Reinterpreting the Disclosure Debate for Web Infections

Oliver Day[1], Brandon Palmen[1], and Rachel Greenstadt[2]

[1] StopBadware Project
Berkman Center for Internet and Society
Harvard University
oday@cyber.law.harvard.edu,bpalmen@cyber.law.harvard.edu
[2] Center for Research in Computation and Society
Harvard University
greenie@eecs.harvard.edu

Abstract. Internet end-users increasingly face threats of compromise by visiting seemingly innocuous websites that are themselves compromised by malicious actors. These compromised machines are then incorporated into bot networks that perpetuate further attacks on the Internet. Google attempts to protect users of its search products from these hidden threats by publicly disclosing these infections in interstitial warning pages behind the results. This paper seeks to explore the effects of this policy on the economic ecosystem of webmasters, web hosts, and attackers by analyzing the experiences and data of the StopBadware project. The StopBadware project manages the appeals process whereby websites whose infections have been disclosed by Google get fixed and unquarantined. Our results show that, in the absense of disclosure and quarantine, certain classes of webmasters and hosting providers are not incentivized to secure their platforms and websites and that the malware industry is sophisticated and adapts to this reality. A delayed disclosure policy may be appropriate for traditional software products. However, in the web infection space, silence during this period leads to further infection since the attack is already in progress. We relate specific examples where disclosure has had beneficial effects and further support this conclusion by comparing infection rates in the U.S. where Google has high penetration to China where its market penetration rate is much lower.

1 Introduction

Debate has raged for over a decade to determine the most responsible and productive way to disclose software vulnerabilities, so that software vendors, vulnerability researchers, and the public all benefit from the exchange of knowledge without facilitating the software vulnerability exploitation. While it sometimes makes sense for software vulnerabilities to be hidden for a short period of time if those vulnerabilities have not already been identified by malfeasants, the same cannot be said for websites which distribute malware, because the vulnerabilities in these websites have already been exploited, and because allowing these infections to remain hidden would harm Internet users while abetting attackers.

Compromised websites often infect visitor's computers automatically by exploiting vulnerabilities in Internet Explorer, Firefox, and other web browsers which allow the infected pages to execute malicious code and download additional malware components without the visitor's knowledge or consent. The HTML elements which attackers place on websites to make them infectious, such as hidden iframes and javascript references to third-party malware hosts, can be placed on compromised websites with such ease and automation that a growing number of unsophisticated attackers now participate in malware affiliate networks, which pay these attackers commissions for infecting legitimate websites with their malicious code [4].

Because Internet users who visit compromised websites often have no idea that their computers have been infected with malware, the operators of these websites have little incentive to disclose to their visitors that they may have been infected; doing so could damage the websites brand or reputation, and failing to do so is unlikely to bear any negative consequence for the website owner. Thus, voluntary disclosure of website infections allows webmasters to conceal the risk that their websites pose to Internet users, and to inappropriately externalize the costs of poor website security. This has the potential to create a lemons market [6], where webmasters and web hosting providers who invest in securing their websites against attack are driven out by others who do not invest in security, and who place the burden of resulting website infections on Internet users.

Mandatory disclosure of website infections forces webmasters to accept responsibility for the safety and security of their web properties, and removes the perverse incentives which lead webmasters to systematically under-invest in website security. Google and StopBadware's public disclosures of infected websites have caused webmasters and web hosting providers to pay greater attention to web security. They exemplify a mandatory disclosure regime which we believe should be uniformly enforced, either by public policy or by additional private web gatekeepers like search engines and Internet service providers.

Google attempts to protect users of its search products from these hidden threats with the "safe browsing" [1] program. This program identifies websites that are infected with malicious code through the use of instrumented browsers which reside in virtual machines. These machines create a score based on new network connections, processes spawned, and other criteria which are considered abnormal for machines only browsing a url. Those urls which are deemed bad are shielded from Google users by inserting interstitial warning pages behind links to these websites in returned search results. In addition to providing more information about these warning pages and malware threats in general, Stobadware [2] provides education and technical resources to website owners who wish to clean and secure their websites and have Google's warning flags removed from their website's search results.

This paper describes our experiences implementing and supporting the mandatory disclosure system developed by Google and StopBadware. In addition to describing the trends we have observed in malware infection technologies, we

explore the characteristics of webmasters and web hosting providers that we consider most prone to attack, and compile statistics from our clearinghouse of infected websites, identifying particular web hosting providers that host an unusually large number of infections. We conclude the paper with a discussion of the impact that unusual limitations on public disclosure may have had on the proliferation of infected websites in China, and we present our opinion that the mandatory disclosure paradigm which we have prototyped should be expanded to protect more Internet users, and to ensure that all Internet stakeholders make web security a priority.

2 Attack Trends

When the StopBadware project was founded, the Internet malware landscape was considerably simpler than it is today. We framed our software guidelines to define a class of software which causes unacceptable user harm, and focused on identifying borderline applications rather than on the uncontroversial malware that antivirus and security vendors seek to address. At that time, most of the software that violated our guidelines was packaged with popular consumer applications or tucked away in the so-called 'dark corners' of the Internet: websites promoting software and media piracy, pornography, drugs, and gambling. In order to have her PC compromised, an Internet user was first induced, by deception or ignorance, to manually download and run the malicious software. In that environment, the task of identifying, unmasking, and incentivizing the reform of distributors was more easily accomplished for many reasons. In particular, malware distribution was almost invariably an intentional act, either by software developers who packaged the exploits with their consumer applications, or by shadowy web hosts who deliberately added exploit links to their web pages. This made it fairly simple to encourage the reform or abandonment of particular applications and websites by inviting public scrutiny of the offenders and by contributing to public education about the hazards of downloading untrusted software. Unfortunately, the success that security watchdogs like StopBadware have had in improving public caution against traditional malware distribution channels has had the ancillary effect of encouraging malware creators to develop new methods of exploiting Internet users. Three important conditions of the malware environment have made it particularly difficult for web consumers to avoid malware threats and for StopBadware to combat them:

First, the malware community has embraced 'long-tail' network economics, which postulates that considerable value can be derived from exploiting a large number of small, niche markets. In the malware context, the expected value of stolen financial information, passwords, and other personal data that can be collected by attacking a large number of poorly secured niche websites exceeds the value of attacking a single, large website that is well protected. To this end, malware distribution networks often no longer attempt to create demand for false or dubious websites (against which the public is now fairly well warned), and instead invisibly hijack traffic from thousands of legitimate websites by exploit-

ing security vulnerabilities or misconfigurations in those sites and then adding a small amount of malicious code to those sites which does not otherwise affect the website's functionality. Since exploits can now be downloaded and executed automatically upon visiting a compromised page, visitors to these normally safe websites are often unaware that they have become vulnerable to identity theft, or that their computers have been conscripted into the ranks of a botnet. When StopBadware's collaboration with Google to blacklist URLs that victimize the Internet users began in August, 2006, most of the sites that were added to our clearinghouse belonged directly to those parties who profit from the distribution of malware. Today, a large number of these domains belong to third-party hacking victims whose only responsibility for malware distribution is the mismanagement of their websites' security, and who often believe that StopBadware has mistakenly and carelessly advised web users to avoid visiting their personal blog or small business website.

This disconnect between webmaster perceptions of security and reality frames a second notable development in the malware environment: the emergence of a vulnerable class of web content providers we call 'consumer webmasters'. These are individuals who have benefited from the simplification of web publishing techniques without having gained a technical understanding of how to keep their websites secure. In addition to neglecting to use strong passwords and correct file permission settings, consumer webmasters tend to deploy off-the-shelf web scripts like blogging platforms and photo galleries which, especially when they are not updated with security patches in a timely manner, significantly increase the number of vulnerabilities composing a site's attackable 'surface area'. Mid-tier shared web hosting services also contribute to the problem. These high-volume, low-margin web hosts often pack thousands of clients onto each physical server, such that the exploitation of a single software vulnerability or poorly protected user account can result in thousands of compromised web sites. In order to cater to the widest variety of clients without incurring the costs of server customization, these web hosts often enable dozens of redundant or seldom-used features by default, the vulnerabilities of each of which can compound the vulnerability of the server as a whole. Finally, the threat that inexperienced consumer webmasters and insecure web hosts pose to Internet users is exacerbated by the fact that even when Google and StopBadware positively determine that a website has been compromised, the consumer webmaster of that site often has an insufficient understanding of the problem to identify and remove the malicious code and secure the site against future attacks.

The frequency with which StopBadware encounters webmasters and web hosts who are more concerned about losing traffic or customers than they are about making their websites safe for the public is alarming, and informs the third challenge which we now face in our campaign against the spread of malware: the ability of web content providers to conceal and externalize the costs of malware infection under voluntary disclosure policy, which does not require that webmasters disclose their infections to the public. Website owners who do not inform the public that their websites have been compromised possess asym-

metric or insider information which systematically results in harm to Internet consumers. The user protections enabled by Google's interstitial warning pages and StopBadware's website review clearinghouse help to spread responsibility for Internet security among more Internet stakeholders, but are insufficient in scope to address the source of this incentive problem. Vulnerable Internet users who visit compromised webpages directly, or through links from other pages, rather than through Google's search results, are not protected from infection, and even Google's safe-browsing program lacks the capacity to identify all new malware threats before many Internet users are infected. While the impact of Googles warnings often prompts webmasters to clean the infections from their websites, it often takes some time for the problems to be fixed, during which many Internet users who access the infected websites directly are exploited. StopBadware hopes to form partnerships with additional web gatekeepers like search engines and potentially Internet service providers to make our threat disclosures more comprehensive, but these measures treat the symptoms of an incentive problem. If webmasters held web hosts responsible for the security of their servers, and if Internet users held webmasters responsible for the safety of their webpages, all Internet stakeholders would find it in their interests to protect themselves against malware infection.

2.1 Drive-By Downloads

In our experience, automatic or 'drive-by' downloads from trusted websites have become the most common form of malware distribution on the Internet today. In the past, Internet users could avoid malware infection simply by choosing not to download and run unknown applications, browser toolbars, or plug-ins—and a great deal of effort was spent teaching people to avoid these downloads. Although this education did reduce the effectiveness of traditional, deceptive but consent-driven malware distribution channels, it turned a blind eye to the automatic object downloads embedded in HTML webpages, like images, iframes, and JavaScript. When malware distributors learned to use these embedded web objects to exploit browser vulnerabilities (such as MDAC, Shell.Object, and ANI), it became unnecessary to induce web users to download and install exploits - Internet users could be infected simply by rendering the code of a compromised webpage in a vulnerable browser.

The 'hidden iframe' attack is one characteristic form of drive-by download that malware distributors utilize to deliver exploit payloads to unsuspecting Internet users. StopBadware first encountered this type of attack in December, 2006, when it received a review request from the owner of a website called SantaLinks, which Google had flagged as potentially harmful. When we tested the site, we were initially perplexed by Google's malware determination, since we did not discover any visible links to malicious downloads on the site; however, a closer inspection of the site's HTML code revealed a hidden iframe at the bottom of the page which automatically exploited a known Internet Explorer vulnerability to install malware. The website owner removed the offending iframe code in time for the holidays, but attackers soon reinfected the website because the

initial site vulnerability was not repaired. Reinfections are common for websites whose infections are caused by the exploitation of software vulnerabilities which remain on the server, even after the symptoms of an initial infection, such as foreign iframes, have been removed. The iframe attack that SantaLinks suffered was relatively simple, but it illustrates several key developments in the way malware is distributed. Most importantly, SantaLinks was an extremely innocent appearing website whose credibility Internet users had no reason to doubt. Previously, malware distributors expended great effort concealing the nature of their exploits as desirable downloads, and typically preyed upon appetites for pornography and illicit software which overcame Internet users' defenses against the known risks of such downloads. Now, no such efforts need to be made, except to ensure that the iframe or javascript that loads an exploit is not discovered by the user or the webmaster. Placed in the midst of a long document, a simple tag of the form

```
<iframe src="third_party_url" height=0></iframe>
```

can easily avoid the detection of an inexperienced webmaster, but can launch a visitor's web browser through a chain of JavaScript tests and additional iframes which ultimately results in the automatic download and execution of the precise exploit that will compromise that particular visitor's computer. If a concerned user or webmaster does investigate the source of a mysterious iframe, he often finds that the resulting JavaScript code has been obfuscated, and is unintelligible to casual human readers as well as to many text signature-based antivirus scanners.

Example: The following script for inserting a malicious iframe:

```
<SCRIPT>window.status='Done';document.write('<iframe name=0b617b46901
src=\'http://77.221.133.188/.if/go.html?'+Math.round(Math.random()*55640)+'5\'
width=214 height=260 style=\'display: none\'></iframe>')</SCRIPT>
```

might appear on an infected website in this obfuscated form:

```
 <script>function v47befeddcf5b2(v47befeddcf9ba){ var v47befeddcfdac=16;
 return(parseInt(v47befeddcf9ba,v47befeddcfdac));}function
 v47befeddd09a0(v47befeddd1198){ var v47befeddd1d95=2; var
 v47befeddd15ac='';for(v47befeddd1991=0;
 v47befeddd1991<v47befeddd1198.length;
 v47befeddd1991+=v47befeddd1d95){v47befeddd15ac+=(String.fromCharCode(v47
befeddcf5b2(v47befeddd1198.substr(v47befeddd1991, v47befeddd1d95))));}
return v47befeddd15ac;}
document.write(v47befeddd09a0('3C5343524950543E77696E646F772E7374617475733
D27446F6E65273B646F63756D656E742E777269746528273C696672616D65206E616D653D3
0623631376234363930312073726335C27687474703A2F2F37372E3232312E3133332E313
8382F2E69662F676F2E68746D6C3F272B4D6174682E726F756E64284D6174682E72616E646
F6D28292A3535363430292B27355C272077696474683D323134206865696768743D3236302
7374796C653D5C27646973706C61793A206E6F6E655C273E3C2F696672616D653E27293C2F
5343524950543E'));</script>
```

Adding to the sophistication of this exploit-chain approach, many of the links in this chain can be hosted in different domains, on different servers, and in different countries, making it very difficult to disable or even map the complete malware network, since a single URL change at any level of the distribution infrastructure can introduce new exploits or replace a server that has been blocked or disabled by Internet service providers or law enforcement officials.

2.2 Weaponized Exploit Packs

Because the hidden iframes and obfuscated javascript discussed previously are invisible to web users, attackers no longer need to customize the placement and appearance of exploits to blend into each page that those attackers compromise; thus, the process of adding these tags can be automated. Using new toolsets, an attacker who has accessed a vulnerable server can add the same hidden iframe or obfuscated javascript to every web page on that server with trivial effort. If this server belongs to a shared web host, hundreds or thousands of different websites with vastly different audiences will all be simultaneously converted into malware distribution channels. Because of the ease with which these commoditized attacks can be performed, the expertise required of attackers who hope to profit from malware distribution has diminished—any person who possesses a basic understanding of web code is capable of launching a scripted attack. To further enhance the labor productivity of these freelance attackers, malware distributors now market weaponized exploit solutions like 'Icepack,' and 'Mpack', which package complicated hacking procedures with push-button simplicity to black-market entrepreneurs who desire a share of the malware bounty [3]. These software packages were initially sold for as much as $1000, but they are now freely distributed on hacking forums, and allow almost anyone to deploy a private malware distribution network. The producers of these 'weaponized' exploit kits even sell technical support and software updates containing new exploits and evasive techniques like IP-filtering and geo-targeting, which allow attackers to minimize exposure to security firms and maximize the value of each infection.

Although obtaining and deploying these weaponized exploit packs is relatively simple and inexpensive, there remains a certain amount of risk associated with running a malware server. Black market entrepreneurs who are willing to assume this risk are known to develop affiliate networks around their exploit platforms, thereby employing many other attackers to place the entrepreneur's malicious iframes on vulnerable websites. The affiliate network tracks the number of infections generated by each affiliate, and returns a small fee which is usually dependent on the country where the infected computer resides [4]. The similarity borne by these malware affiliate networks to legitimate publisher advertising networks is not coincidental - the success of each depends primarily on the number of webpages enlisted to display the syndicated content, rather than on the efficacy of that content. In fact, most of the 'commercial' exploit packs that exist target software vulnerabilities that have already been patched by vendors; however, if even 5% of the visitors to a compromised web page have failed to apply those security patches, and if links to the exploit server are sufficiently

widespread, the aggregate number of resulting infections will be large. The similarity of advertising network and malware network economics has encouraged other black market entrepreneurs to bypass hacking altogether by simply using javascript or iframe-based advertising networks as malware vectors, or by developing their own dubious advertising networks which are then redistributed by syndicating ad networks like Clicksor.

3 Market Failure: Consumer Webmasters and Mid-Tier Web Hosts

With these new tools of exploitation and profit, a growing community of freelance attackers scours the web for server vulnerabilities which will allow attackers to add malicious code to innocent websites. Although the occasional discovery of vulnerabilities in a major website or web service can be exceptionally profitable, freelance attackers are much more likely to earn steady incomes by compromising a large number of small, poorly protected websites than by expending great effort attempting to penetrate the defenses of a few large sites. This increased demand for vulnerable websites to attack has prompted some hackers to compile lists of such sites, which they sell in bulk to the attackers. The simplest way to compile such voluminous lists is to identify vulnerabilities in off-the-shelf software products like database applications, web-host control panels, and blogging platforms, and then determine which websites have those vulnerable software products enabled and unpatched. This can often be accomplished just by searching for particular identifying text-strings in commercial search engines.

The efficiency of targeting websites which have inadequate defenses and standardized software that is out-of-date has led to the systematic exploitation of consumer webmasters. Consumer webmasters tend to be individuals who have no formal IT training, and who have learned to minimally use web server technologies for specific purposes such as publishing a blog, promoting a small business, or providing a topical discussion forum. Consumer webmasters face technological problems as they arise, rather than attempting to identify potential problems and prevent them in advance, and commonly ignore skill-demanding best-practices in favor of expedient, functional solutions. Some consumer webmasters possess the skills required to install and tweak software platforms like WordPress or phpBB, but fear upgrading these platforms as security updates are released, lest the upgrades break the existing system and require repairs which demand greater technological sophistication than the webmaster possesses. Others hire third parties to customize open-source content management systems or e-commerce applications for their small businesses, and then neglect to maintain the websites in any way, imagining that because they have not altered the sites since their creation, the sites remain pristine and secure. In short, consumer webmasters want their websites to 'just work', and invest little effort in developing the fundamental understanding of Internet technology that would inform decisions to deliberately address website security risks before they are exploited. Although an understanding of Internet security is certainly not a prerequisite for

operating a website, forcing webmasters to accept responsibility for the safety of their web properties ensures that webmasters are incented to demand better security from their web hosting providers.

The websites operated by consumer webmasters rarely require much processing and network bandwidth, so these site owners are unwilling to pay the extra costs associated with obtaining and supporting dedicated web hosting. Instead they purchase basic shared web hosting packages that firms market by competitively increasing the number of features available on each plan while reducing their prices to nearly the marginal cost of administrating a single additional user account. In many ways, this competitive pressure on web hosts is a positive development, since it allows many more web users to operate websites affordably. Unfortunately, our experience has been that consumer webmasters tend to choose between these mid-tier hosting providers on the basis of comparative feature propositions marketed by the web hosts, rather than by determining which web hosts offer the best combination of features and security. Because competition between mid-tier web hosts is intense, and the fixed cost of adding additional features to bargain hosting plans is low compared to the marginal revenue to be gained by expanding the host's client-base, many of these web hosts now bundle multiple database applications, several popular scripting languages, and dozens of 'one-click-install' web applications with every plan that they sell. This feature bloat constitutes a significant threat to the security of servers operated by mid-tier web hosts not only because the vulnerabilities of each feature compound the vulnerability of the server as a whole, but also because many of these mid-tier web hosts are unprepared to uniformly deploy the hundreds of security patches that the vendors of these products release each year. Each time a web host attempts to update features, it risks breaking one or more of the many software dependencies inherent to its complicated systems. Since server stability is a far more visible feature of hosting quality to consumer webmasters than server security, mid-tier web hosts often refrain from updating their older systems even when they apply security patches to brand new servers. Finally, some mid-tier web hosts make themselves particularly vulnerable to attack by deploying off-the-shelf server control-panel software like cPanel or Plesk, whose standardized vulnerabilities can be exploited to commoditize the attack of multiple web hosts, thousands of servers, and potentially millions of websites [5].

Because a large number of vulnerabilities can exist in a single website and server, when a website does become compromised it is often difficult for exploited Internet users to assign blame for the security lapse that permitted the attack, and to determine which parties, if any, were negligent. Ideally, website attackers would be discovered and punished by law enforcement, but the structure of malware distribution networks is such that it is extremely difficult to identify and prosecute these criminals. Web hosting providers typically argue that website security is the responsibility of website owners, and that they are not responsible for the safety or security of their clients' websites. But when an attack on a single client's website has the potential to compromise additional websites and servers, the web host should play an active role in enforcing the security even of client

websites, in the same way that a landlord might require certain safety practices of his tenants. Web hosts are loathe to perform this monitoring, because doing so would result in added costs, a slippery-slope toward content censorship, or legal liability; and because there is little way for the public to know just how secure or insecure any particular web host's services are, the web hosting market exhibits traits of a 'lemons' market [6], where secure web hosts are driven out at the cost-margins by impune, insecure web hosts. Website owners bear similarly little liability to Internet users for the safety of their websites, and therefore have little incentive either to secure their websites or to disclose attacks when they occur. The ability of web hosts and website owners to externalize the costs of lax web security to Internet users by failing to disclose the potential for harm constitutes a market failure that must be addressed to ensure that all Internet stakeholders take effective precautions against malware infection.

4 Vulnerability Disclosure

The debate surrounding the proper way to disclose software security vulnerabilities is intense and unresolved. This problem has been studied extensively by the economics and information security community [7–16].

Software vendors insist with some force that when a software vulnerability is discovered, the vendor of that software should be notified sufficiently in advance of public disclosure to allow the vendor to produce and deploy a patch. In theory, this would prevent malfeasants from becoming aware of vulnerabilities until it is too late to exploit them; but in practice, attackers may discover the vulnerabilities independently and may then exploit them even more effectively because they are not publicly acknowledged [13]. Unfortunately, software vendors almost always prefer to hide the vulnerabilities in their products, and are willing to pay considerable bounties to independent vulnerability discoverers in exchange for non-disclosure by the discoverers [15]. Since there is no general consensus on which policy is socially optimal (or rather, the optimal solution depends on the case), voluntary or delayed disclosure has become the norm for software vendors and independent security analysts alike. Because the public is left unaware of the vulnerabilities, it is unable to defend against the exploitation of those vulnerabilities; and perhaps more importantly, it fails to sufficiently pressure vendors to focus on security, detect vulnerabilities, and patch them expediently [10]. However, the context in which the problem has been studied is that of application software running on end hosts, not web infections.

Like software vendors, website owners commonly object to Google's immediate public warnings about their websites when it is determined that they host or distribute malware, believing that they should be entitled to a grace period during which they can clean and secure their websites before they suffer the financial or reputational consequences of public disclosure[3]. These webmasters

[3] Google does attempt to contact webmasters when their sites are initially added to Googles blacklist, but there is no reliable system to ensure that webmasters receive these communications.

value the reputation of their brands more than they value the safety of their visitors. Their websites are not merely vulnerable, they are already compromised; they are actively harming internet users, and they need to be quarantined immediately. Arora, Telang, and Xu summarized the effects of late disclosure in traditional software products as reducing the time window that customers are exposed to attack, but decreasing the vendor's willingness to deliver a quick patch [8]. To use this logic for web infections is disingenous; in this case, late disclosure *increases* the time customers are exposed to attacks, decreases the vendor's willingness to deliver patches, and limits the ability of customers to discover that they have been compromised. Keeping these infections secret even for a short period of time would abet attackers, whereas publicly disclosing the infections ensures that internet users are informed of the risks of visiting the infected websites. By publicly disclosing and, to the extent that websites depend on Google for traffic, quarantining websites that distribute malware, StopBadware and Google force website owners to address the security issues that they would otherwise force their visitors to bear without consent. Although this can be frustrating for website owners who are themselves victims of attack, we believe that it is their responsibility to ensure that their web properties do not threaten public safety. Still, many website infections are caused not entirely by the negligence of website owners themselves, but also by the lax security standards of their web hosts. Just as novice or apathetic webmasters externalize the costs of poor website security to internet users, impune web hosts externalize the costs of poor server security to consumer webmasters, who have few means of recourse.

5 Methods for Identifying Most-Infected Web Hosts

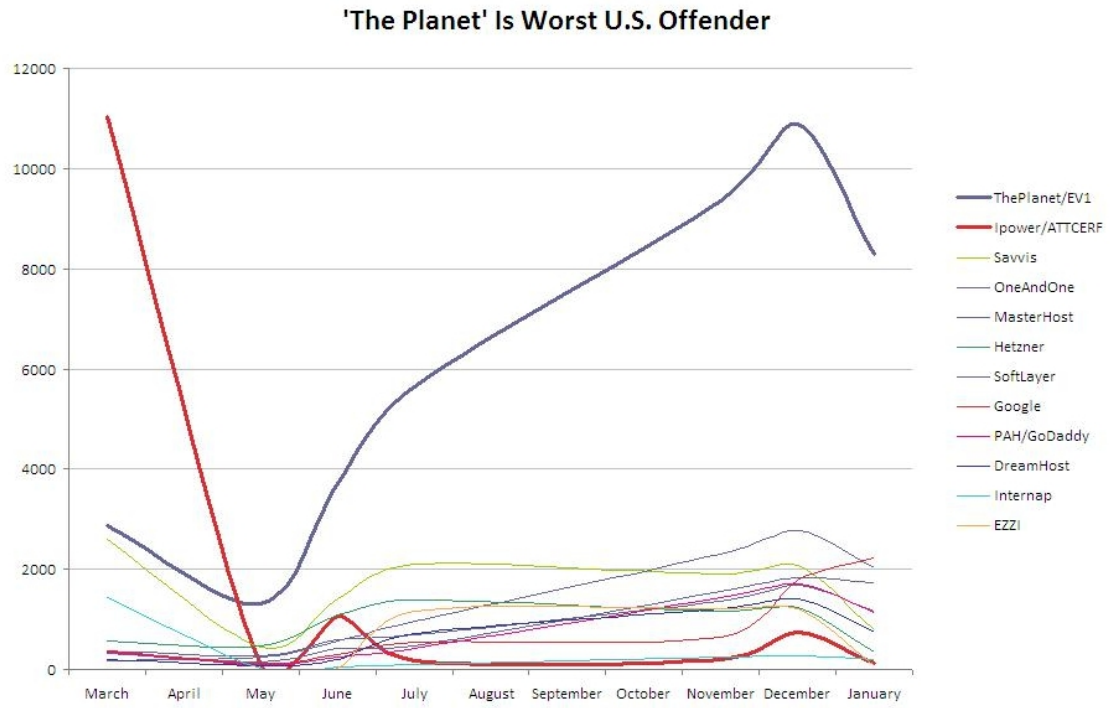
StopBadware's list of infected websites is currently derived from a single data source: Google. Google's Security Team sends us a list of URLs that Google has determined to host malware, which we tag in our clearinghouse with the information we develop through our own testing and through interaction with webmasters and the public. Google's method of constructing this list of infected URLs is described by Provos et Al. [1]. Because StopBadware's list of infected websites is dependent on Google's malicious website collection and detection methods, it is possible that some systematic bias exists in our data, reflecting the limitations of the scope and depth of Google's index, or the particular types of infection detected by Google. For example, if Google only tests websites using Internet Explorer, it will fail to detect infections that exclusively exploit other web browsers. We believe that Google's data is representative of the Internet as a whole, but it is probably not comprehensive. Because many website infections are caused by links to third-party servers, the availability of these referenced servers can affect the infectiousness of the compromised webpages. Other infections are cleared by website owners or advertising networks after Google has reported the sites to us but before StopBadware has independently tested those sites. Either of these factors can create inconsistency between Google's list of

infected websites and StopBadware's testing and reporting process, since a site that infects users at one moment might appear to be clean in the next. In order to maximize the accuracy of our data by limiting our study to websites which we know first-hand to be infected, we constrained our study to the list of websites whose infections StopBadware had confirmed. StopBadware does not attempt to confirm infections on websites whose owners have not requested reviews from us, so the list of confirmed infections used in this study reflects the subset of website owners who requested StopBadware's assistance, and therefore excludes those websites which are likely owned by malfeasants directly, and those whose owners chose to deal with the infections without our assistance. The IP addresses for these confirmed, infectious websites were resolved using a DNS server controlled by StopBadware. Although it is common for malware distribution servers to change IP addresses rapidly in order to avoid detection and blacklisting, we believe that the IP addresses of the compromised personal and consumer websites that predominated our sample are unlikely to change frequently. In the future, we plan to resolve IP addresses for all URLs supplied to us by Google or other data partners at the time we receive those URLs, not just those which we have confirmed to be infected. Once this list of IP addresses was compiled, we used a free 'who-is' lookup server provided by Team Cymru in Chicago to group the IPs by Autonomous System Number (ASN), registered AS name, registration date, country of registration, and registrar. This information was then linked in our database to the original website URLs and IP addresses, allowing us to determine which ASNs hosted the largest number of infections. ASN grouping is not perfect, since some IP addresses do not map to any existing ASN, and some ASNs are subleased, which can make certain web hosts appear more secure than they really are. Furthermore, some ASNs are relatively small, while others are Class B blocks, which can contain tens of thousands of IP addresses, each of which could host thousands of URLs. To add granularity to our investigation, URLs were also grouped by IP address, which revealed a few cases in which nearly all of an ASN's infections were hosted on a single host IP.

6 Web Host Infection Results

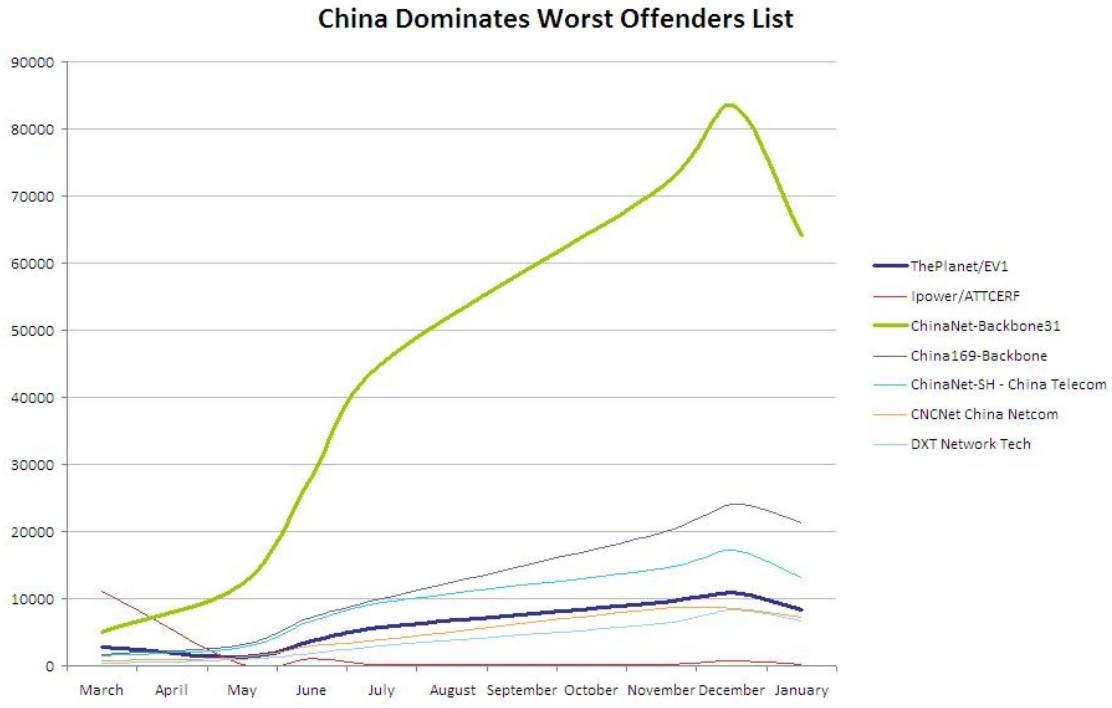
Although StopBadware does not conduct comprehensive vulnerability scans of web hosts or particular servers, we use the information contained in our website clearinghouse to identify web hosts that host an unusually large number of compromised websites, an indicator that those hosts are either structurally insecure or undedicated to clearing infections after they occur. We publish this information to inform webmasters about the hidden risks of contracting hosting services with these web hosts, and to encourage the public to pressure the web hosts to reform their security practices. Our first public report on highly infected web hosts was issued in May '07, and highlighted the security risk posed by one hosting company in particular: IPowerWeb [17]. At that time, IPowerWeb hosted over 10,800 infected websites; which composed more than 20% of all websites in our sample, and nearly four times the number hosted by the second most

infected host. As it happened, IPowerWeb was undergoing a merger at the time StopBadware released its report, which resulted in enormous public and private pressure for the company to take security more seriously. As of January '08, only 129 of the infected websites in our clearinghouse were hosted by IPowerWeb - a commendable improvement. Even so, the total number of infected websites reported to us by Google increased over 400% during the period between March '07 and December '07, and another web host has developed an unusually large number of infections. The Planet, which is controlled by the private equity firm GI Partners, now hosts roughly 8,300 infectious websites as shown in Figure 6. No matter which party is responsible for the initial security lapses that caused these infections, if The Planet ceased to abdicate responsibility for the security of its servers and forced its clients to clean and secure their websites, it could have a substantial positive impact in the fight against the spread of malware.



6.1 The Panda in the Room

Although The Planet hosts far more infected websites than any other host in the United States or Europe, even this threat is overshadowed by the volume


China Dominates Worst Offenders List
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
March
April
May
June
July
August
September
October
November
December
January
ThePlanet/EV1
Ipower/ATTCERF
ChinaNet-Backbone31
China169-Backbone
ChinaNet-SH - China Telecom
CNCNet China Netcom
DXT Network Tech

of infectious websites which are hosted in China. China's single most infected ASN (#4134) hosted nearly 83,600 infectious websites in December '07, as seen in Figure 6.1 which constituted approximately 30% of our entire website sample. The top 5 Chinese ASNs host over 50% of the world's infectious websites, while the top five ASNs in the rest of the world account for a mere 7.6% of this total. Although the Chinese population is large, internet penetration in China does not exceed that of the rest of the world, and even if Chinese websites are concentrated on fewer ASNs in general, the total number of infections in China far exceeds the total in the rest of the world. We can only speculate why China has an abnormally high rate of infections. Although the value of financial information stolen from Chinese internet users may be low compared to financial information stolen from Americans, the ease with which some Chinese websites can be attacked and many Chinese internet users infected creates a comparative advantage for the production of Chinese bot-networks, which can be used to mount distributed denial-of-service attacks or to send enormous quantities of spam worldwide. Furthermore, many Chinese internet users possess virtual assets in online community and game accounts, which are commonly stolen, aggregated, and exchanged on online auction sites for real currency and value.

We propose that the single most important factor which leads Chinese websites to become infected at a higher rate than websites in the rest of the world is the relative lack of public disclosure and quarantine. Although Google does provide interstitial warnings in its Chinese search results as it does elsewhere, Google controls only about 24% of the Chinese search market. Baidu, China's leading search engine, holds a 61% share of the Chinese search market, and currently offers no clear warnings or protections against harmful websites in its search results. Because Chinese internet users generally do not know which websites host malware and have no clear recourse mechanism to punish or publicly shame insecure web hosts, many Chinese web hosts and website owners do not make the security and safety of their websites a priority.

The Chinese disclosure environment can be viewed as a worst-case scenario for what can happen when web content providers are not accountable to web consumers for the safety of their internet properties. This observation informs the importance of our quest to disclose website infections to the public, to pressure web hosts to take an active role in ensuring the security and safety of their servers, and to educate and support consumer webmasters and internet users who seek information and resources to protect themselves from attack and exploitation on the web. It will be interesting to observe timed attacks on Chinese websites during the 2008 Summer Olympic Games in Beijing. The official website of the 2008 Olympic Games (beijing2008.cn) is hosted on the China Netcom network, which currently hosts over 8,000 infected websites. As the Olympic Games approach and progress, many Olympics-oriented web properties which are hosted on Chinese networks will become highly valuable temporal attack targets. Like the Superbowl 2007 website, which was also attacked, the 2008 Olympics website has little experience defending itself against determined attackers. If the Olympics website is compromised for even one short, peak-traffic

period, perhaps surrounding the opening ceremonies, millions of computers could be infected worldwide. Of course, the official 2008 Olympics website will not be the only Olympics-oriented web property that is targeted by attackers; many other websites owned by Olympics enthusiasts and opportunists will appear this summer, some of which may be even more vulnerable to attack than the official Olympics website. Baidu's lack of malware disclosure mechanisms may provide an interesting opportunity to further test the theories of this paper, by observing the patterns of website infection and visitor exploitation which occur in relation to the games, and by measuring the comparative protective effect that Google's interstitial warnings provide to Google Search users within the limited scope and timeframe of the games.

7 Recommendations

The current voluntary disclosure paradigm for software vulnerabilities is broken. It allows vendors to systematically under-invest in software security while externalizing the costs of resulting software vulnerabilities to end users without those users' informed consent. In the Internet context, voluntary disclosure leads web hosting providers and website owners to take inadequate measures to secure their services against attackers, since they are unlikely to be held responsible for damages to Internet users in the event that their websites become infected. Even when website owners are aware that their websites have been compromised and are actively harming Internet users, many of these website owners deliberately attempt to conceal the attacks, because they value the reputation of their brands more than they value the welfare of their visitors. Similarly, web hosts fail to disclose their security failures because their reputations are guarded from public scrutiny by the intermediating brands of their clients; and thus, the market for web hosting services is also a 'lemons' market.

Google and StopBadwares mandatory disclosure of web infections begins to solve this market failure by informing consumers of risks that website owners and software vendors would otherwise attempt to hide. Other potential remedies, such as civil suits by exploited Internet users against negligent webmasters, could also be effective in shifting the burden of responsibility for web security from consumers to web content providers[4]. One example of mandatory disclosure policy that could be expanded to require webmasters to disclose infections to their visitors is California Senate Bill 1386, which demands that companies disclose incidents which have resulted in the exposure of sensitive customer information. Unfortunately, these legal remedies would be difficult to apply and enforce consistently across the varying legal landscapes of the many countries where malware infections occur. For example, it would be unreasonable to expect American product liability laws to have a substantial impact on Internet

[4] Some have cited the increased investment in fraud-prevention technology resulting from placing the burden of liability for ATM fraud on banks, rather than on account holders, as an example of how civil liability could be used to promote greater investment in Internet security [18].

security in China. Mandatory disclosure of infected websites, whether publicly or privately enforced, can be sufficient protection and remedy for Internet consumers, provided that the disclosures actually succeed in informing all visitors to those websites of their risk of infection. Our warnings play an important role in protecting and informing consumers of the risks of visiting particular websites, but our defensive efforts will not be sufficient to stem the malware tide without the aid of other web gatekeepers, ranging from search engines to web hosting providers. Furthermore, our public warnings about infected websites succeed only in correcting the misallocation of the economic burdens of malware, and do not directly address the underlying security issues which allow these infections to occur. Ultimately, we hope that the pressure on webmasters that our warnings create will encourage them to learn about Internet security, and to demand better security from their hosting providers, so that infections are prevented and neither Internet users nor consumer webmasters become victims of attack. Similarly, web hosts and Internet service providers should be held responsible for the safety of properties hosted on their networks. The positive change enacted at iPowerWeb following StopBadware's report on infected web hosts confirms our belief that mandatory disclosure policy can be effective in encouraging web hosts to invest in good security practices. We therefore propose that in general, when particular websites are determined to host or distribute malware, web service providers should be required to clear the infections or to quarantine those websites. This will extend the protections currently enjoyed by users of Google Search to the rest of the Internet public.

The 2008 Olympic Games in Beijing will provide an interesting opportunity for the global public to pressure China to address its disproportionate malware infection problem. If China fails to contain and clear these infections in time, many 'virtual visitors' to the games around the world will likely fall prey to identity theft and other forms of Internet crime as a result of visiting compromised Olympics-oriented websites. China is already expected to make compromises in certain areas of its Internet policy, such as permitting specific IP addresses assigned to Internet cafes, hotels, and conference centers in the vicinity of the games to access web content that is ordinarily blocked by the 'Great Firewall of China', in order to present itself well to the visiting international community this summer [19]. Thus, it seems possible that Chinese authorities might be more responsive than usual to complaints about China's malware problem, if enough people are made aware of the issue. We hope that the exposure produced by this paper will help inform the public about the perverse incentives that are created when website infections are concealed instead of cleared, and that it will encourage more web gatekeepers, in China and elsewhere, to begin to address these problems with greater responsibility and openness.

8 Conclusion

Website owners and web hosting providers externalize the costs of lax web security by concealing website infections from the public, which harms Internet

users. Google's interstitial warning pages force disclosure of website infections, and cause significant reductions of traffic to these infected websites during the period that the warnings are active. This causes website owners to accept responsibility for the safety of their services, and prevents many Internet users from becoming infected and exploited online.

The consequences of inadequate website infection disclosure are seen in Chinas high malware infection rate, where Google's limited market share implies that fewer Internet users are warned against infected websites. To correct this lack of disclosure in China, we encourage Baidu, China's leading search engine, to adopt a private mandatory infection disclosure regime similar to Google's; thereby expanding protection for Internet users and ensuring that expectations and responsibilities for website security are consistent around the world.

9 Acknowledgments

This work has been supported in part by the Berkman Center for Internet and Society and The Center for Research and Computation and Society (CRCS).

We would also like to thank Team Cymru for providing IP to ASN translation service, Google for the use of their data on malicious websites, and John Palrey, Jonathan Zittrain, Maxim Weinstein, and the rest of the StopBadware team for help and support.

References

1. Provos, N., McNamee, D., Mavrommatis, P., Wang, K., Modadugu, N.: The ghost in the browser analysis of web-based malware. In: HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, USENIX Association (2007) 4–4
2. : Stopbadware. http://www.stopbadware.org (2008) Berkman Center for Internet and Society.
3. OMurchu, L.: Honor among thieves?

   `http://www.symantec.com/enterprise/security_response/weblog/%2007/11/honour_among_thieves.html`

   (2007) Symantec.
4. : Finjan web security trends report q2-2007. http://www.finjan.com (2007)
5. Geer, D., Bace, R., Gutmann, P., Metzger, P., Pfleeger, C.P., Quarterman, J.S., Schneier, B.: Cyberinsecurity: The cost of monopology. Computer and Communications Industry Association (CCIA) (2003)
6. Akerlof, G.A.: The market for "lemons": Quality uncertainty and the market mechanism. The Quarterly Journal of Economics **84**(3) (1970) 488–500
7. Anderson, R.: Open and closed systems are equivalent (that is, in an ideal world). In: Perspectives on Free and Open Source Software, The MIT Press (2005) 127–142
8. Arora, A., Telang, R., Xu, H.: Optimal policy for software vulnerability disclosure. In: Workshop on Economics and Information Security. (2004)

9. Arora, A., Krishnan, R., Nandkumar, A., Telang, R., Yang, Y.: Impact of vulnerability disclosure and patch availability: An empirical analysis. In: Workshop on Economics and Information Security. (2004)
10. Camp, L.J., Wolfram, C.D.: Pricing security: Vulnerabilities as externalities. Economics of Information Security **12** (2004)
11. Cavusoglu, H., Cavusoglu, H., Zhang, J.: Economics of security patch management. In: Workshop on Economics and Information Security. (2006)
12. Choi, J.P., Ferstman, C., Gandal, N.: Network security: Vulnerabilities and disclosure policy. In: Workshop on Economics and Information Security. (2007)
13. Granick, J.S.: The price of restricting vulnerability publications. International Journal of Communications Law and Policy **9** (2005)
14. Rescorla, E.: Is finding security holes a good idea? IEEE Security and Privacy **3**(1) (2005) 14–19
15. Schechter, S.E.: How to buy better testing: using competition to get the most security and robustness for your dollar. In: Infrastructure Security Conference. (2002)
16. Swire, P.P.: Security market: incentives for disclosure of vulnerabilities. In: CCS '05: Proceedings of the 12th ACM conference on Computer and communications security. (2005) 405–405
17. StopBadware: Stopbadware.org identifies companies hosting large numbers of websites that can infect internet users with badware. http://www.stopbadware.org/home/pr_050307 (2007)
18. Anderson, R.: Why information security is hard—an economic perspective. In: 17th Annual Computer Security Applications Conference (ACSAC). (2001)
19. Fallows, J.: "the connection has been reset". The Atlantic Monthly (2008) http://www.theatlantic.com/doc/200803/chinese-firewall.