN CONTROL OF THEIR SITES?

Having established that their sites have been compromised, website owners chose various corrective courses of action. 46% of respondents fixed the compromise themselves after consulting various online resources.

A further 13% of the "other" respondents also resolved the issue on their own by restoring from backups, reinstalling the compromised plugin, or deleting the malicious files and scripts manually. Overall, 58% of respondents claim to have successfully resolved a site compromise using publicly available resources and their own skills.

"I feel so helpless and don't know/understand how to prevent this from happening again!"

Website Owner

Compromised Websites: An Owner's Perspective

Over a quarter of the website owners who responded still faced a compromised site; Less than 0.5% of these had approached a security provider, IT expert, or their web hosting provider. 8% of those who responded "other" were either unsure of what to do next or had not taken any action, indicating that their sites were also still compromised. Results seem to indicate that failure to seek help contributed to the persistence of site compromise.

Surprisingly, 5% of respondents chose to do nothing and believed that the problem had been resolved. Some responded to the news of their compromised site by taking the survey.

"The process of getting back online is onerous and not helpful. [Google] needs to be much more proactive in helping us [webmasters], not just "protecting our users." Who are we, chopped liver?!"

Website Owner

What action did you take/ are you taking to fix the compromised site?

(more than one response allowed)

- Read through some forums and help websites and removed the problem myself
- I've tried several approaches, but my site is still compromised
- Followed instructions received from a security company/organization to fix the problem
- My website provider/hosting company cleaned it up for me
- Called in a security expert/IT company/web developer to sort it out
- Nothing - it seems to be OK now
- Abandoned the whole thing – set up a new site with a new provider
- Other



Source: StopBadware, Commtouch

Compromised Websites: An Owner's Perspective

DID THE HOSTING PROVIDERS ASSIST AFFECTED WEBSITE OWNERS?

As stated previously, most website owners (58%) chose to resolve the problem themselves. Clearly some of these had no choice, since 19% of respondents were refused help or didn't receive any response from their hosting provider.

Of those who did request help, 60% received free assistance, 33% received no assistance and 7% had to pay to get their compromised site repaired.

8% of those who responded to the survey did not provide an answer to this question.

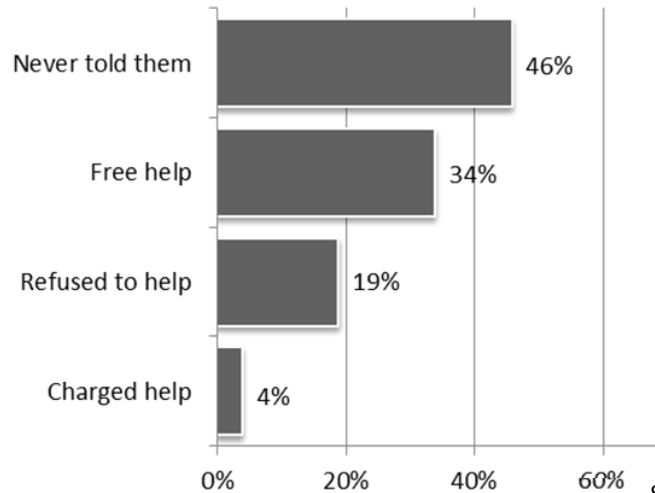
"I feel that [my hosting provider] handled this well....I was just being lazy - I hadn't updated the password to a new one that included numbers and characters. This just brought home the need for vigilance."

Website Owner

What role, if any, did your website provider/web hosting company play in resolving the compromise?

(more than one response allowed)

- None. I never communicated with them about this
- They provided free assistance to help fix the compromised site
- None. They refused to help fix the compromised site or didn't respond to my request
- They charged me extra to help fix the compromised site



Source: StopBadware, Commtouch

HOW DID THE EXPERIENCE CHANGE THE ATTITUDE OF WEBSITE OWNERS TOWARD THEIR HOSTING PROVIDERS?

Forty percent of survey respondents changed their opinion of their web hosting providers following the experience of a hacked site. The default association seems to be negative, as 58 respondents (nearly 10%) indicated they are thinking about leaving their providers even though they had no interaction with the providers during the experience.

That said, it is clear that a hosting provider's approach to supporting victims of website compromise affects customers' perception. Webmasters were three times as likely to consider leaving providers that charged extra or refused to provide

"I changed hosts because they basically said 'Run virus protection. You're on your own.'"

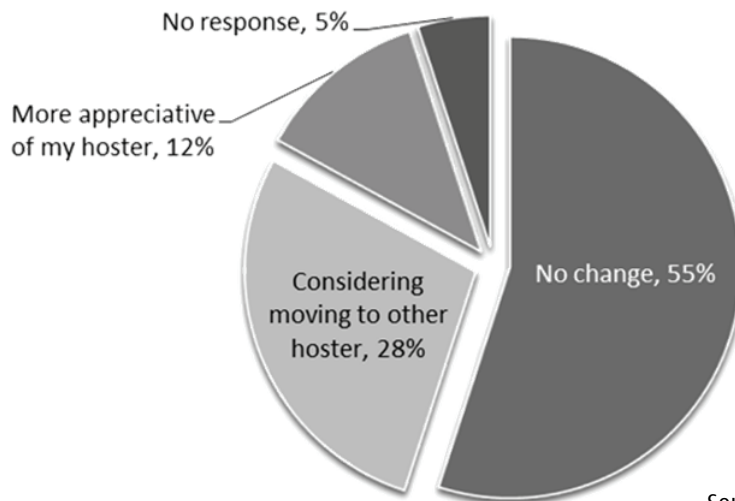
Website Owner

Compromised Websites: An Owner's Perspective

support for remediation than those that offered free support. And, conversely, site owners were five times as likely to say they were more appreciative of providers that offered free assistance than of those that charged or provided no support.

Did this experience change your opinion of your website provider/web hosting company?

- No
- Yes, I am considering moving to a new provider because of this experience
- Yes, I am more appreciative of my current provider



Source: StopBadware, Commtouch

Preventing compromised Websites

Many website owners who responded to this survey seemed to be unaware that their websites could be compromised and unsure of how they might clean up their sites and keep them secure. Even so, 40% of survey respondents believed their websites were infected through software vulnerabilities, stolen credentials, and/or via an infected machine. These are all common attack vectors; risk of compromise can be reduced by following these basic tips:

- Keep software and all plug-ins updated. Whether you run popular content management software (e.g., WordPress, Joomla, Blogger) or custom software, make sure that software and all third party plug-ins or extensions are updated. Remove plug-ins or other add-ons that aren't in use.
- Use strong, varied passwords. WordPress login credentials, for example, should be different from FTP credentials. Never store passwords on your local machine.
- Regularly scan your PC for malware.
- Use appropriate file permissions on your web server.

"I'm still not confident in [the] security of my website. This has happened before, and the hosting provider says it's up to me to keep it secure....I'm not sure how to keep it secure."

Website Owner

Compromised Websites: An Owner's Perspective

- Research your options and make security a priority when choosing a web hosting provider. If you aren't confident you can protect your site on your own, consider using an add-on security service from your hosting provider or a third party website security service.

StopBadware, along with a great many security companies and organizations, offers free educational and community resources for website owners looking to prevent or clean up compromised websites. For more information on cleaning and securing your website, visit www.stopbadware.org/home/security or <https://badwarebusters.org>.

Conclusions

Legitimate websites are a valuable prize for cybercriminals, and the abuse of these sites affects both their owners and the greater security ecosystem. The survey, though not scientific, highlights some important themes in the experience of the victims of website hacking.

First, many consumer and small business site owners lack awareness of the threat to their sites and how to get assistance once their sites have been compromised. One opportunity to provide awareness and to direct owners toward resources comes in the form of browser and search engine warnings, which are the prevalent means by which owners learn their sites have been hacked. This fact also highlights the need for improved methods of notifying site owners proactively when hacking is detected on their sites.

Web hosting providers, too, play a role in awareness and remediation, particularly given site owners' tendency to seek assistance from their providers following a compromise. Site owners show a willingness to leave their hosting providers after negative incidents, and they demonstrate an increase in loyalty after especially positive experiences. This indicates that hosting providers have an opportunity to strengthen their brand reputations—and support the security of the ecosystem—through their efforts to educate, support, and protect their customers.

Finally, the diversity of platforms hosting compromised sites, and the variety of methods by which they were compromised, demonstrate the opportunistic nature of cybercriminals. Website owners, hosting providers, security organizations, and other parties will have to work individually and together to create an equally diverse set of innovative solutions to combat the threat of compromised websites.

Compromised Websites: An Owner's Perspective

About StopBadware

StopBadware makes the Web safer through the prevention, mitigation, and remediation of badware websites. It began as a project of the Berkman Center for Internet & Society at Harvard University before spinning off as a standalone nonprofit organization in 2010. Corporate partners include Google, PayPal, Mozilla, Verizon, and Qualys. StopBadware is based in Cambridge, Mass. For more information, visit www.stopbadware.org.



About Commtouch

Commtouch® (NASDAQ: CTCH) safeguards the world's leading security companies and service providers with cloud-based Internet security services. Real-time threat intelligence from Commtouch's GlobalView™ Cloud powers its Web filtering, email security and antivirus solutions, protecting thousands of organizations and hundreds of millions of users worldwide.



- Visit us: www.commtouch.com and blog.commtouch.com.
- Email us: info@commtouch.com.
- Call us: 650 864 2000 (US) or +972 9 863 6888 (International)

REFERENCE:

http://w3techs.com/technologies/overview/content_management/all