Trends in Badware 2007

What internet users need to know

The internet holds an unprecedented wealth of information, but it can also be dangerous. We've heard a lot in the past few years about the social dangers of the internet, and less about technical dangers such as malicious programs. Many of us know how to avoid viruses sent over email as attachments, but a rising trend of malicious software available on the internet coupled with new opportunities for making money through online criminal activity has created new dangers.

When the first computer viruses appeared in our email inboxes years ago, most virus authors simply wanted to showcase their skills and gain notoriety. Today, badware authors are part of a thriving global criminal economy that depends on constantly evolving techniques to place damaging software applications on the machines of ordinary computer users.

Badware is software that fundamentally disregards a user's choice over how his or her computer will be used. There are several commonly recognized terms for types of badware, including spyware, malware, and deceptive adware.

At first, badware found on the web was obvious and annoying like the emailed viruses we're used to. A badware application might barrage a computer user with pop-up ads or present system messages that interfered with your day-to-day activities. If your computer had a virus, it was obvious that your computer was "sick." You would then call the "doctor" by installing and running an anti-virus program, and your computer would be healthy again. Because badware was obvious, it was easy to target and remove.

> "The odds are that you already know someone whose computer has been affected by badware"

But as internet users learned how to protect themselves, badware producers began taking a more subtle approach. Badware is no longer as obvious as an in-your-face pop up ad. For many badware applications, you may only know that your computer is becoming slow or feels sluggish, or you may not notice anything at all. Some of these badware applications may directly target your bank account or other private information, while others may steal resources from you such as computer cycles, or allow criminals like spammers to gain control of your machine.

The odds are that you already know someone whose computer has been affected by badware - even if that person doesn't yet know it themselves. How does a computer get infected with badware in the first place? Most of us know that there are potential dangers in the "dark corners" of the internet. Pornography and gambling sites, for example, have long had a reputation for distributing badware. But these days, badware is no longer confined to the "dark corners." Even your own home-grown website may currently be distributing badware without your knowledge. Although "dark corners" are still dangerous, badware producers are now finding more subtle and deceptive ways to install their software on your computer without luring you away from the topic areas and websites you trust. An important step in protecting yourself against these new threats is learning about trends in badware and the ways badware is distributed online.

StopBadware.org gratefully acknowledges the contributions of our partners, allies, sponsors, and community members, without whom our research would not be possible. In particular, we are indebted to the malware research team at Google for the raw data on which our research is based, and to the StopBadware Working Group and Advisory Board for their expertise and guidance.

Badware Trends

When it comes to combating badware, one of your best weapons is a skeptical eye. If an offer looks too good to be true, it quite probably is. If a product or service on the internet says that it's free or provides miraculous results, then there is a good chance the site may have badware or may try to pull you into an undesirable marketing scheme. But badware can be hard to avoid even when you know what to look for.

"Badware can be hard to avoid even when you know what to look for"

Let's say you carefully avoid all "dark corners" of the web. Your browsing history is pristine and you never open email from strangers. Still you wake up one morning, grab your decaf coffee with skim and no sweetener, sit down to read the morning news.... and WHAM! Your computer is hit with pornography and pop-ups, and it takes 45 minutes to get to your home page. What happened?

Like many other web surfers, you may have been the victim of a "drive-by download." The grim description of this type of attack highlights how little participation the victim has in initiating it. As in offline drive-by attacks, the victim is going about his normal life and is simply in the wrong place at the wrong time. Drive-by downloads use vulnerabilities in web browsers to infect your computer with badware when you visit a normally benign website. You may not even be aware that your computer has downloaded anything while you were browsing your favorite places online.

"Any website, no matter how trusted, can be vulnerable to attack"

Of course, something has to happen to turn a normally innocent and safe website into a distributor of drive-by downloads. In many cases, an otherwise innocent website is hacked due to poor security, such as software that has not been updated with security patches or unaddressed vulnerabilities on the servers that host the website. StopBadware receives data from our partners on Google's malware research team, who scour the internet for sites distributing badware. Most of the sites Google has reported to us in 2007 have been normally benign sites which were compromised and turned into distributors of badware without the knowledge or permission of the website's owner.

Drive-by downloads and website hacking add a scary new element to the badware problem. It's no longer possible for a conscientious user to protect herself simply by staying away from the internet's more questionable areas like software piracy, pornography, drugs, and gambling. Any website, no matter how trusted, can be vulnerable to attack. Knitting sites, outdoor equipment retailers, and even Santa Claus's website can be compromised and made to infect users who simply visit a web page. This means the security-conscious user must find new ways to stay protected from badware. The first step to protecting yourself from badware is learning more about it, from common ways badware is distributed to new threats on the horizon. As new ways of distributing badware emerge, your best defense is keeping yourself up to date - from frequently updating the protective software you use on your computer, to keeping informed about new dangers so you will know how best to avoid them.

"Your best defense is keeping yourself up to date"

Website Identity Theft

In the early days of badware on the web, before the rise of drive-by downloads, an internet users had to be tricked into actively downloading a file to get badware onto the user's machine. When drive-by downloads became more popular, the bar was lowered, as badware producers only needed to drive traffic to a web page they owned which hosted drive-by downloads. Still, that method of distribution requires a considerable amount of effort. Tricking a user involves enticing them to a website which is either a forgery or preys on base instincts such as drugs, sex, or gambling. Driving traffic to questionable sites requires advertising to a large number of susceptible users, usually through spam emails or web based forums. Posting to a forum is free, but all it takes is one vigilant person to expose the scam, and spamming requires time or financial investment to reach a large audience.

Now, rather than simply driving internet users to their own webpages that host drive-by downloads, attackers take advantage of the traffic and goodwill already built by other, innocent sites and silently direct that traffic to their own pages. Malicious hackers embed code in the sites they compromise that can invisibly open windows to other, dangerous webpages. Visitors to the compromised sites are generally not even aware that their browser has also loaded a malicious webpage, or that their computer has downloaded anything.

> "Why would a hacker target a small web-based business or personal blog?"

Hacking websites used to be something of a game for the prize of notoriety, so the average website owner didn't have to worry about being attacked. Why would a hacker target a small web-based business or personal blog when there are much bigger and more visible targets? The answer is that the rules of the game have changed, and criminal organizations can now profit from compromising even small websites by attacking many sites at once. StopBadware has seen hundreds, and sometimes thousands, of sites that have been compromised at the same time with links pointing back to a single central point of infection.

Malicious hackers are attracted to the areas where easily exploitable vulnerabilities are most commonly found. These vulnerabilities are frequently concentrated on the tightly-packed shared hosting servers commonly used by small websites. Attackers seek out server vulnerabilities that affect large numbers of sites, and quickly inject those sites with malicious code. And on many shared hosting servers, a hacker only needs to compromise one website's account to affect all the sites hosted on that server. The vulnerabilities of shared servers make badware distribution easier than ever, because it can be done on a massive scale.

> "Attackers seek out server vulnerabilities that affect large numbers of sites"

Consumers have come to depend on relatively inexpensive hosting for their personal sites, as have many small businesses that rely on an internet presence for publicity or sales. Many small site owners do not have the knowledge necessary to keep their own sites secure, and rely on their hosting provider for everything from security to site design using provided templates. At the same time, the shared hosting providers that host the majority of small websites may compromise on security in order to be able to offer hosting at the competitive prices consumers have come to expect.

The tide may slowly be turning, however. More mid-tier hosting providers are becoming aware of the new hacking risks to their customers, and are updating their server software or security permissions systems to help protect the sites they host. Many of the website owners StopBadware has spoken with have expressed a willingness to pay a little more in hosting costs for the peace of mind of knowing their site is safer.

Website owners themselves can take extra safety precautions. Some sites are vulnerable simply due to insecure passwords based on dictionary words, which attackers can easily guess using automated programs. It's also important that site owners keep any software under their control updated regularly, especially when new security patches are announced. The common kinds of software most likely to be in the site owner's control are web content management systems, blog systems, wikis, and shopping carts. Site owners can also be vigilant about monitoring their own sites. For sites with high traffic, compromises are often noticed quickly as visitors report problems on their machines or drive-by download attempts that are prevented by their anti-virus and anti-spyware programs. In contrast, infections on smaller sites can go unnoticed for weeks or months without active monitoring.

Compromised Websites

Common Attacks

While there are many different ways a hacker can compromise a website, two types of attack emerged as by far the most popular over the first half of 2007. These are the use of iframes to load malicious pages in frames inside otherwise benign pages, and the use of javascript browser exploits. Both attacks are based on the use of new code injected into the source code for a website.

"An iframe creates a small 'window' on a webpage so that another page can load inside the embedded window"

Iframe tags are one of the many kinds of tag codes that can be used as part of the source code that creates a website. An iframe creates a small "window" on a webpage so that another page can load inside the embedded window. Iframes are not always used for nefarious purposes - one frequent use, for example, is to embed remotely hosted dynamic content such as online maps into web pages. When used by malicious attackers, an iframe can be made so small that it is invisible, and the visitor to the infected page never knows that another page is also loading in the tiny iframe window. Hidden iframes are most commonly inserted at the very top or the very bottom of a web page's source code.

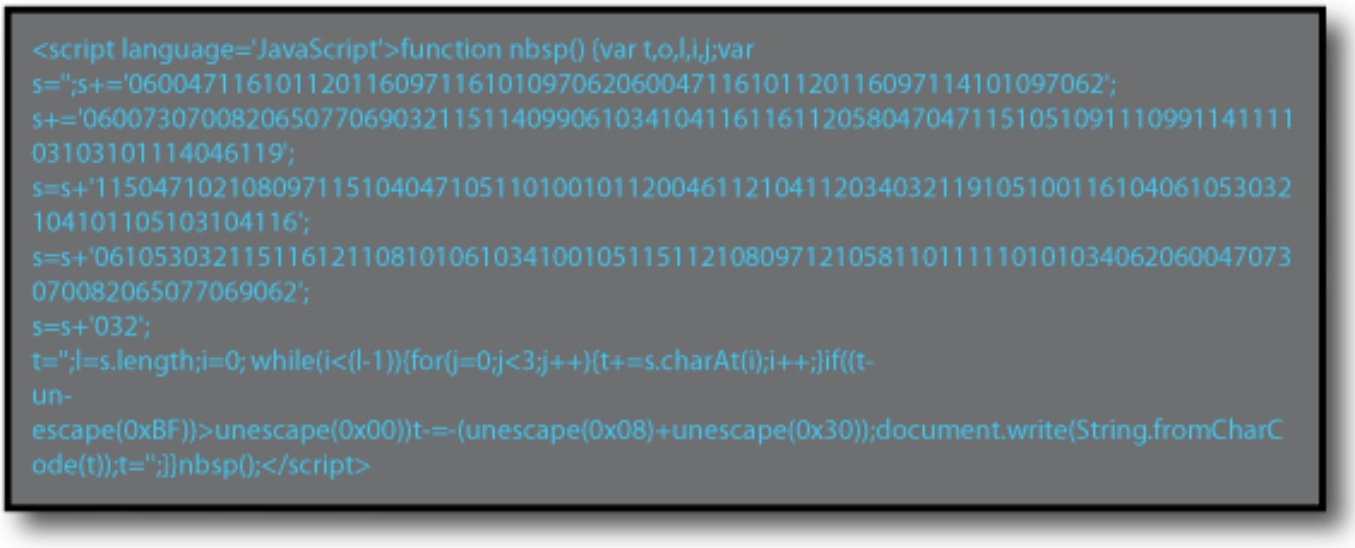
```
<iframe src="http://example.com/exp/forum.php" style="visibility: hidden; display: none"></iframe>
```

Iframes can create hidden links to other websites

Javascript is a kind of code that can be read by web browsers, and is used to add functionality to a site. Many popular websites and web-based applications depend on the use of javascript to work well. When used to distribute badware, javascript is often encoded or encrypted to make its malicious nature difficult to detect.

Not all encoded and encrypted javascript is bad, but it's a good first place to look if you suspect a website has been compromised. If you know what to look for, these blocks of code can be easy to spot. One common encoding technique for javascript creates strings of percent signs with two characters after them (e.g. %AA%BB%CC), and another creates strings that consist of "\u" with four characters after (e.g. \u0048\u0069\u0021). These blocks of encoded text can take up several paragraphs.

Encrypted code is harder to find, because there are no set patterns. However, encrypted code will look like a block of unintelligible text. Normal javascript uses a syntax based on actual English words. Encoded or encrypted text appears in a site's source code as completely unintelligible blocks of letters, numbers, and symbols.



Encrypted code appears as unintelligble text, symbols and numbers

Coding and encryption of javascript have their legitimate uses. For example, some developers use encoding to make it harder for automated programs to detect email addresses displayed on a site, protecting the addresses from spam harvesters. Unfortunately, not all encoding and encryption is easy to decode and check for potential harm. Many malicious hackers are now using advanced encryption techniques that are much harder to detect.

Third Party Content

Websites can also be compromised through the use of third party content. A common type of third party content is advertising provided by ad networks. In this kind of advertising, a website owner agrees to place code on their site that shows the ads provided by the network, in exchange for payment when visitors click on the ads. The website owner may have some control over which ads display on their site, but in general the ads themselves are chosen by the network. Most online ads include a link to a website for the advertised product. If one of the websites that is linked from an ad is distributing badware, the ad becomes a dangerous link on an otherwise benign site.

"Choosing to use third party content means inviting someone else to have control over part of your website"

Ads are one of many ways websites can use third party content. Many sites use independently hosted counters to track the number of visitors they receive. Some sites use decorative images or games that are provided by third parties and hosted remotely. If one of these counters or images is compromised, it can in turn compromise the otherwise innocent site that displays it.

In many cases, third party content is perfectly fine. Many providers of ads and other remotely hosted content take steps to ensure their products are safe. If you're a website owner considering using third party content, carefully research providers before placing their content on your site. Often other internet users and

webmasters will have information about problematic ad networks and other third party offerings. Choosing to use third party content means inviting someone else to have control over part of your website, and entrusting them with the security of the content they send to your site. Choose carefully, and stay vigilant, to help keep your site secure.

Timely Targets

The Miami Dolphins's website normally sees predictably steady amounts of traffic during the football season. When the Dolphins hosted the Super Bowl football championship game in January 2007, it created a temporary spike in visits from users who are considered high value targets by badware producers. In this case, those targets were people, predominantly American men, who were fans of both the Super Bowl and the online multi-player game World of Warcraft. Days before the big game, attackers infected the Dolphins's site with a trojan that installed keylogging software onto visitors' computers, allowing the attackers to spy on keystrokes and steal passwords. Stolen passwords to accounts on online games such as World of Warcraft can then be sold on the black market.

> "Even corporations with seemingly very secure networks can be susceptible"

It was no accident that the Dolphins's site was hacked so close to the date of the Super Bowl game, at a peak in the site's traffic. This ensured that the maximum number of victims was infected before the hack was detected and removed. The attackers in this case apparently discovered a previously unknown vulnerability in the website's code, which they used to gain access to the website's database and inject malicious code onto the site. Even corporations with seemingly very secure networks can be susceptible to this kind of attack.

One of the first cases that StopBadware encountered in the seasonal targets trend was an attack on a popular Santa Claus site in December 2006. The site becomes popular only during the Christmas season, when its sharply increased traffic makes it a prime target for badware distributors. The site was such a good target, in fact, that shortly after it was cleaned up it was attacked again. After the holiday passed, the site was no longer a target and likely will not be again until the next Christmas season.

The Dolphins's homepage was attacked before the Super Bowl

These attacks aren't confined to holidays and other calendar events, however. Another reason for a sudden jump in the number of visitors to a site is a link to that site from a prominent source such as a popular blog or news site. In one incident, a site that was linked to from the popular blog BoingBoing was then compromised, a maneuver colloquially known as "link jacking." While BoingBoing edited its post as soon as the attack was discovered, the link drew a huge amount of traffic to the compromised site, leading to an unknown number of badware infections.

One surprising source of time-sensitive attacks is the unfortunate side-effect of a positive and important security practice. When software companies discover security holes in their products and release patches to fix them, they trigger a flurry of activity among badware distributors. The patch is studied and reverse

engineered to reveal the underlying flaw the patch was designed to fix. It is then possible for an exploit to be designed specifically to take advantage of this flaw. The time period between a patch's release and its adoption by a majority of users of the affected software is ripe for attack. Attackers can then seek out web servers running unpatched versions of server software and take control, or design new exploits for unpatched flaws in popular web browsers.

Exploits can be created quite rapidly, much quicker than software companies can get the word out to all their users about an important new security patch. Many small website owners are not aware of the urgency and importance of updating web content management software they use, and allow their sites to go months, even years, without updated software. One WordPress blog software security hole that was patched in 2006 was exploited within 24 hours of the patch becoming public, yet even today some sites still run unpatched versions. And many internet users are not running up to date software on their own computers, from web browsers to anti-virus and anti-spyware protection.

Even Santa Claus's website was vulnerable

Dark Corners

We all know that walking down a dark alley alone at night can be dangerous. In the offline world, we know to avoid the physical places where illegal and barely-legal commerce and the crime that often follows with it takes place. While it may feel safer to visit these same kinds of spaces online, it's not much of a surprise that these "dark corners" of the internet hold more than their share of unpleasant surprises.

Serials, 'Warez' and Emulator Sites

When a piece of software costs hundreds of dollars off the shelf, there can be a substantial temptation to obtain it by illicit means. Why not simply download that same piece of software from the internet for free? Badware authors and producers capitalize on this temptation and use it to lure us into their traps. This "free" software is known in internet subculture as "warez," software that's traded in violation of copyright law. Warez can be downloaded from numerous warez-focused sites on the internet. It is very common to discover badware on your machine after visiting or downloading software from one of these sites.

Even if you obtain an illicit copy of software on CD instead of through a download, you will probably need a serial number or "key" to unlock the install files that actually put the software onto your computer. Some websites distribute the keys used to crack pirated software CDs. On many such sites, your path to the page containing the serial number key may include pages with drive-by download exploits. These sites are frequently updated with new exploits so even good virus and spyware protection may not completely protect you from becoming infected.

Another dangerous behavior is the use of serial key generators or "keygens." These are programs that can create serial keys for any number of software applications so that they can be used without paying for the original software. Using key generators is a little like playing roulette. They can install keyloggers that will record every keystroke you type on your machine and send your passwords and personal information to third parties. Again, having up to date protection may not keep you from becoming infected.

Some folks may fondly remember playing the video games of past years on classic systems such as Nintendo 64 or Atari. While the machines originally sold to play these games are no longer in commercial circulation, there are now sites where software is used to emulate the original hardware of classic video game systems. These sites are not condoned by the original copyright holders of the games involved, but until recently have not attracted attention outside a niche community of retro games fans. Mainstream video game producers have recently begun updating their older games to market them to new audiences, boosting the popularity of classic games. Some unscrupulous games emulator site owners are taking advantage of this increased public interest and are using exploits, false redirects and deceit to infect the machines of their sites' visitors. The promise of free entertainment has a hidden cost for users who end up with infected machines.

Pornography and Gambling

Many people remember seeing adult entertainment phone numbers advertised heavily on late night television. Users of these services generally dialed a number with a 900 area code and paid high fees for each minute they were connected. When StopBadware began our research in 2006, many pornography sites (especially those targeted to Americans but based outside the United States) installed software that caused the user's modem to dial a 900 number, claiming that their special dialer software gave users access to exclusive pornographic content. Users were lured by poor disclosure or simple deception into dialing and accepting the charges for these fee-based numbers. In extreme cases, dialer software could dial out to a 900 number even while the computer was unattended. As broadband internet access becomes more prevalent, the spread of deceptive dialer software is dropping off and badware providers are looking for new ways to capture money from those seeking pornography online.

Fake Video and Audio Codecs

If you are a fan of downloading video content from the web, then you may be familiar with the use of "codecs." Video and audio codecs are like a set of instructions your computer can use to allow you to watch and hear content. Suppose you have a file that contains something you want to watch, but it will not play on your machine. A quick internet search reveals that you need a specific codec to play the video. You do another round of searching and find a "codec pack" that says it contains the codec you need. Unfortunately, you don't know what exactly is contained within the software package. Trojans and adware can be found hidden in bundled software. When you download and run the package, you may be exposing yourself to badware.

Some codecs come bundled with badware

Similarly, websites that contain pornographic material may instruct you to download a plug-in codec to watch online videos. These can be false codecs that open up your computer's system to harmful software. Fake video codec sites often center on pornography, but these tactics could easily be used by any type of website.

Social Engineering

In the offline world, we know that not all crime takes place in the "dark corners." We need to be wary of scams and tricks, of people or businesses masquerading as something they're not. The same holds true online, in the crowded meeting places of social networks and in the shady business practices of spam and rogue software distributors.

Social Networking Sites

Online social networking is a fascinating phenomenon that's developed over the last few years, but like "dark corners" social networking sites need to be treated with caution. These sites are risky more because of their popularity than the specific types of social network technology involved.

Many features of social networking sites create easy opportunities for unscrupulous individuals to attempt to exploit your trust. Badware on these sites can be delivered through advertising, global and private messages and other means. A favorite method used by badware distributors is sending messages and "friend invites" from fake profiles.

You can catch these fake profiles before they do any damage to your computer by asking yourself a few simple questions before visiting a new profile or following links to another website:

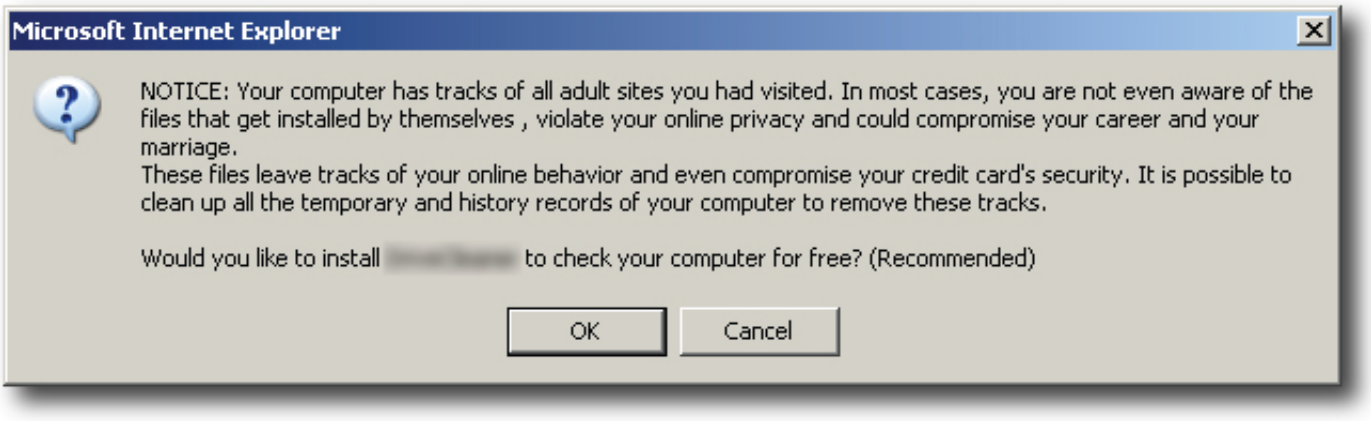
Look for clues that a profile may be fake before following links to external sites

- Is this message, invitation, or attachment from someone you don't know?
- If it is from someone you know, was the message, invitation or attachment unexpected?
- Does the profile try to lure you away to another site or "deal" that seems too good to be true?
- Is the user profile brand new with very few friends or not much personalization?
- Do the images on the profile appear to be too polished or glamorous to be real?
- Does the profile contain images in places where you'd expect to see text?
- Is some of the language of the message or profile incomprehensible?

If the answer to one or more of these questions is yes, be wary. Ignore the invitation, mark it as social network spam or have someone experienced with badware investigate further.

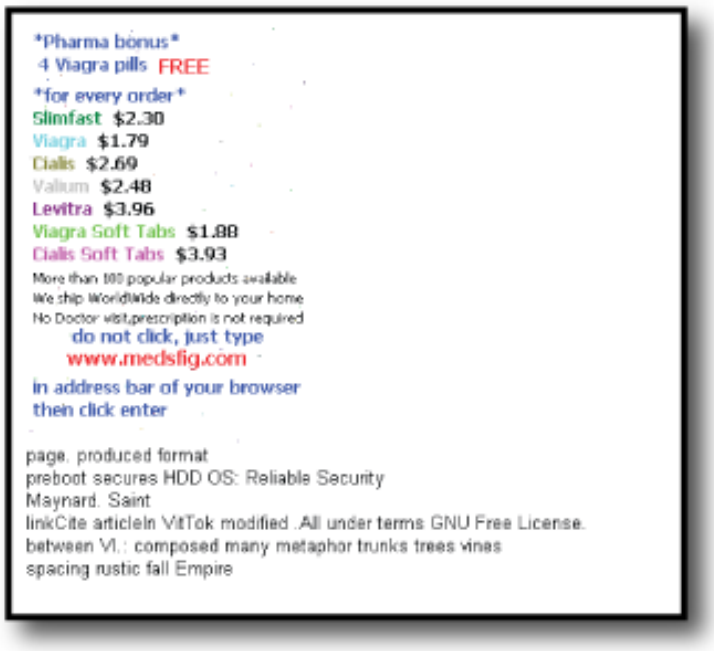
Rogue Software

Rogue computer programs are applications that pose as legitimate products with pictures of professional looking packaging and slick interfaces to trick the user into thinking they are doing something beneficial. This particular type of software can be especially predatory and deceptive. These products rely on fear and misplaced trust in the authority of computer "experts" and are not above resorting to extortion to separate you from your money or infect your machine.



Rogue software is often "advertised" through pop-ups disguised as error messages

Often a victim's introduction to this type of software begins with a website pop-up. This pop-up advertisement looks suspiciously like an error message from your operating system or from a legitimate anti-virus or anti-badware application. The message displays a frightening warning informing you that your system is in jeopardy due to spyware, malware, viruses or other causes. It encourages you to click the pop-up to scan your machine or to repair it. Starting this process will eventually lead you to downloading an application or a web browser plug-in that installs the rogue product on your computer, and your computer may also become infected with a drive-by download along the way.



Spam tries to drive traffic from email to websites

When you run the rogue application it may display misleading and exaggerated claims about problems it claims to have found on your computer. These claims generally will be repeated often every few minutes or every time you reboot your machine, unless you give in and purchase an updated or full version of the software. These annoying warnings can appear with pop-ups, system messages, and audible alerts that are quite alarming to the average user. This type of software tends to be difficult to remove and may make repeated threats to encourage you to purchase the software rather than proceed with an uninstallation.

Spam

The average email user is by now fairly well educated about spam and its common potential dangers. You can receive spam by having your email address posted on the web, signing up with your email address on a web site that gives away or sells your information, or by being in the email

"Be skeptical of offers that seem too good to be true"

address book of someone whose machine has been infected with badware.

Often spam is associated with phishing sites that attempt to fraudulently acquire sensitive information, but there can be other dangers to spam. Unexpected attachments can contain viruses, trojans and other types of badware that can directly hurt your machine. A newer threat is spam emails that try to trick you into clicking links to sites that host badware, including sites with drive-by downloads.

Badware producers use deceptive means to persuade you to forward spam messages to your friends and family by including jokes, inspirational messages, breaking news, or even virus warnings. A good email scanner can give you a certain degree of protection but will not catch everything. Be skeptical of offers that seem too good to be true, and be wary of clicking links sent with little information or from unknown senders. Keeping a watchful eye and educating yourself are your best protection against this type of attack.

Fighting Back

The current state of badware on the internet is troubling, but not without hope. In the past few years, badware grew from a somewhat fringe threat that primarily affected users who weren't doing enough to protect themselves, to a menace that can lurk on even the most innocent-seeming website. Internet users no longer need to be persuaded to visit a malicious website or to download a questionable application; infection can now be as simple as a visit to a normally trusted site.

The rates of infection are running high. Our Badware Website Clearinghouse, which features data provided to us by our partners at Google, has grown to around 200,000 currently infected sites, many of them innocent sites that have been compromised by attackers. If even a small percentage of computers used to visit these sites are themselves infected, there are vast numbers of compromised computers in homes and offices around the globe. Every infected computer is another potential tool for the criminals behind badware to distribute spam, attack legitimate websites, and spread the infection.

Internet users do not have to face this threat alone, however. There are numerous anti-virus and anti-spyware tools that can help protect computers from badware. And several companies, including StopBadware's partners, are working to expose compromised websites as they become infected so that users can avoid visiting them until the sites have been cleaned.

How can you protect yourself? No single tool or strategy is a perfect solution. There will always be new exploits that even excellent protection applications may not catch. The best defense is to update your software as quickly as possible whenever new patches are announced, whether it's for your

Tips for Staying Safe Online

- **Install anti-spyware and anti-virus software**

Using trusted protection applications and keeping them up to date is a good defense against many threats.

- **Keep your software up to date**

In many cases, updates to operating systems and browsers can fix vulnerabilities that are used by badware distributors.

- **Stay educated**

Sites like StopBadware.org offer public announcements, reports, and discussion groups to help keep consumers informed of current and potential threats.

> "No single tool or strategy is a perfect solution"

web browser, your website's content management system, or your computer's anti-virus and anti-spyware protection software.

StopBadware advises that internet users install multiple applications to protect themselves against badware, since one may catch what another does not. If you have already invested in a commercial solution there are many excellent free products available to supplement and enhance your existing defenses. Make sure that the software is up to date and scan your computer frequently to catch any recent infections.

In addition, many modern operating systems include a way to automatically install critical updates, plus a software firewall to increase your defenses. It's a good idea to turn these on and allow them to do their job. Many of the websites that can infect your machine rely on exploits that have already been patched. The only way your computer can become immune to those exploits is if the patches are installed. If a software firewall is turned on, it can block some malicious programs from accessing information on your machine.

> "You can help us fight back"

StopBadware is working on more ways for the internet community to fight back. We have a thriving discussion group for everyone from newbies to techies to help each other and discuss the best strategies to deal with and prevent infection. And we're planning even more exciting ways for folks who love the internet to band together, like forums where you can post about sites or software you've found to be suspicious and get help from others.

Badware is a serious problem, and with its deep roots in the criminal element it's not going to disappear easily. StopBadware aims to use the power of the diverse and connected internet community to help stop badware in its tracks. You can help us fight back by spreading the word about badware and its prevention, or by joining our community of users. Together, we can help make the internet a safer place.

StopBadware.org is a research initiative and community-based campaign against badware, run out of Harvard Law School's Berkman Center for Internet & Society in collaboration with Oxford University's Oxford Internet Institute. StopBadware has received funding support from several prominent technology companies, including Google, Lenovo, PayPal, Sun Microsystems, and VeriSign. Consumer Reports WebWatch serves as an unpaid StopBadware advisor.