



Global threat report

June 2010

Feature Article: Drive-by Surprises in
Cyber-Gangsta Land



Table of Contents

| | |
|---|---|
| Feature Article: Drive-by Surprises in Cyber-Gangsta Land | 3 |
| AMTSO Under Pressure | 4 |
| The Top Ten Threats | 5 |
| Top Ten Threats at a Glance (graph) | 9 |



Feature Article: Drive-by Surprises in Cyber-Gangsta Land

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

How many times have you heard someone say “I’m not worried about getting drive-by viruses, I don’t go to dodgy sites”? So what’s the deal with drive-by downloads anyway?

The term “drive-by download” is more-or-less interchangeable with “drive-by install” so in principle any installation of malware through websites, e-mail messages, deceptive pop-ups, etc, can be regarded in a sense as a drive-by when it means that the victim is unaware of the download and didn’t expect or agree to it. But in its general meaning, it refers mainly to downloads and installations of malware from websites. Quite often drive-by malware is installed alongside user requested downloads, or as a condition for users to access certain sites or services (most often pirated software repositories).


So, dodgy or not? That is the main question then. Research gathered in the last two years claims that four out of every five websites that have been found to be infected with drive-by malware, belonged to innocent companies or individuals, completely unaware that they’ve been hacked and infected with malicious code.

ESET Ireland had a very recent and rather interesting experience with hacked sites. Our media clipping agency kept sending publishing alerts from some local agricultural website. Surprised that they’d mention ESET so often, I took a closer look at their website, and although there was no mention of ESET on it, the html code of the site included a bunch of lines advertising

“free software downloads”, including ESET software. Not, of course, legitimate free downloads to the product, but something you certainly wouldn’t want on your hard drive. I wouldn’t call this a drive-by in itself, but more a way of driving traffic to an unsavoury site using illicit Search Engine Optimization (SEO) techniques injected without permission into an innocent site. This is very indicative of the low-level general unawareness of such occurrences. When we contacted the company concerned, of course, they had no idea there was anything wrong with their website.

According to various sources, 10% to 20% of all websites are infected and will try to install drive-by malware. They do this by targeting various vulnerabilities in potential victim systems, but the owners of these systems may vary widely in how careful they are about updating systems and software, and this has a major effect on the levels of damage they can actually achieve. Clearly, a consistently patched system is far less vulnerable than a PC owned by someone who is careless about applying updates. Nearly all of the sites that contain these drive-by attacks include or are retrofitted with so called “exploit packs.” These are kits designed to probe the visitor’s browser for known security vulnerabilities (Eleonore, Justexploit, Yes, Fragus, to name a few). According to research, the most vulnerable browsers are older versions of Microsoft Explorer. For instance, Mozilla’s Firefox vulnerabilities result in about 1/3 of the exposure that Microsoft Internet Explorer version 6 does. The applications most susceptible to attack are Adobe Reader, Sun Java, Internet Explorer and Adobe Flash. As most online users utilize at least one or two of these at some time, the chance of infection is ever present.

Many drive-by programs - particularly those propagated via the recently notorious Koobface route - are installed from so-called “.sys” directories of various websites, prompting the user to



install additional components or “upgrades” to their system or browser, in order to allow access to the website’s data. The choice of names such as “.sys” serve to additionally reassure the non-tech savvy user into believing he’s dealing with regular and legitimate system updates. So, just blocking the web traffic from conspicuously misused names such as “.sys”, “system”, etc, can significantly decrease the chance of infection.

According to ESET Research Team’s very own Pierre-Marc Bureau, ESET Antivirus has a specific scanner for web traffic and does stop network traffic to known malicious websites (and Pierre-Marc is himself in charge of part of the back end system ESET uses to gather and maintain the malicious websites data). But if the volume of malware samples obtained daily by the ESET lab (anything up to 200,000 or more in a day, nowadays) is anything to go by, keeping on top of the massive numbers game of malware generated versus anti-malware detections, and thus monitoring the appearance and spread of infected websites should prove another serious challenge.

Namely, it’s the stealthy nature of website infections and therefore user infections, that appears to be the greatest obstacle. Websites are unaware they’re hosting drive-by malware, since it is not (usually) really doing anything directly hurtful to their system. Users are unaware of getting infected, since most of the time the only observable symptom is minor slow-downs of their computers. What is the purpose of the cybercriminals behind the infections? Mainly, it is to integrate infected computers into botnets which are then used for their dirty work such as massive spam runs or coordinated attacks on specific targets. Well, for the infected guy, as long as nothing shockingly terrible is happening to him, he hardly notices or cares that he may be sharing the use of a zombie PC with some remote botnet administrator.

But to return to the statement I made in the beginning, perhaps

the guy avoiding “dodgy sites” is right after all. As the recent ESET’s Blog by Randy Abrams reveals


<http://www.eset.com/blog/2010/06/11/161-84-to-infect-20000-users>),

“researchers spent \$161.84 to have approximately 49,000 visitors directed to their adult web sites. As visitors arrived, the research adult web sites would check to see if the browsers had current versions of the Adobe Flash plugin, the Adobe PDF plugin and a Microsoft Office plugin. All of these plugins have had remotely exploitable vulnerabilities. The researchers discovered that over 20,000 of their visitors had at least one outdated plugin, which means that these visitors are easy victims for drive by infections.”

What to do then? As with all IT security related issues, recognizing the problem should be the first priority, then keeping all and especially third-party software regularly patched and updated against vulnerabilities, then using common sense and not confirming pop ups that prompt for allowing additional “components” to install, and lastly perhaps really considering which neighbourhoods to visit online, and which best avoid. Of course, a good antivirus program will stop many of the malicious programs that a driveby tries to install in its track, but even the best security software can’t catch everything, and it’s not sensible to assume that because you have good security software, you never have to think about your own actions.

AMTSO Under Pressure

June saw a good deal of action on the AMTSO (Anti-Malware Testing Standards Organization) front, according to David Harley, ESET’s Sr. Research Fellow and a Director of AMTSO.



The announcement that two more guidelines documents had been approved by the membership and been added to the organization's documents page at <http://www.amtso.org/documents.html> generated a lot of media interest.

- The paper on AMTSO Whole Product Testing Guidelines (<http://www.amtso.org/amtso---download---whole-product-testing-guidelines.html>) is important because most tests focus only on simplistic detection rates, in some cases actually disabling part of the product's functionality in order to isolate a single protective layer. "Whole Product Protection Testing Guidelines" advocates a more balanced look at the effectiveness of products, taking into account multiple layers of detection and protection.
- The paper on AMTSO Whole Performance Testing Guidelines (<http://www.amtso.org/amtso---download---amtso-performance-guidelines.html>) addresses an issue where irrelevant metrics are over-emphasised by the implementation of poorly-conceived benchmarking methodologies. In such a case it's as easy to bias a performance test as it is to bias a detection test.
- In addition, four major research papers have been added to the testing-related resources page at <http://amtso.org/related-resources.html>. All four papers, presented at recent high-profile security conferences, discuss testing methodologies that are a better reflection of the real world.

However, we've been seeing a lot of negative publicity. Surprisingly, while everyone expects the anti-malware industry to be accountable to the testing industry as representing the

customer's interests, many people have a problem with the idea that a tester might also be accountable to the customer, and even more so that a coalition of testers and vendors (funny how many people choose to forget that testers are represented in AMTSO as well as vendors) might, as a group, also represent the interests of customers. The waters have been muddied further by the controversial claims of a testing organization, formerly a member of AMTSO, to be the only testing organization conducting real world testing.

It seems that there is an absolute mistrust of the security industry in general and the anti-malware industry in particular, whereas the media are much readier to abandon critical thinking when examining and recycling a tester's claims. Highly-rated security blogger Brian Krebs wrote a fairly balanced piece, though he referred to us as "cantankerous" and also forgot to mention that we're not just a group of vendors. The AMTSO Board put together a response to Brian's article which I quoted more or less in full on the AMTSO blog at <http://amtso.wordpress.com/2010/06/29/brian-krebs-on-av-testing/>. However, it seems likely that this debate will continue well into July.


The Top Ten Threats

It probably comes as no surprise that Conficker is once again the top-ranking threat, though perhaps it should, given the age of the extant versions. INF/Autorun continues to be prevalent, even though it's now fairly easy to disable the default setting that makes this attack possible.

1. Win32/Conficker

Previous Ranking: 1
Percentage Detected: 9.79%

The Win32/Conficker threat is a network worm originally



propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC subsystem and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lang=en.

What does this mean for the End User?

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at <http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx>. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: <http://www.eset.com/threat-center/blog/?cat=145>

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these

commonsense precautions. However, the Conficker Working Group estimates that there are still over 6 million infected machines out there.

2. INF/Autorun

Previous Ranking: 2
Percentage Detected: 6.57%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

What does this mean for the End User?

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (<http://www.eset.com/threat-center/blog/?p=94>; <http://www.eset.com/threat-center/blog/?p=828>) to disable the Autorun function by



default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at

<http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun> useful, too.

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 4.26%

This is a family of Trojans used in phishing attacks aimed specifically at game-players: this type of Trojan comes with keylogging and (sometimes) rootkit capabilities which gather information relating to online games and credentials for participating. Characteristically, the information is sent to a remote intruder's PC.

What does this mean for the End User?

These Trojans are still found in very high volumes, and game players need to remain alert. While there have always been unpleasant people who will steal another gamer's credentials just for the heck of it, trading in virtual cash, treasure, avatars and so on is now a major source of illegal income for cybercriminals. It's also important that participants in MMORPGs (Massively Multi-player Online Role Playing Games) like Lineage and World of Warcraft, as well as "metaverses" like Second Life, continue to be aware of the range of other threats like griefing ranged against them. The ESET Research team considered gaming malware in detail in the ESET 2008 Year End Global Threat Report, which can be found at [http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport\(Jan2009\).pdf](http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf)

4. Win32/Agent

Previous Ranking: 4
Percentage Detected: 3.25%

ESET NOD32 describes this detection of malicious code as

generic, as it describes members of a broad malware family capable of stealing user information from infected PCs.

To achieve this, the malware usually copies itself into temporary locations and adds keys to the registry which refers to this file or similar ones created randomly in other operating system's folders, which will let the process run at every system startup.

What does this mean for the End User?

This label covers such a range of threats, using a wide range of infection vectors that it's not really possible to prescribe a single approach to avoiding the malware it includes. Use good anti-malware (we can suggest a good product [\[2\]](#)), good patching practice, disable Autorun, and think before you click.

5. JS/TrojanDownloader.Pegel.BR

Previous Ranking: n/a
Percentage Detected: 2.29%

This is an obfuscated script that is injected into web pages. This script redirects to other web pages infected with IFRAME tag injection from which downloads and executes malicious code to the victim machine.

What does this mean for the End User?

Malicious scripts and iframes are a major cause of infection, and it's a good idea to disable scripting by default where possible, not only in browsers but in PDF readers. NoScript is a useful open source extension for Firefox that allows selective disabling/enabling of Javascript and other potential attack vectors.

6. INF/Conficker

Previous Ranking: 5
Percentage Detected: 1.47%

INF/Conficker is related to the INF/Autorun detection: the detection label is applied to a version of the file autorun.inf used to spread later variants of the Conficker worm.

What does this mean for the End User?

As far as the end user is concerned, this malware provides one more good reason for disabling the Autorun facility: see the section on INF/Autorun above.

7. Win32/Sality

Previous Ranking: 6
Percentage Detected: 1.40%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.

It modifies EXE and SCR files and disables services and process related to security solutions.

More information relating to a specific signature:

http://www.eset.eu/encyclopaedia/sality_nar_virus_sality_aa_sality_am_sality_ah

What does this mean for the End User?

This is a classic example of malware that uses a range of techniques (file infection, autorun infection, polymorphism, terminating known security software, drive enumeration) to give itself the best possible chance of infecting and surviving once it gets a foothold. It pays to ensure that your security software is still operational, as many malicious programs try to disable AV processes, and Sality's continued prevalence after

several years in the wild indicates that these strategies are pretty successful.

8. Win32/Qhost

Previous Ranking: 19
Percentage Detected: 1.16%

This threat copies itself to the %system32% folder of Windows before starting. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker. This group of trojans modifies the host's file in order to redirect traffic for specific domains.

What does this mean for the End User?

This is an example of a Trojan that modifies the DNS settings on an infected machine in order to change the way that domain names are mapped to IP addresses. This is often done so that the compromised machine can't connect to a security vendor's site to download updates, or to redirect attempts to connect to one legitimate site so that a malicious site is accessed instead. Qhost usually does this in order to execute a Man in the Middle (MITM) banking attack. It doesn't pay to make too many assumptions about where you are on the Internet.

9. Win32/Spy.Ursnif.A

Previous Ranking: 10
Percentage Detected: 0.93%

This label describes a spyware application that steals information from an infected PC and sends it to a remote location, creating a hidden user account in order to allow communication over Remote Desktop connections. More information about this malware is available at <http://www.eset.eu/encyclopaedia/win32-spy-ursnif-a-trojan-win32-inject-kzl-spy-ursnif-gen-h-patch-zgm?lng=en>

What does this mean for the End User?

While there may be a number of clues to the presence of Win32/Spy.Ursnif.A on a system if you're well-acquainted with the esoterica of Windows registry settings, its presence will probably not be noticed by the average user, who will not be able to see that the new account has been created. In any case it's likely that the detail of settings used by the malware will change over its lifetime. Apart from making sure that security software (including a firewall and, of course, anti-virus software) is installed, active and kept up-to-date, users' best defense is, as ever, to be cautious and proactive in patching, and in avoiding unexpected file downloads/transfers and attachments.

10. HTML/ScrInject.B

Previous Ranking: 22
Percentage Detected: 0.84%

Generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

What does this mean for the End User?

Malicious scripts and malicious iframes are a major cause of infection, and it's a good idea to disable scripting by default where possible, not only in browsers but in PDF readers. NoScript is a useful open source extension for Firefox that allows selective disabling/enabling of Javascript and other potential attack vectors.

Top Ten Threats at a Glance (graph)

Analysis of ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 9.79% of the total, was scored by the Win32/Conficker class of threat.

