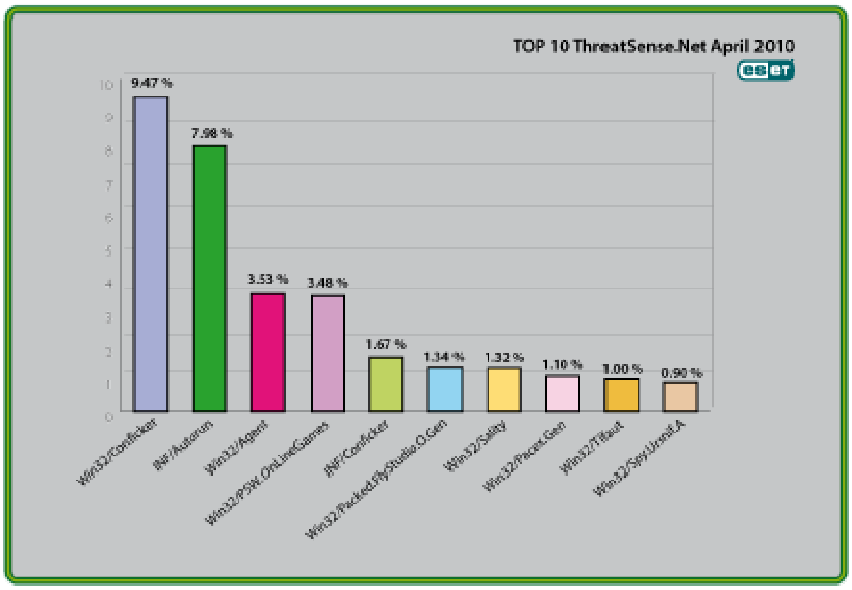
Global Threat Trends – April 2010

Global Threat Trends is a monthly report created by ESET that includes a review of the current events in the world of information security and the top ten threats of the month.

Table of Contents

Figure 1: The Top Ten Threats for April 2010 at a Glance



Analysis of ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 9.47% of the total, was scored by the Win32/Conficker class of threat. To read a more detailed review of the threats that made it to the top 10, go to page 7 of this report.

Changes to the Threat Report

In March 2010 we changed the format of this document, as we found that some people thought it was just a list of the top ten threats, which hasn't been the case for a long while. Of course, those data are still included, but we've moved them to the end of the document. As you'll see from the Table of Contents, this edition of the monthly threat trends report includes one or two further changes to the format and, more importantly, the content of the document.

We'd like to know what you think, though. If you have any thoughts on how the look and feel of the document could be improved, and what further changes you'd like to see to the content, we'd be very interested to hear about it. Please comment at http://www.eset.com/blog/2010/04/29/monthly-threatsense-report-what-do-you-think in the first instance.

Feature Article: How free is free Antivirus?

A number of tests recently seem to be intended to prove that free antivirus is as good as commercial AV, while Rafe Needleman tells us in a CNET report (http://news.cnet.com/8301-1009_3-20003722-83.html?tag=nl.e757) not to pay for security software. He's not the first commentator to suggest that it's somehow immoral to make a living out of programs that fight malware. (Presumably we should get proper jobs and program anti-malware applications in the evenings.) We don't think that Free AV is a bad thing, in principle, as long as it's used legally, and even more importantly, that users don't expect more from it than it can realistically deliver. In fact, ESET offers a free webscan service, though we wouldn't advise the use of such services as a substitute for a full-strength anti-malware program.

Here, Urban Schrott, of ESET Ireland, considers the issue. An expanded version of this article is available at http://www.eset.com/blog/2010/04/14/guest-blog-how-free-is-free-antivirus.

A while ago I encountered an article in a consumer magazine about "ten things you should never have to pay for" and antivirus software was listed as one of them. Their argument was simple: why pay for something if you can get it for free? The topic has already been discussed before, but perhaps we should revisit whether it is really the same (or equally effective) to use a free antivirus rather than a for-fee product?
First, we have to define the concept of "free". Most commercial security vendors also offer a "free" version of their software. It is usually of limited functionality when offered without a fixed time limit, while versions with full functionality are offered with a limited trial time, after which they normally become inactive. Many "free" products, for instance, offer free detection of malware, but require payment for removing it. Some offer "free" detection and removal, but only of certain types of malware. Those same vendors, however, also offer a "full" unlimited version of the software, for which a fee is (of course) payable.

Loss Leaders

In today's world, oversaturated with marketing, giving away a certain amount of product without charge is common practice, as it is good for brand building. Yet a brand is not built for the pleasure of seeing a product become more popular, but in the long run, to increase sales and revenue. The "free" tag on a time- or function-limited product is therefore just an introduction to the "full" version rather than a free service to computer users, out of the goodness of the vendor's heart. Much as we'd love to give our own products away, we have to eat, as do our wives, families, mistresses, aging parents, mortgage lenders and so on.

Then there are security suites supplied by the makers of operating systems. It could be considered a triumph of marketing over security, offering a "free" security suite which tries to graft security onto an operating system riddled with all those security holes that cyber criminals happily exploit, rather than building integrity into an operating system from the ground up. But also, is it really free if in essence it is just a value-add to an operating system you have already paid for in the first place?

Free But Fake

Reluctance to pay for security software can actually put you in danger. (For more on this, see Cristian Borghello's paper on "Free but Fake: Rogue Anti-Malware" at http://www.eset.com/resources/white-papers/Free_but_Fake.pdf.) Many outright fake, fraudulent and rogue anti-malware "products" advertise themselves as "free antivirus software". An unwary computer user searching the web for "free antivirus" can easily be diverted to sites of lesser virtue through SEO (search engine optimization: a range of techniques used by legitimate companies and cybercriminals alike to ensure that their URLs are highly placed in web searches). Once there, they are prompted to download harmful content, which is likely to result in the victim's losing money through fraud or extortion.

Efficiency and Functionality

A full security product nowadays is much more than just an antivirus product. A cyber criminal's main focus is on trying to find new ways to get in and do their dirty work, and they have the time and the resources to do just that. Threats therefore come in just about any imaginable shape and form.

Swimming the Channel

Malware is spread through many channels:

- By emails and other forms of messaging carrying malicious attachments or links to sites using drive-by downloads or social engineering to install malware such as fake codecs.
- Auto-infecting computers through the Autorun function, or via apparently innocent programs that download serious malware.
- Persistent randomized attempts to probe computer IPs for soft spots

Conclusion: The Price of Freedom

The development and maintenance of a comprehensive security solution requires skilled manpower, elaborate lab setups and top-of-the-range technology, and none of this comes free. This is something some testers tend to overlook, in their rush to make it look as though free security software is functionally on a par with full-blown commercial suites.

Important parts of the battle against cyber crime are strategic thinking and the development of new ways of combating threats. Detecting threats is one aspect, and one that is constantly being reviewed and upgraded. Moving on from the traditional "signature" type of virus definitions, we've seen the development of sandboxing, behavioural detection, heuristics, advanced heuristics, now cloud integration and so on.

As detection strategies have become more proactive, this has increased the need to maintain a careful balance between maximum protection and minimal false positives, effective disinfection, and non-viral attacks through channels that were barely thought about in the heyday of the virus in the 1990s. This entails complementary technologies such as intrusion prevention, anti-spam capabilities, website security, even the possibilities of social engineering attack prevention or limitation.

The debate about free or for-fee is really just a debate on how the sales model for any product is actually set up. For some classes of user (most often, home users), there may be such a thing as a (legitimately) free lunch* but people who lunch for free legitimately or not, may find that the meal is less nourishing than they expect.

At ESET Ireland we recently ran a poll on what people find most important in a security product. The choices were detection, footprint and price. High detection was chosen as the most important factor by most users, low footprint was considered as a useful feature, while price was hardly ever mentioned. This does suggest that users do have their priorities straight in what to look for in security software. If only certain journalists were less eager to cut corners, with spectacular announcements of wonderfully simple solutions to complex problems…

Urban Schrott
IT Security & Cybercrime Analyst
ESET Ireland
*There is no such thing as a free lunch: http://en.wikipedia.org/wiki/Tanstaafl

Infosecurity Europe and Apple Security

ESET was strongly represented at this year's expo at Earls Court, in London, where many photographers were observed taking pictures of the company's very impressive stand, taking particular interest in the Awards Wall and the ESET android, who seems to get bigger every year. All credit to our colleagues in the UK and Bratislava for making the exercise such a success. ESET LLC was also represented there in the person of David

Harley, who presented on "Apple, Security, and the Power of Perception" in the Business Strategy Theatre. A paper on the topic will be available shortly from the ESET white papers page at http://www.eset.com/documentation/white-papers, but here are some of the main points from the presentation.

- Viruses aren't a big problem nowadays on Macs *or* Windows, but that doesn't mean there are no security issues on *either* platform.
- A survey carried out by CERC (Competitive Edge Research and Communication, Inc.) recently on behalf of Securing Our eCity (http://www.securingourecity.org/) revealed that:
    - More people own PCs than Macs (but you probably guessed that), more people own PCs *and* Macs than own *only* Macs, and 2.1% of respondents didn't know what they own.
    - Nearly 10% of all groups think Macs aren't vulnerable at all. That's 16% of Mac users and 12% of PC users.
- Any computer user who believes that his system is so secure that he doesn't have to care about security is a prime target for social engineering attacks.
- The number of malicious programs targeting OS X is tiny, compared to Windows. But there are already more malicious binaries than there ever were pre-OS X viruses specific to that platform.
- Issues with jailbroken iPhones have highlighted weaknesses in the model of protecting smartphones using an application whitelisting mode, as testified by the escalation in exploitation of a single vulnerability from Proof of Concept code to multi-platform hacker tool to functional botnet.
- OS X's security model is better in conception than implementation
- The sky isn't falling, but even home users shouldn't take their security for granted.

David suggests that "if you want to give anti-malware a moment a miss at the moment because you're too bright to fall for social engineering Trojans, you're prepared to accept the relatively small risk in terms of volume, you aren't worried about 0-day self-launching exploits, and so forth, be my guest…But don't act on the unfounded assumptions that there is no Mac malware, or that only viruses matter." (http://macviruscom.wordpress.com/2010/02/04/is-there-such-a-thing-as-mac-malware/)

False Positives and SEO

David also mentioned to us that when he first arrived at Earls Court, he was greeted by the sight of a couple of guys in hoodies with a phrase parodying a famous line spoken by

Michael Caine in "The Italian Job". The front of the hoody read "You're only meant to blow the bloody *virus* up" on the back, and a pointer to McAfee's unfortunate update 5958 on the back. Very amusing, but while McAfee are our competitors, it wouldn't be appropriate to attempt to make marketing capital out of the incident (though one or two less scrupulous vendors did). While we'd all love to give you 100% detection and 0% false positives, the ever-shifting nature of the threatscape makes that impossible. Fortunately, most FPs affect only a few people, but if anyone tells you that their product couldn't be the cause of a widely publicized problem like this, ask to speak to someone with a clue. As David said in one of his other blogs (http://avien.net/blog/?p=503):

> "the measure of a vendor's worth isn't whether it generates a false positive, or whether it offers a convincing auto-da-fé before being burned at the stake on a fire fed by its own product packaging, but what positive act of remediation it responds with."

And there we would have been happy to leave it, had the fraternity of bad guys and malware author not seized upon the opportunity to deliver a massive SEO (Search Engine Optimization) campaign. For quite a while, using a search engine to hunt for information using a range of terms related to the issue would generate a huge quantity of hits on links that would redirect an incautious user to sites pushing fake antivirus programs. Eleven hits out of the first 20 were malicious with a set of search terms we used, as described at http://www.eset.com/blog/2010/04/22/mcafee-fp-news-misused-for-more-seo. We're all too aware that the bad guys will take any opportunity for a little destructive social engineering: the actions of spoilt celebrities, the worlds of sport and entertainment… They aren't squeamish about using ecological crises, plane crashes, or terrorist acts either. Still, we suspect that they get an extra kick at the chance to capitalize on the misfortune of one of the companies that make it more difficult for them to play their ugly games.

In fact, the blog on this topic continues a successful run of collaborations between the teams in Slovakia, Latin America and California in tracking and publicizing SEO poisoning and associated exposure to fake security software.

What Else is in the Pipeline?

David Harley, Andrew Lee and Pierre-Marc Bureau are also presenting another paper on Apple security at the upcoming EICAR conference in Paris (http://www.eicar.org/conference/2010/Eicar-Conference_2010_Agenda.pdf). Ján Vrabec and David Harley will be presenting a paper on performance testing at the same conference. Later in the month, ESET will be strongly represented at the CARO and AMTSO workshops in Helsinki.

Talking of AMTSO (the Anti-Malware Testing Standards Organization), a Virus Bulletin article by David Harley, who is a member of the AMTSO Board of Directors, is now available on the AMTSO website at http://amtso.org/documents.html. A number of new links have also been added to the ESET white papers page at

http://www.eset.com/documentation/white-papers, including "A Tried and True Weapon: Social Engineering" by Cristian Borghello, translated by Chris Mandarano, and "Re-Floating the Titanic: Dealing with Social Engineering Attacks" by David Harley.

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. While it's not reflected in the top ten figures, there's a notable spike in detections of the EICAR test file, which suggests that someone is doing an astonishing amount of testing…

1. Win32/Conficker

Previous Ranking: 1
Percentage Detected: 9.47%

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 sub-system 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&lng=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: 7.98%

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/Agent

Previous Ranking: 4
Percentage Detected: 3.53%

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 ☺), good patching practice, disable Autorun, and think before you click.

4. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 3.48%

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

5. INF/Conficker

Previous Ranking: 5
Percentage Detected: 1.67%

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.

6. Win32/Packed.FlyStudio.O.Gen

Previous Ranking: 19
Percentage Detected: 1.34%

Flystudio O.Gen are detections for obfuscated FlyStudio executables. They are separated from generic Win32/Packed.Flystudio (without any letter) as that detection covers legitimate Flystudio code as well.

What does this mean for the End User?

Obfuscated executables are not always malicious: sometimes obfuscation is used as a means of legitimate digital rights management (DRM) by hampering attempts at malicious reverse engineering. However the use of packers and obfuscators has been a fairly reliable indicator of malicious intent for some years now, and some vendors detect almost any obfuscated code as malicious or potentially malicious.

7. Win32/Sality

Previous Ranking: 23
Percentage Detected: 1.32%

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 to 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/Pacex.Gen

Previous Ranking: 9
Percentage Detected: 1.10%

The Pacex.Gen label designates a wide range of malicious files that use a specific obfuscation layer. The .Gen suffix means "generic": that is, the label covers a number of known variants and may also detect unknown variants with similar characteristics.

What does this mean for the End User?

The obfuscation layer flagged by this detection has mostly been seen in password-stealing Trojans. However, as more malware families appear that don't necessarily use the same base code but do share the same obfuscation technique, some of these threats are being detected as Pacex.

However, the increased protection offered by multiple proactive detection algorithms more than makes up for this slight masking of a statistical trend: as we discussed in a recent conference paper, it's more important to detect malware proactively than to identify it exactly. ("The Name of the Dose": Pierre-Marc Bureau and David Harley, Proceedings of the 18th Virus Bulletin International Conference, 2008 - http://www.eset.com/download/whitepapers/Harley-Bureau-VB2008.pdf; "The Game of the Name: Malware Naming, Shape Shifters and Sympathetic Magic" by David Harley - http://www.eset.com/download/whitepapers/cfet2009naming.pdf)

9. Win32/Tifaut

Previous Ranking: 6
Percentage Detected: 1.00%

The Tifaut malware is based on the Autoit scripting language. This malware spreads between computers by copying itself to removable storage devices and by creating an Autorun.inf file to start automatically.
The autorun.inf file is generated with junk comments to make it harder to identify by security solutions. This malware was created to steal information from infected computers.

What does this mean for the End User?

See INF/Autorun above for discussion of the implications of software that spreads using Autorun.inf as a vector.

10. Win32/Spy.Ursnif.A

Previous Ranking: 20
Percentage Detected: 0.90%

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.