Dasient

Drive-by-Downloads, Web Malware Threats, and Protecting Your Website and Your Users

Discover the 5 most critical malware attacks hurting businesses, and ways to defend your website against them

SHIFT IN HOW MALWARE IS SPREAD

The rise in advanced Web-based technologies has created vast new opportunities for collaboration and interactivity. Just a few years ago, blogging was a niche application, and "user generated content" and "mash-ups" were not in our vocabulary. Modern websites have enormous interactivity and often combine "best of breed" software and content to create a rich user experience. A single website may now be sourcing in ads from a third-party network; using third-party "widgets" to provide user functionality (such as polls or the ability to share with friends); and accepting user submitted comments, photos and videos. As the web offers more and more functionality and rich user experiences, there is an overall trend of applications moving from the desktop to the Web (through software as a service model).

The emergence of interactive, dynamic web applications, as well as the tendency of websites to combine "best of breed" software and content, has enormous implications on web security. Attackers are now targeting the medium where users spend the majority of their time—namely, websites and web applications, rather than traditional email and desktop applications—to propagate viruses and malware. Attackers take advantage of the interactivity, interconnectedness, and interoperability of the web to exploit "structural vulnerabilities" to increase the footprint and effectiveness of their attacks. One of the favorite attack methods of hackers over the last few years has been to distribute malware from legitimate websites. In these attacks, the hackers will compromise a legitimate website and silently place a piece of malicious code that is presented to all visitors of the website. Unsuspecting users will have a virus downloaded to their personal computer by visiting an infected web page. Sometimes, the virus is downloaded without any user interaction ("drive by download"); in other cases, the user is prompted to click a button ("social engineering malware") or to download what appears to be legitimate file ("dangerous download"), and then receives a virus. Given the enormous growth in malware attacks, users who interact on the web to extend business opportunities and the social boundaries of their lives are therefore at great risk. And businesses who depend on their website for customers, sales, and brand are also at great risk of loss from the emergence of malware attacks.

To provide a sense of the scale and scope of malware attacks on websites, consider the following statistics:

- Every 1.3 seconds a new web page is getting infected
- As of Q3 2009, every month almost 2,000,000 web pages across more than 210,000 websites are infected with Malware. This is almost double the number of web pages reported for Q4 2008 [1].
- 77% of Web sites with malicious code are legitimate sites that have been compromised [2]
- The number of malicious sites has grown 671% from 2008-2009
- 57% of data-stealing attacks are conducted over the Web

FIGURE 1: EMAILS WITH INFECTED ATTACHMENTS, 2005-2008

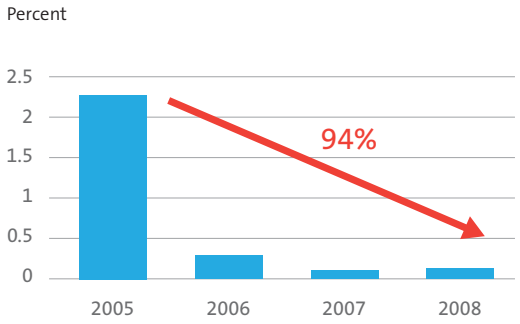
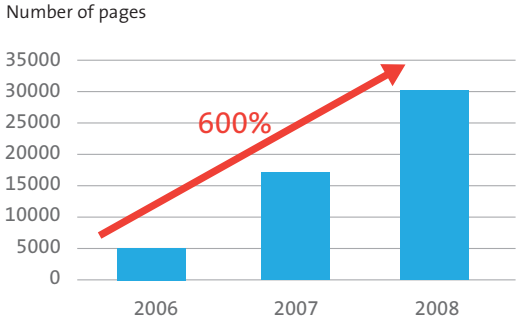


FIGURE 2: MALWARE-INFECTED WEB PAGES DISCOVERED EACH DAY



[1] Microsoft Security Intelligence Report, April 2009

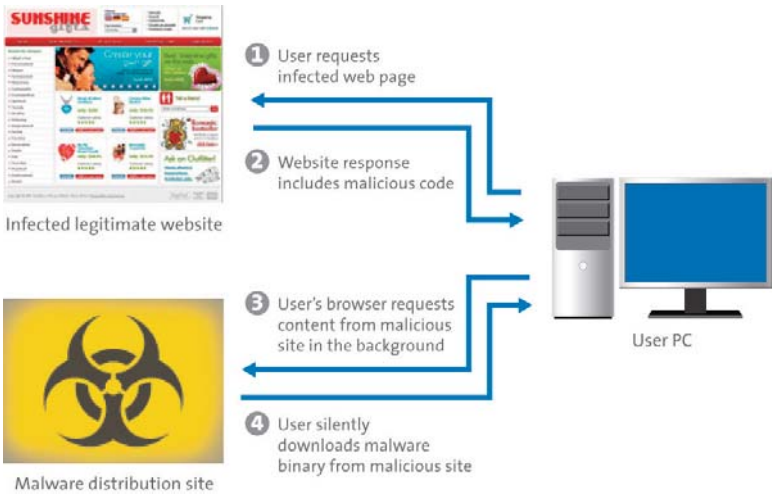
[2] Websense State of Internet Security, Q1-Q2 2009

AUTOMATION OF ATTACKS

So, why are Websites being targeted for malware attacks? The simple answer is that malware attacks on websites are the best way for hackers to distribute viruses. In the past, viruses used to spread via email attachments, or by coaxing users to download and install malicious files. While these attack methods are still being used today, they are being supplemented and in many cases replaced by the preferred method of drive-by-downloads attacks from legitimate websites.

A drive-by-download occurs when a user visits a web page and malicious code is automatically and silently downloaded and installed on the user's computer, without any interaction from the user. Once the virus is on the user's PC, the hackers gain remote access to the computer and can steal sensitive information such as banking passwords, send out spam or install more malicious executables over time.

FIGURE 3: HOW ATTACKERS USE WEBSITE TO DISTRIBUTE MALWARE



STRUCTURAL VULNERABILITIES CREATE OPPORTUNITIES FOR ATTACKS

Over the last few years, awareness of web application vulnerabilities has grown among web security professionals. Attacks such as SQL injections, Cross-Site Request Forgery (CSRF), and Cross-Site Scripting (XSS) exploit web application vulnerabilities to plant malware such as drive-by-downloads on legitimate websites. Theoretically, a website can "fix" or "patch" web application vulnerabilities on a website, assuming that (1) the website is aware of the vulnerability, and (2) the website has the technical capability and resources available to perform the fix. However, in addition to exploiting well-understood web application vulnerabilities in websites, attackers also often exploit so-called "structural vulnerabilities" that cannot be easily fixed or patched. In Q4 2009, for example, several publications discovered structural vulnerabilities created by the origin policies for third-party Flash objects embedded on websites. These types of threats are fundamentally serious because they emerged from third-party content rather than form a software application which can be fixed with a patch. There is no simple remedy for closing this vulnerability. Examples of structural vulnerabilities include:

- Third-party advertisements
- Usage of third-party widgets
- Mash-ups
- User generated content

These vulnerabilities open sites up to a number of potential exploits, not least of which is being turned into a delivery vehicle for malware, wherein a site inadvertently infects some or all of its visitors with malicious software. With web-based companies and website owners sourcing in more and more content and applications from each other and from users, the threat is more tangible than ever. They include enabling user collaboration, sharing content such as comments, links, photos and files as well as employing syndicated ad networks such as Real Simple Syndication (RSS) or mashup. These vulnerabilities are already relatively widespread: For example, 66 percent of the top 500 sites in the US run ads, 47 percent of the top 100 accept user-generated content, and 75 percent of the top 100 newspapers in the US enable user comments. This can in turn trigger losses in traffic, reputation, and revenue, as visitors discover the infections and as the site is evaluated by the search engines, browsers, and AV providers that blacklist dangerous sites. Other than taking drastic measures like abandoning third-party content and ad networks altogether, there is nothing site owners can do to guarantee they will not be exploited.

HOW ATTACKS OCCUR

Hackers are targeting innocent, legitimate websites with drive-by download malware attacks in order to propagate viruses. The drive-by-downloads do not require any user interaction other than loading an infected web page which will in turn pass on the infection to all its visitors with a virus.

THE 5 MOST CRITICAL MALWARE ATTACKS

There are many different ways in which a website can suffer a malware attack. In the following section we cover the 5 most business-critical types of attacks (not presented in any particular order).

Vulnerable Web Applications

One way in which hackers can compromise a website is via attacks against vulnerable web applications running on the site. According to a recent SANS study [3], "Attacks against web applications constitute more than 60% of the total attack attempts observed on the Internet. These vulnerabilities are being exploited widely to convert trusted web sites into malicious websites serving content that contains client-side exploits. Web application vulnerabilities such as SQL injection and Cross-Site Scripting flaws in open-source as well as custom-built applications account for more than 80% of the vulnerabilities being discovered."

In these attacks, the attackers identify websites that are running vulnerable versions of blogging or content management software, shopping cart applications, or discussion forum software. Poor input sanitization or output escaping result in SQL injection or cross-site-scripting (XSS) vulnerabilities in these web applications. The attackers exploit the vulnerabilities in these web applications in order to plant malicious code onto the website. For example, in a SQL injection attack, the hackers send database commands into form fields (like login or comment forms) instead of legitimate user input. The database commands are constructed in a way that they trick the web application into executing the commands and planting malicious code into the database. If the web application calls on the database to generate dynamic web pages (for example, calling the database to generate parts of the header or footer), the malicious code planted in the database could be presented to users, resulting in infections.

When a user visits an infected website they are sent to the malicious site, of course without their knowledge and as if the JavaScript is from the genuine site. The attacker can attempt to exploit the user in the background. The SQL injections continues to live in the database of a website typically until the users make the website aware of the problem, in which case the webmaster can take action to remove it. Removing the malware does not prevent a new SQL injection to attack the site in the future. It is also important to note that attackers can modify the website's content by compromising the underlying web server using specific network or scripting application vulnerabilities.

[3] SANS Top Cybersecurity Risks Sept 2009 (http://www.sans.org/top-cyber-security-risks/)

Stolen Admin Credentials

Rather than using code injection like SQL injections or Cross-site Scripting, attackers can steal FTP credentials to compromise websites. Hackers could get access to the website administrator's PC by infecting the administrator's personal computer with a virus and subsequently could log the user's FTP or admin password for their website. Once the hackers gain access to the user's FTP credentials, they can conduct a wide variety of attacks, such as placing malicious JavaScript or iframes into html or native javascript files on the site; or altering the website's .htaccess file to redirect visitors to a malicious site.

In 2009, for example, the Gumblar virus infected over 80,000 websites with Web-based malware. Gumblar was able to use compromised FTP credentials to allow attackers to gain access to legitimate websites. Once malware was placed on a legitimate website, any visitors of those sites would get infected with a virus. The virus would log the keystrokes of those infected users, in some cases stealing FTP credentials to other websites if the users happen to administer websites from their PC. Thus, a positive feedback loop was created, where Gumblar would infect websites, users would get a virus from visiting those sites, Gumblar would harvest FTP credentials and infect more websites, and the cycle would continue. The security implications resulting from gaining FTP credentials are far more serious than the impact of SQL injections. With SQL injections the hacker uses the vulnerability of a website to attack and in the end gains some access to the website it attacks. As previously mentioned, SQL injection vulnerabilities can theoretically be fixed. However, in case of stolen FTPs, attackers gain webmaster administrative privileges and can plant malicious code at will. There are no traditional vulnerabilities that can be "closed" in this case.

FIGURE 4: EXAMPLE OF MARTUZ ATTACK (VARIANT OF GUMBLAR), WHICH USED STOLEN FTP CREDENTIALS TO ATTACK LEGITIMATE WEBSITES

Malvertisements/ Malicious ads

Malicious ads (also known as "malvertising") are another way for a website to experience a malware attack. Rather than infecting a website directly, malicious banner ads that may look legitimate, can be planted in syndication services that operate through Google, Yahoo! or other third-party ad networks. Once a malicious ad is in an ad network, it can be presented to users on various websites by the ad network simply rotating through its inventory of ads. This is often a difficult attack to detect on a website. Users who visit sites that use syndication services may experience an intermittent or a fast flicker of the flash malware ads which seem harmless. However, the ad often installs a trojan on the infected PCs. Malvertisements often exploit code which target operating systems and application vulnerabilities. Malvertisements can severely impact a website's reputation with its users, as well as with search engines.

FIGURE 5: RECENT HIGH PROFILE MALVERTISING ATTACKS

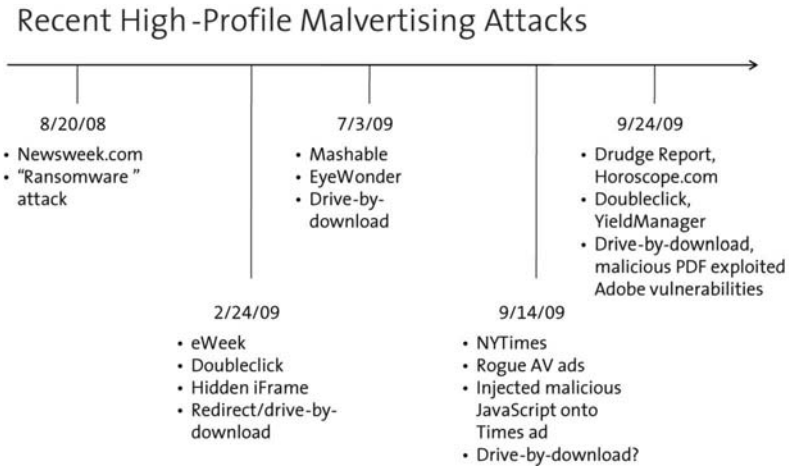
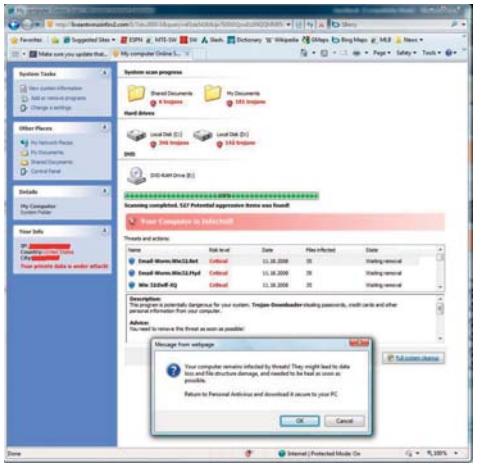


FIGURE 6: SCREEN SHOT OF RANSOMWARE/SCAREWARE ATTACK COMMON WITH MALVERTISING



Third-party widgets

Modern web pages are becoming more complex. In order to offer the best user experiences, as well as to manage the operations of their website, businesses often include widgets from third parties onto their web pages. Examples include the e-commerce payment buttons, poll widgets, social applications (such as reviews), traffic counters, and analytics packages. Any of these third-party widgets could be potential sources of malware infections or mashups.

For example, suppose several thousand websites are all using a particular third-party traffic counter (abctrafficcounter.com). The attackers were able to compromise the third-party that hosts the traffic counter (abctrafficcounter.com) and place malicious code into the widget application itself. Now, all of the several thousand legitimate websites that use abctrafficcounter.com's traffic widget are at risk of infecting all of their own users, since abctrafficcounter.com widget is serving malware.

By compromising a popular "widget maker" website (abctrafficcounter.com) and exploiting the interconnected nature of the web, the attackers have been able to increase the footprint of their attack significantly.

User generated content

User generated content has revolutionized user experience on the web. Unprecedented amounts of interactivity and highly engaging content are now possible.

However, the ability for unknown users to submit comments, links, HTML code, and files (including images, video, and documents) has created opportunities for attackers to abuse websites to propagate malware. One security company found in a recent study that 95% of comments to blogs, chat rooms and message boards are spam or malicious [4].

Attackers can use URL shortening services to mask malicious links that they place on websites. They can also embed malicious scripts in PDF files or images, which they can then upload to legitimate websites. If the web applications being used on a website do not properly sanitize user input, the attackers can even place malicious HTML and javascript code into comment forms on the site. All of these attacks could result in a malware infection on the website, which in turn could result in users of the site contracting a computer virus.

[4] Websense State of Internet Security, Q1-Q2 2009

THE IMPACT

The impact on websites suffering from the above mentioned threats are enormous. If undetected, the website will now infect any visitors with a virus. This can severely damage the website's reputation with its existing and potential customers, as well as create liability issues. For example, visitors to the site may see a warning from their anti-virus software upon loading an infected URL in their browser. Or, the visitor may read news stories, see comments on blogs, or receive Tweets from users reporting malware on a particular legitimate website. These experiences would clearly make existing or potential customers of a website suspicious and reluctant to visit the site that has been attacked.

In addition to the loss of brand, reputation, and customers, websites that suffer malware attacks may also experience liability issues such as data theft. As previously noted, 57% of data-stealing attacks now occur on the web. Any e-commerce, financial services or healthcare website that hosts sensitive user information (such as credit card data, or other

FIGURE 7: FIREFOX MALWARE WARNING
WHEN YOUR SITE GETS ATTACKED, THIS IS WHAT YOUR FIREFOX VISITORS SEE

personally identifiable information [PII]) is at risk for data theft as a result of a Web-based malware attack. Suppose that there is a banking site called ABCBank.com. The website suffers a malware attack and is now serving a drive-by-download from its homepage. Any visitor to ABCBank.com's homepage will be infected with a virus on their PC. This virus logs keystrokes and allows the hackers to steal the user's passwords. Suppose after visiting the homepage, these visitors now enter their login information to check their balances at ABCBank.com. The attackers have successfully harvested the login credentials for ABCBank.com. If the malware attack is undetected, potentially hundreds or even thousands of users can have their ABCBank.com credentials compromised in this way. The attackers have successfully targeted the users of ABCBank.com by inserting the malicious code on the homepage of the bank's website.

The extreme pain point from suffering a malware attack is for the website to get blacklisted.

Search engines, browsers, and security companies now regularly blacklist websites that are found to be serving malware drive-by-downloads. Google, Yahoo!, Firefox, Internet Explorer, Norton, and McAfee all blacklist legitimate sites that have been infected with malware. The blacklisting has an immediate impact on the website's traffic and revenues, as well as heightens the damage to a website's brand and reputation. In June 2009 a survey that was conducted by Dasient, customers whose website had been compromised and subsequently blacklisted expressed their frustration and uncertainties about the impact to their businesses. Dasient's survey revealed amazing facts:

- 39% of the sites were infected and blacklisted multiple times
- 73% of the sites remained blacklisted for more than 1 day
- Almost half of the sites lost at least 40% of their overall traffic while they were blacklisted by a single provider

"The warning from Google stopped a lot of our traffic... The attacks occurred weeks ago, and I'm only now getting back to my normal levels of traffic. We lost thousands of dollars of business in goodwill alone from our customers"

-Owen Taylor, AGFax.com

"Our entire site became inaccessible, and patients and doctors were unable to utilize vital information. We saw the number of visitors drop off by 20% for the entire month of August"

- Anthony Della Camera, Kidney.org

"Traffic and sales tanked... On those days on which we were blacklisted, we lost about 80% of our traffic and sales."

- Heiko Mitzkus, EnlightenLiving.com

Above are some direct quotes from survey respondents whose website suffered a malware attack and have been blacklisted.
These statistics clearly demonstrate the need for a complete solution that helps scan pages, monitor regularly, detect the problem and is capable of pinpointing the website compromise down to the line of code that caused the blacklisting.

THE REMEDY

Detection and remediation

Given the significant growth in malware attacks against websites and the subsequent impact on web businesses, it is important for webmasters and security professionals to proactively defend their websites. For businesses of all sizes with the goal of protecting their customers, online revenue and brand, an "early warning" detection and recovery system for malware attacks is necessary. Businesses should have the peace of mind that their website is being regularly scanned for malware. The best detection mechanism scans all pages for malware drive-by-downloads, malicious downloads (including PDFs, images, and executable files), and links to external sites. Automated remediation tools that neutralize web-based malware infections can help enable a rapid recovery from such attacks.

OVERVIEW OF DASIENT SOLUTIONS

Malware Monitoring

Dasient's WAM Malware Monitoring periodically scans a website for malware infections. The Malware Monitoring is based on Dasient's patent-pending Malware Analysis Platform, which crawls a website and analyzes the content on each page for signs of compromise and malware infection. The Malware Analysis Platform utilizes behavior-based technology and machine-learning-like algorithms to determine whether a malware infection has occurred. Dasient's Malware Analysis Platform also leverages telemetry data that Dasient collects by monitoring millions of sites across the web. If any of these sites suffers a new kind of malware attack, Dasient learns about the new attack and automatically updates the defenses for customers. The telemetry data that is collected enables Dasient to stay on top of the latest attacks that are being developed by hackers. The Malware Analysis Platform, which has already identified over 100,000 unique malware attacks, uses this knowledge base of defenses to protect customers from the latest attacks.

FIGURE 8: DASIENT INFECTION LIBRARY REPORTS UNIQUE MALWARE ATTACKS REGULARLY

If Dasient's WAM Malware Monitoring detects that a customer's website has been infected, the customer receives an immediate alert with diagnostic information to remove the infection. Armed with the diagnostic information, the website or its web hosting provider can remove the malicious code, in many cases before the site harms many of its users, suffers damage to its brand and reputation, or gets blacklisted. Dasient continues to monitor the site and send alerts if malware activity is detected in
the future.

FIGURE 9: DASIENT CUSTOMERS RECEIVE INFECTION ALERTS FOR EACH MALWARE INFECTED URL

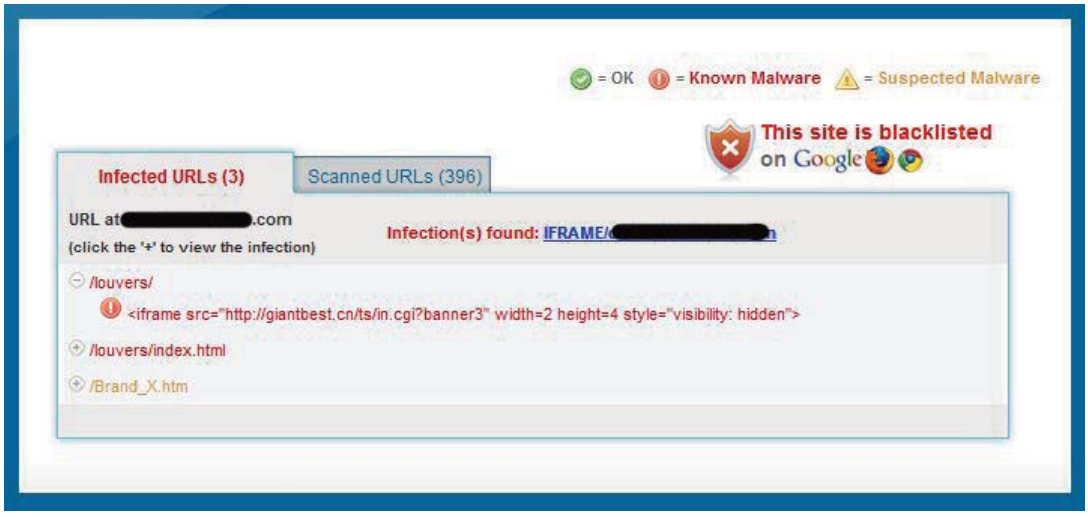
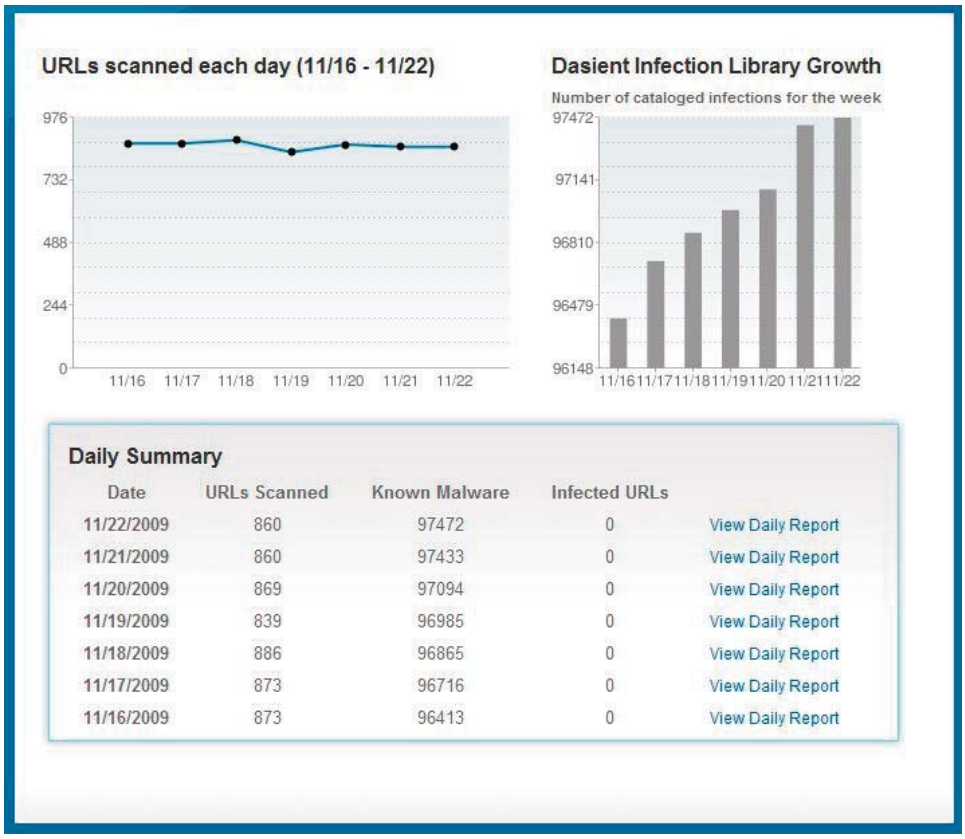


FIGURE 10: DASIENT CUSTOMERS RECEIVE WEEKLY REPORTS WITH DETAILED SCAN INFORMATION



Malware Scanning API

The Dasient WAM Malware Scanning API enables our customers to make API calls directly to Dasient Malware Analysis Platform which analyzes the content on an individual web page for signs of compromise and malware infection. A customer using Dasient Malware Scanning API sends Dasient the API requests containing the URLs that they would like us to scan. Customers can make multiple API calls in a day. Dasient's Malware Analysis Platform receives the list of URLs in each API call and performs scans of each URL individually. In case of discovery of an infection in a particular URL, customers receive immediate alerts with diagnostic information to block the infected pages or remove the infection before getting blacklisted.

As a result, the site can continue to operate as normal and avoid getting blacklisted, even after suffering from a malware attack. Dasient will continue to receive URLs from the customers, monitor those URLs, and sends alerts if malware activity is detected in the future. The following

are important characteristics of the Malware Scanning API:

- The API is based on JSON-encoded format and enables on-demand scans of customer URLs. This helps customers avoid getting blacklisted and ultimately protects their brand and revenue.
- Dasient WAM Malware Scanning API empowers you to instantly discover malware activity on specified URLs
- The API supplies you with actionable information to help you block infected pages and/or resolve the malware problem instantly and continue with business operations.

Malware Recovery Service

Dasient's patent-pending Web Anti-Malware (WAM) Recovery automatically quarantines a malware infection discovered by Dasient's Malware Monitoring system. Dasient's Recovery service leverages a web server module that is installed by the customer or its web hosting provider.

When a customer's website is infected with malware, Dasient's Malware Monitoring service detects the infection and generates quarantining instructions to protect the website from the attack. Dasient's servers make an authenticated connection to the web server module running on the customer's infrastructure. The Dasient web server module which is installed on customer's server receives detailed instructions which identify the exact URLs and the specific attack code that needs to be remediated. The Dasient web server module then automatically filters the malware infection out of any infected web pages before sending the page to end users. With Dasient's Recovery service, the site no longer infects users and is no longer at risk of suffering brand damage or getting blacklisted. The WAM Recovery Service is conducted in two ways:

1. Through a fine-grained recovery mechanism where Dasient Recovery service automatically filters out Malware infections before infected pages are served to end uses and therefore providing a greater level of user experience
2. Through a coarse-grained recovery mechanism. When an infection occurs on a URL, Dasient Recovery service blocks infected pages and as a result the infection is avoided. Users will not gain access to the infected pages.

Conclusion

Web Malware attacks pose a serious threat to your website and your users. The shift in malware spread, the automation of the attacks and structural vulnerabilities are far more daunting than ever before. Dasient recommends a proactive approach to web businesses to defend themselves against malware attacks and avoid losses of traffic, reputation, and revenue. Prevention alone is not the solution. Dasient recommends detection and remediation Web Anti-Malware (WAM) services that provide end-to-end protection by monitoring websites for Web-based malware infections. When an infection is detected, alert is sent to the website owner along with diagnostic information to remove the malicious code. Dasient WAM also offers automatically recovery against any malicious code.

For more information about Dasient Web Anti-Malware, please visit www.dasient.com

ABOUT DASIENT, INC.

Dasient is an Internet security company that protects businesses from web-based malware attacks. It is the first to develop a complete Web Anti-Malware service that can monitor and quarantine malware on websites to help businesses avoid losses of traffic, reputation, and revenue. Dasient was founded by senior engineers and product managers from Google, Hewlett-Packard, and McKinsey. The company is backed by a group of seed investors who also invested in VeriSign, Citrix, Twitter, Digg, Tumbleweed, Finjan, and more.

www.dasient.com
530 Lytton Avenue, Suite 256, Palo Alto, CA 94301
Tel: 1-650-384-0535 E-mail: sales@dasient.com

Dasient