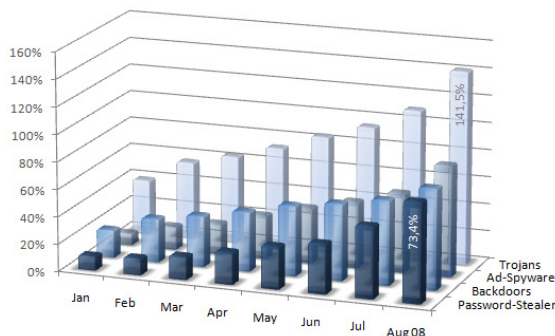


The State Of Malware – Summer 2008

The Internet today provides endless wealth of information, education and entertainment. Connection to the Internet is a need that all corporations now have. In fact, a *safe* connection is a business-enabler.

Where there is money, the bad guys quickly follow. A barrage of new types of malware and attack methods – all with focus on financial gain – is continuously unleashed on PC users and corporations. Password-stealing malware, for example, has grown by more than 70 percent in just one year.



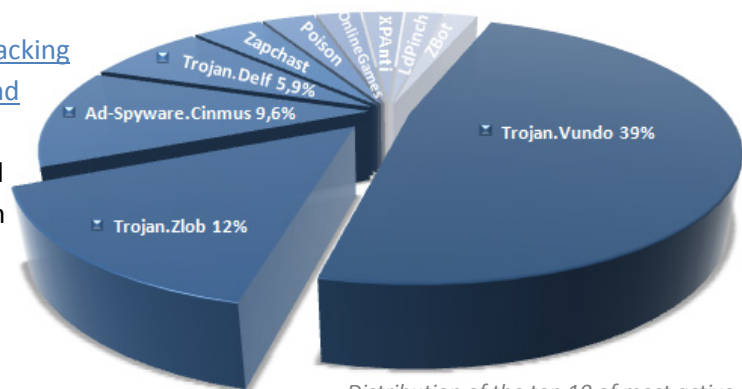
Growth of malware types by new unique variants, relative to the state in August 2007.

Attackers also continue to be creative in finding new attack vectors and target platforms. For example: brute-force [attacking of popular routers](#), [infection of audio and video media files](#), and [malware for the MacOS X platform](#). And the widespread compromise of legitimate Websites—an issue ascribed to the year 2008—continues to negatively affect users.

Looking at the top 10 most active and evolving malware families, the

roster continues to be headed by the infamous [Vundo](#) and [Zlob](#). However, from June through August the [ZBot](#) spyware family has been rapidly closing the gap, with a growth rate (i.e. the amount of unique new variants) of 103 percent in only two months. ZBot – also known as “Wsnpoem” – surreptitiously downloads an encrypted configuration file to users’ PCs; this contains further instructions from a Russian server and sends stolen data back “home” through HTTP POSTing.

The Secure Anti-Malware Engine can help in two ways here: (1) first, the malware itself can be blocked as “Trojan.Spy.ZBot” immediately; (2) and second, mobile computers that may have been infected while a user was on the road (i.e. outside the protection of the corporate network protection such that when they re-enter, they may be identified as infected through “Potentially Unwanted Program” heuristics) can be quarantined or blocked until cleaned.



Distribution of the top 10 most active, evolving malware families (by new unique variants)

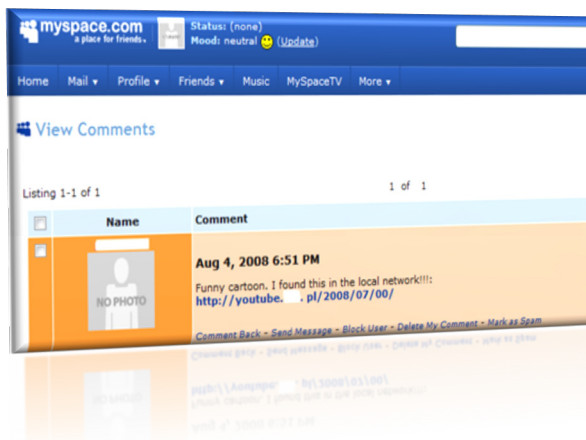
New Worm Hits “Web 2.0” Sites

In early August, a new worm began propagating on the popular social networking Websites *MySpace* and *Facebook*.

This worm misuses the functions of these popular networking sites, posting comments and sending messages to the friends in your contact list, like this:

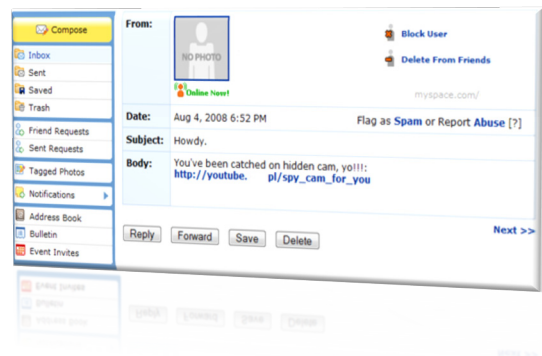
- “Paris Hilton Tosses Dwarf On The Street”
- “OMG!!! This is you on hidden cam”
- “You must see it!!! Funny video clip”
- “Funny cartoon! I think it’s FAKE!! What do you think about this?”

The message lures recipients to click a link that leads them to the malicious Web site, where the worm infects them. Here is an example of a comment generated by the worm:



Users who click to see the funny videos are actually redirected to a fake YouTube-lookalike page. The user is informed that their version of Flash Player is out of date. A file called “codecsetup.exe” – which is in fact a copy of the worm itself – is presented as a fix. If the user falls prey to this common social engineering trick and executes the worm, the whole malware spreads. The worm uses variants that target either MySpace or Facebook.

It automatically sends personal messages directly to all your contacts. This is what the message looks like to the recipient:



The worm then contacts a server in the Czech Republic with an HTTP POST request to obtain further instructions. In so doing, the malware authors can adjust the actions, links and comments posted by the worm.

For example, if the fake codec domain is terminated or blocked, the malware authors can instruct the worm to point to a new malicious location in subsequent messages and comments. After the new instructions are received, all new friends of its victims will receive messages showing the updated malicious destinations.

This worm – currently targeting MySpace and Facebook – shows us that in today’s Web 2.0 world one cannot trust any content...even that coming (allegedly) from your friends.

As has been known about Email messages for years, social network messages and their sender addresses can also be forged, pretending to come from your personal contacts, but, in reality, being forwarded by malicious software instead.

The Secure Anti-Malware Engine blocks this threat proactively as “Trojan.Downloader.Gen”.

Compromise Of Legitimate Websites

2008 – The Year of SQL Injection

Since April, a dramatic increase in [SQL Injection](#) attacks against Web applications has taken place. A run of SQL injection attacks has occurred nearly every week, infecting legitimate Websites and directing visitors straight into the hands of malicious code. The attackers often use SQL injection against ASP and ASP.NET Websites that insufficiently verify user input.

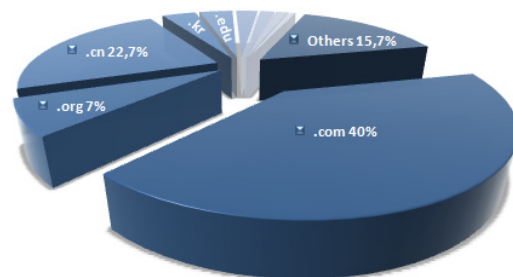
In one such instance, for example, more than 240,000 compromised Web pages had been serving exploits for a dangerous code execution [vulnerability in Flash Player](#).



Attackers usually attempt to include malicious script references in Web pages that are stored in [Content Management System] SQL databases.

The first attacks were observed from China as attempts to push password-stealers for online games. Later in the year, the “Danmec” (also known as “Asprox”) botnet joined the SQL injection onslaught. Infected computers were instructed to perform automated SQL injection attacks, but also host the malicious exploit toolkit pointing to infected sites. As with the Storm worm botnet, domains are

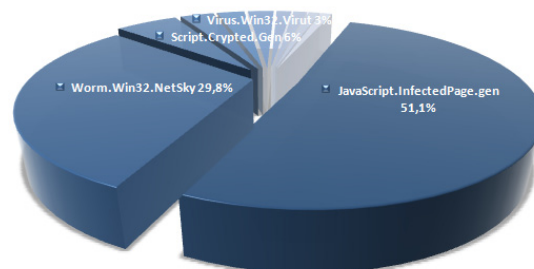
hosted on the botnet itself and leverage [Fast-Flux](#) techniques.



Top 10 Top-Level Domains by number of infected Web pages. "Others" are .net, .biz and similar.

As unsuspecting users surf to previously legitimate Web pages that now contain a malicious script reference, their browsers will load the malicious code from the attackers' server, which then tries to leverage vulnerabilities and turn the visitors into new [unaware] members of the botnet.

Of the more than one million Web pages infected through SQL injection worldwide, as of mid-August over 22 percent of them belong to the Chinese top-level domain. Another 3.7 percent are education (.edu) sites. In the distribution of most prevalent malware families, infected pages account for more than half of the top 10.

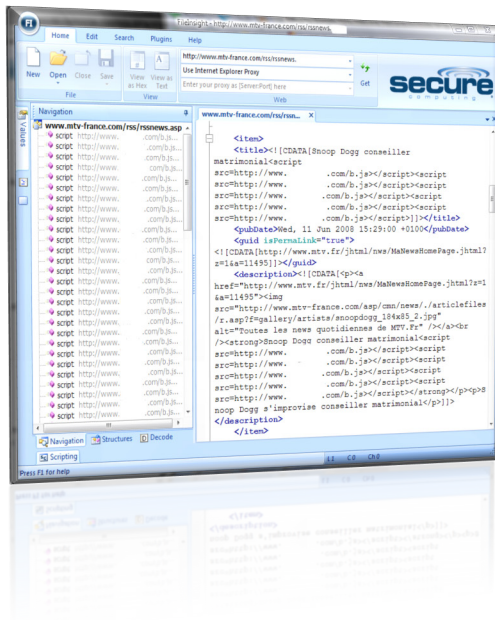


Distribution of the top 10 most prevalent malware families as of August 2008, both Web and Mail.

And infections spare no file formats. Even Cascading Stylesheets (CSS), intended to define nothing more than the layout and design of Websites, are increasingly used to host malicious code. For details, we recommend “Websites face new threat from hijacking blogs” in the August issue of ComputerWeekly (also available [online](#)).

Infected Lifestyle Site and RSS Feed

When a major music television channel's Website fell victim to a SQL injection attack, not only did the site's Web pages get infected, but its RSS feed as well.



The biggest concern with infected RSS feeds is that every RSS reader or Web site (including the content) will host the malicious scripts on their Web sites as well, unless the malicious script references are filtered out. Older WordPress installations, for example, do not filter anything and the full content including the script would be aggregated into any such WordPress blog. This is one example of the threat posed by Web 2.0 content mash-ups, where sites include pre-generated content feeds and unknowingly spread malicious code further.

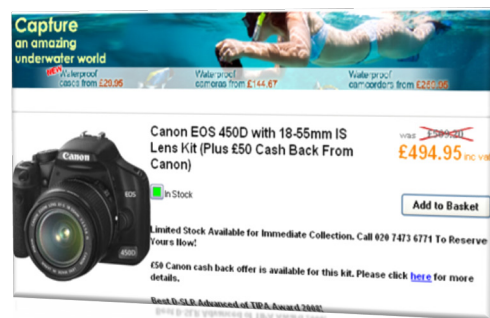
Compromised Shopping Site Serves Zero-Day Exploit

Sometimes, bargain shoppers get more than they bargained for...

In early August, a popular UK-based e-commerce site was infected with malicious

content. As is typically with Web 2.0 threats, site visitors wouldn't recognize anything unusual or suspicious at all. Only a closer look by a professional into the actual HTML source code would reveal an infection.

But these attackers managed to include a malicious and invisible IFRAME into the Web site. So the surfer looking at the latest gadgets like MP3 players, digital cameras and other goods, ends up unknowingly following the IFRAME, causing their browser to include the malicious code.



In this particular case, an IP address from the United States would present the browser with obfuscated script code. A closer look into the malicious code reveals that the malware authors tried to leverage the recent Zero-Day vulnerability in the "ActiveX Control for the Snapshot Viewer for Microsoft Access" ([MS 955179](#)). The Zero-Day would then be used for a drive-by infection with a password-stealer, which, among others, looks for Yahoo! credentials.

The Secure Anti-Malware Engine proactively blocks the infected Web site as "Script.Infected.WebPage.Gen". So, regardless of whatever new vulnerability finds its way into an attacker's arsenal of exploits, risk is mitigated and blocked immediately.

New Platforms And Attack Vectors

Multimedia Malware

In early July, a new Trojan began spreading in the wild, infecting multimedia files on victims' hard drives with malicious content (also see Dark Reading's *"Trojan Attacks Multimedia Files Stored on Hard Drives"* [online](#)). The malware embeds a malicious command into multimedia files based on the Advanced Systems Format (ASF), as widely used for video and audio content such as Windows Media Audio (WMA) music files and WMV video files. In addition, the Trojan also takes all a user's MP2 and MP3 files (MPEG-1) and converts them to WMA files first, prior to infection. The more or less meaningless ".mp3" file extension remains unchanged, so users don't notice the infection.



The victim of this first stage may subsequently exchange MP3s or WMV videos through a peer-to-peer file sharing network, where other users may download the infected audio or video files. However, when trying to play back the infected files, Windows Media Player will automatically open the default browser and redirect them to a malicious resource on the Web. The user is then fooled into believing a codec would be needed to play back the content and when downloading it, they instead end up installing a password-stealing Trojan.

Users downloading content from P2P networks need to exercise caution at all time, and should also be sensitive to pop-ups

appearing upon playback of a downloaded video or audio stream.



The Secure Anti-Malware Engine proactively blocks the Trojan as "Heuristic.Crypted" and also generically blocks any multimedia file infected by the Trojan as "Trojan.ASF.Hijacker.gen".

Trojan Attacks Routers

A new variant of the DNSChanger Trojan was released into the wild in June. It conducted brute force attacks against the Web interface of routers that use basic access authentication. This latest Trojan's aim is to gain access to routers in order to change the DNS settings to point to a host address supplied by the attackers. The devastating effect is that any DNS query coming from within that network and passing through the cracked router is under control by the attackers. Even users whose machines are not directly infected by DNSChanger itself might then receive malicious content injected when visiting their favorite legitimate Web sites, which they trust and believe to be clean and safe.

The Trojan uses a list of hard-coded credentials (“dictionary attack”) consisting of known default passwords. This poses a great security risk for users that do not change their router’s factory default settings. The Trojan tries one combination per approximately 100 milliseconds, which comes to 600 combinations per minute.

Once DNSChanger has successfully cracked the credentials via brute force, it has access to all the settings and functions provided by the router. The new DNSChanger variant knows about a few popular router Web interface URLs that the Trojan uses to change the DNS settings. An obvious sign of infection is that non-existing domain names are resolved by the DNS server, and changed or added by the malware. In fact, the rogue DNS servers, which are located in the Ukraine, will resolve any domain name you provide.

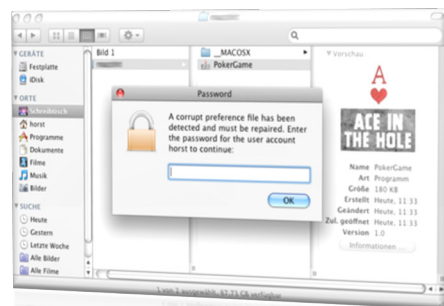
The behavior is entirely controlled by the attackers’ DNS servers. For example, friendfinder.com is known to be a target of malicious redirection. The attackers can resolve any existing domain name to servers hosting crafted content (phishing) or servers dynamically modifying real content. Once your DNS settings are under control, the possible negative effects are nearly limitless. Even clean machines are affected, once a previous infection on just one client behind the shared router successfully cracks the router login.

Spotlight on MacOS X

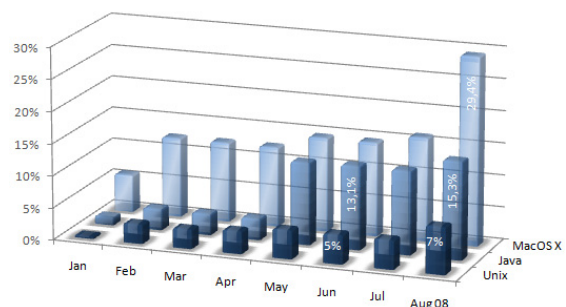
A newly discovered Zero-Day vulnerability in Apple’s Remote Desktop application again attracted malicious code writers’ attention to the MacOS X platform. The privilege escalation vulnerability that allows locally logged-on users to run shell scripts as “root” was exploited by a first Trojan (“AppleScript.Hovdy.A”), which, among other

things, adds new admin accounts to the system.

Another new MacOS X Trojan (“AppleScript.Hovdy.B”) masquerading as the poker game “Ace in the Hole” seems to be coming from the same author. The Trojan displays a fake error message to users asking for their real password as the Trojan pretends to require this in order to fix a corrupt file—a classic social engineering trick.



Along with the actual system’s IP addresses (local and public), the victim’s user name and root password are first encrypted using a simple substitution cipher and finally emailed to the remote attacker. This new Trojan makes use of the Secure Shell (SSH) protocol, enabling it on compromised MacOS X computers and then allowing remote access for the attacker via SSH.



Growth of malware for alternative platforms, by new unique variants, relative to the state in August 2007.

The number of unique malware variants for the MacOS X platform has accordingly seen a significant increase – up 29 percent in one year. However, compared to malware on the Windows platform, it’s still marginal.

New Zero-Day Vulnerabilities Exploited In The Wild

Around July's "patch Tuesday," two new Zero-Day code execution vulnerabilities for certain versions of Microsoft Office started being exploited in the wild. Attackers were exploiting the lag time in patch shipping.

The "Vulnerability in the ActiveX Control for the Snapshot Viewer for Microsoft Access Could Allow Remote Code Execution" (Microsoft Security Advisory [955179](#) published July 7th) was exploited first through infected Websites pointing to a malicious server hosted in Russia that was carrying it.

Exploitation of this vulnerability in the wild was blocked proactively by the Secure Anti-Malware Engine as "JS.CodeUnfolding.gen" and others call it "Packed.JS.Agent.p." Proof-of-Concept code to exploit the vulnerability also became publicly available on the Internet.

A second new vulnerability, "Vulnerability in Microsoft Word Could Allow Remote Code Execution" (Microsoft Security Advisory [953635](#) published July 8th) was exploited in the wild at the same time. The Secure Anti-Malware Engine proactively blocked it as "Exploit.Win32.Ginwui.gen", and others called it "Trojan-Dropper.MSWord.Agent.cq" or "Troj/MalDoc-Fam."

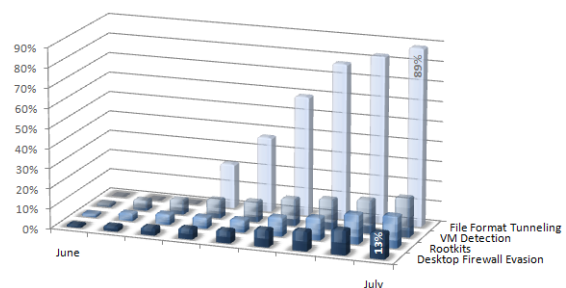
Trends in Malicious Techniques

Rootkits and Stealth Behaviors

Rootkit technology by now is incorporated into many of the most notorious malware families. Rootkit techniques include hiding of files and registry keys that belong to the malware, to the latest and most sophisticated rootkit known as "Rustock.C".

Other methods of stealthy malware operation have become mainstream. One example is the evasion of Desktop Firewalls. This technique can be found in many general-purpose Trojan downloaders today.

In order to circumvent firewall alarms, these Trojans inject their code into processes such as *Internet Explorer*, *Firefox* or *MSN Messenger*, performing network activity from within these trusted applications and processes. Another approach is to misconfigure the targeted firewall to allow the application before starting any network communication.



Relative growth in the usage of rootkit- and stealth techniques, in the month June and July.

Just as attackers don't want to be detected by affected users, they also want to make analysis by security researchers as difficult as possible. To do so, the presence of Virtual Machines – often used for a first analysis – is usually detected by today's malware, which behaves unobtrusively thereafter.

The [Vundo Trojan](#) has recently added the ability to remotely detect the presence of a Virtual Machine. It does this by transferring the "C:\\" drive's hard disk serial number – which is bound to particular manufacturers (such as VMware) – to its servers located in the Netherlands. If blacklisted ranges of serial numbers are detected on the remote site, the malware is then told to *behave* and not show any signs of actual intent.

File Format Tunneling

Rootkit techniques, desktop firewall evasion and Virtual Machine detection have already become mainstream. The new file format tunneling techniques that entered the scene in June have already seen a tremendous increase (see chart above).

General-purpose downloaders, such as for the “Mezzia” Trojan family, have begun to download what appears to be on first glance nothing more than a graphics file—a valid image that can be displayed without problem. The actual malicious payload is appended as custom data to the image, and extracted at runtime by the downloader. Content-based anomaly detection is also hindered by using compression for the payload, similar to the hosting graphics format. No significant anomalies can be determined based on information entropy; for example, both alleged and benign images appear compressed at similar quality.

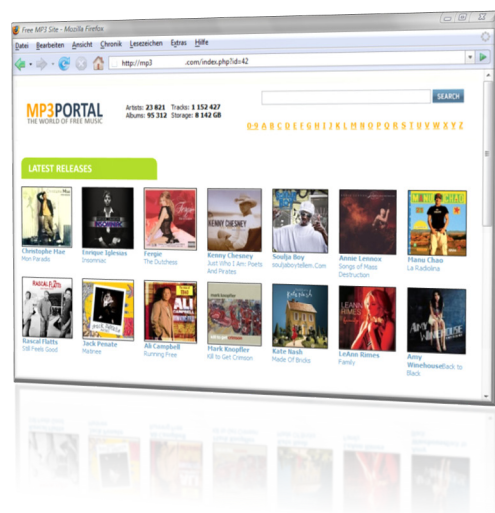
By end of July, another such mash-up technique, called “[GIFAR](#),” has been unveiled as a potential attack method for uploading Java applets to social networking sites, auction sites and others that normally do not allow upload of active content. By appending the Java applet archive (JAR) to a GIF image, the upload would not be blocked based on the trusted MIME type. But when visiting the site that embeds this hybrid GIF and JAR file later on, the user’s Java environment would execute the Java applet due to a design flaw in the ZIP file format (on which JAR is based).

Social Engineering

The most frequently seen social engineering trick, and obviously still successful unfortunately, remains the “missing codec”

trick. The attackers first lead users to sites seemingly offering adult content – often crafted as fake YouTube-lookalike portals – but when the visitor tries to play any of the videos, a message tells them the video codec is missing and needs to be installed first. We have not yet seen an incident where the codec offered did not turn out to be malware.

The phrase “Where There Is Porn, There Are Zlobs” is still applicable today, but adult-related themes are also being extended to music, offering free MP3’s.



Users visiting Web pages like the one shown here are presented with music albums, and informed they can download individual tracks. In fact, this is a downloader for the Zlob malware, and no music is provided at all.

The files downloaded have a double file extension – for example “<something>.mp3.exe” – and as per Windows default settings, known file extensions are not displayed in Windows Explorer. Even the icon of the malware executable was crafted to pretend to be a media file. If users don’t take caution, they can easily run the malware by double-clicking a fake MP3 file. As a basic computer “best practice” it’s best to stay away from potentially dodgy “free” offers, like MP3 portals that you aren’t already familiar with.