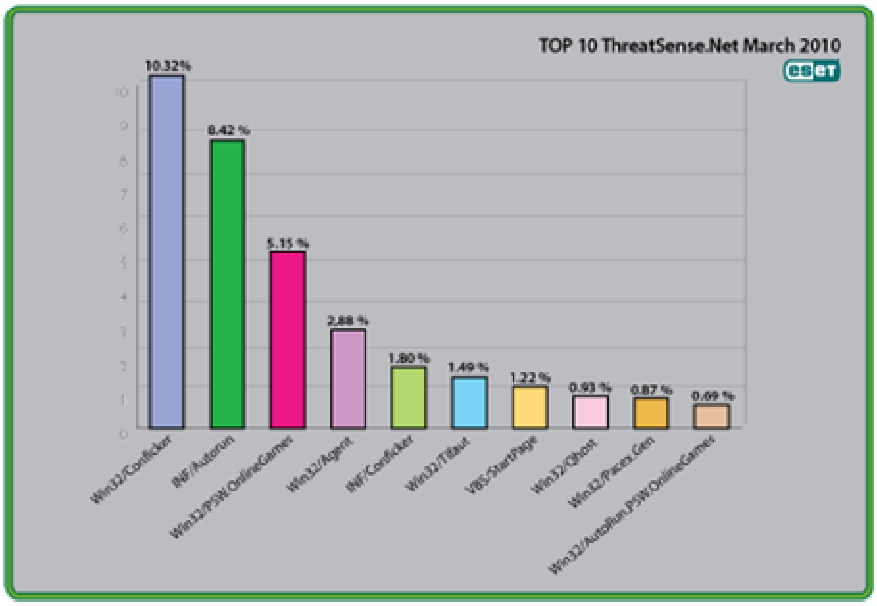
Global Threat Trends – March 2010

Figure 1: The Top Ten Threats for March 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 10.32% of the total, was scored by the Win32/Conficker class of threat.

More detail on the most prevalent threats is given at the end of this report, including their previous position (if any) in the "Top Ten" and their percentage values relative to all the threats detected by ThreatSense.Net®. But first, here is the news from ESET about other security and cybercrime issues this month.

The Threat Landscape in March, 2010

Yes, we've changed the format of this document, as we found that a lot of people thought it was just a list of the top ten threats. If you're still interested in those data, they're still here, but we've moved them to the end of the document. So what else has been happening in the world of security, malware and cybercrime?

Blackhat SEO: malicious links in search results and on Twitter

Right at the end of the month, the horrific bombings in Russia led to massive exploitation by criminals of search engines and Twitter to drive people towards malicious URLs pushing fake antivirus and other nastiness. The Research teams in San Diego and Latin America spent a lot of time in this issue, as can be seen from http://www.eset.com/blog/2010/03/30/here-come-more-of-the-ghouls and http://www.eset.com/blog/2010/03/29/russian-metro-bombings-here-come-the-ghouls.

Mac Attacks at CanSecWest 2010

If you're a Mac user, especially if you've been looking at the beta version of our Mac product (see http://www.eset.com/mac), you may also be interested in some of the topics discussed at the CanSecWest conference in Vancouver this month (http://cansecwest.com/). In particular, vulnerability researcher Charlie Miller claimed to have found "20 zero-day holes … contained in closed source Apple products", using a home-brewed fuzzing tool (to be precise, a short Python script). He's been tightlipped about the exact nature of the flaws, stating that he won't just hand over the details to Apple (or Microsoft, or Adobe, whose products he also put under a fuzzing microscope) because:

> "We find a bug, they patch it. We find another bug, they patch it. That doesn't improve the security of the product. True, [the software] gets incrementally better, but they actually need to make big improvements. But I can't make them do that."

What on earth, you may ask, is fuzzing? Sutton, Greene and Amini, in a book called "Fuzzing: Brute Force Vulnerability Discovery" (Pearson, 2007), define it as:

> "…a method for discovering faults in software by providing unexpected input and monitoring for exceptions."

David Harley wrote at Mac Virus (http://macviruscom.wordpress.com/2010/03/24/cansecwest-go-west-young-mac-but-fuzzily/):

> "Apparently [Miller] wrote a short Python script to change one randomly-selected bit of a PDF or PowerPoint file at each test iteration, and fed it to the target application to see if it crashed. He claims to have found "nearly a thousand unique ways" to make Adobe Reader, Apple Preview, Microsoft Power Point or Oracle's OpenOffice crash. When he looked through the data to see which vulnerabilities were exploitable he claims to have found 20 exploitable bugs in preview compared to three or four in each of the others.

You might think that this is just a vulnerability researcher talking up claims he isn't prepared to back up with evidence. However, he did use one of the exploits he found to make his mark for the third year running at the annual CanSecWest Pwn2Own hacker contest. His Safari exploit earned him $10,000 in prize money. Halvar Flake, Vincenzo Iozzo, and Ralf-Philipp Weinmann put together an exploit that compromised the iPhone (that one earned $15,000!) and didn't rely on jailbreaking. A technique called return-oriented programming was used to evade the iPhone's code-signing mechanism, creating a web page that enables the attacker to steal the iPhone's SMS database in a few seconds. Flake commented:

> "This exploit doesn't get out of the iPhone sandbox….Apple has pretty good counter-measures but they are clearly not enough. They way they implement code-signing is too lenient."

Not that this is all about the fragility or otherwise of Apple's product line. David Harley comments:

> I don't think the "leniency" or otherwise of Apple's code-signing is really the point. It might be a Good Thing to tighten up on iPhone code-signing, but the real point is that it isn't The Answer that will finally solve any and all iPhone security problems. Much the same applies to DEP (Data Execution Protection) and ASLR (Address Space Layout Randomization), both of which were bypassed on Windows 7 in the same contest.

Don't mistake mitigation for impregnability: a sound countermeasure may offer 100% protection in a context that holds little interest for attackers, but when the dollar signs start to flash, whether it's a hacking contest or the monetization of criminal activity, good technology is likely, sooner or later, to go the way of the Maginot line (http://en.wikipedia.org/wiki/Maginot_Line).

England Swings but Londoning Sucks

See http://en.wikipedia.org/wiki/England_Swings, if you're too young to remember Roger Miller's hits in the 1960s). We don't know if Swinging London is still swinging, but the last few years have seen an uptick in scams where criminals hijack email accounts or other messaging/social media accounts such as Facebook, using them to send messages to the real owner's friends telling them that they've been mugged while on holiday or business. This fairly low-tech hacking scam seems to be particularly popular with 419 gangs, who for some reason often claim that the mugging occurred at gunpoint in London – not the world's safest city, but not a hotbed of gun-crime, either – with the result that the scam is sometimes referred to as "the London scam" or "Londoning".

David Harley suggests (http://www.eset.com/blog/2010/03/23/londoning-mugs-and-muggings-revisited):

- Be very suspicious of messages like this, however they arrive and wherever or whoever they come from.
- Don't even think of responding to the request until you've verified the source.
- If the way the message is expressed is uncharacteristic (especially if it sounds more "foreign" than you'd expect), that's a pretty good indication that you're not talking to the person you *think* you're hearing from.
- Be particularly sceptical when a "friend" wants you to send them cash by a scam-friendly channel such as Western Union.
- 419 scams sometimes inventive in social engineering terms, but not necessarily hi-tech: take reasonable precautions to avoid having your accounts (email, Facebook, other social networking sites) compromised. Use hard to break passwords, don't use the same password for multiple accounts, and be on the lookout for any attempt to trick you into giving

> your password away, and that will reduce your attack surface (no guarantees of invulnerability though!)

More Malware (and other Cybercrime)

Earlier this month, Pierre-Marc reported (http://www.eset.com/blog/2010/03/02/more-statistics-on-infections) on updated statistics from our virus lab.

An average of 3 different malware families per infected computer (both globally and in the US). This means that on average, when a computer is infected, we find three different malware families installed ont it. However, this average seems to be slowly but steadily going down each month. This might indicate that malware operators are now tending to consolidate their operations and using single programs to perform multiple actions.

On the other hand, the average in China is an impressive 4.5, suggesting that malware operations are not conducted the same way around the world. Pierre-Marc says:

> We usually see less bank information stealers in Asia but more online game password stealers. Online game password stealers are usually installed by other malware families and don't propagate by themselves, explaining why we see an higher average in China than in the United States.

ESET's labs see more than 200 000 new and unique malicious binary files every day: Pierre-Marc estimates that this means that in the time it would take you to read his blog post, at least 70 unique pieces of malware will have been generated. These figures are based on tools such as ESET's ThreatSense.Net®, which supplements our heuristic technology by using distributed computing to gather threat intelligence: this capability has been extended in version 4.2 of our products, which was recently released.

Randy Abrams and David Harley answered a number of questions about malware and anti-malware naming and classification issues in a blog at http://www.eset.com/blog/2010/03/08/av-lingo-et-al: there are also several papers on the ESET white papers page that deal with these issues in more detail: e.g. http://www.eset.com/download/whitepapers/cfet2009naming.pdf, http://www.eset.com/download/whitepapers/Harley-Bureau-VB2008.pdf. A case in point was addressed by Jeff Debrosse in his blog at

http://www.eset.com/blog/2010/03/22/a-bot-by-another-other-name, when he used Jorge Mieres' blog for ESET Latin America (http://blogs.eset-la.com/laboratorio/2010/02/18/que-hay-de-cierto-respecto-botnet-kneber/) to explain that Kneber and Zeus are essentially the same botnet, despite much confusion in the media.

Craig Johnston commented at http://www.eset.com/blog/2010/03/17/were-not-talking-peanuts-here on the real size of the cybercrime problem, with an impressive battery of supporting statistics, Juraj Malcho published an article for CTO Edge on the use of social engineering in malware (http://www.ctoedge.com/content/weakest-computer-security-link), and Aryeh Goretsky discussed DNS registration scams (http://www.eset.com/blog/2010/03/18/the-return-of-jacques-tits). Randy Abrams, Dan Clark, and Craig Johnston all discussed the international ramifications of US legal measures against cybercriminality (http://www.eset.com/blog/2010/03/24/carrots-sticks-and-cyber-spies, http://www.eset.com/blog/2010/03/24/while-rome-burns), http://www.eset.com/blog/2010/03/24/good-in-theory-but).

At the time of writing we are, as predicted in a white paper published early this year (2010: Cybercrime Coming of Age - http://www.eset.com/resources/white-papers/EsetWP-CybercrimeComesOfAge.pdf), been seeing what's probably the first serious attempt to capitalize on this year's soccer World Cup by using social engineering based on the event to spread malware.

In this case, the attack takes the form of an email allegedly from safari organizer Greenlife, containing a PDF attachment based on Greenlife's genuine guide to the "first African edition of football's most prestigious tournament". However, the attachment has been modified to take advantage of an Adobe Reader vulnerability to install malware onto machines that haven't been updated with the patch released on the 16th February (CVE reference CVE-2010-0188 – see also http://www.adobe.com/support/security/bulletins/apsb10-07.html).

David Harley advises:

- Make sure you're up-to-date on your Adobe patching (and any other high risk application patches, not to mention OS patches)
- PDFs are a risky format these days: if they come from an unrecognized source, or come unsolicited, that makes them all the more risky (and suspicious)

- Keep in mind our advice above: any interesting event (real or imagined) is likely to be used as a hook for social engineering and malware distribution.

- And, of course, check that your antivirus software is up-to-date.

ESET on the Conference Circuit

While EICAR (formerly the European Institute for Computer Antivirus Research: http://www.eicar.org) may be better known by many people for its association with the EICAR test file, it has for many years also run a major security conference with an anti-malware focus. This year's conference (the 19th, taking place between the 8th and 11th of May) will be of considerable interest to those interested in anti-malware testing issues: the pre-conference programme will, according to the conference page at http://www.eicar.org/conference/, be centred "around the topic of AV software and AV policy evaluation."

Several industry papers during the main conference will also address testing issues, including "Real Performance?" by ESET's Ján Vrabec and David Harley, in which they look at commonly used models for performance testing (as opposed to detection testing). David Harley and Pierre-Marc Bureau, along with K7's Andrew Lee, will also be presenting a paper on "Perception, Security and Worms in the Apple" in which they look at the way in which the Apple-using population is slowly being forced towards the same firing line as the rest of us. The paper also looks at changes in attitude, using some data from the CERC survey carried out on behalf of "Securing Our eCity" (see http://www.eset.com/blog/?s=CERC).

David Harley is also speaking on Apple security issues at Infosec Europe (http://www.infosec.co.uk) on the 28th of April in the Business Strategy Theatre (13:20 - 13:45 - Apple, Security And The Power Of Perception). He'll also be spending time on the ESET stand (see the exhibitor directory on the main page) and happy to talk to anyone who wants to talk to *him*.

ESET is also well-represented at the Virus Bulletin conference, which takes place between the 29th September and the 1st of October 2010. "AV testing exposed" by Peter Košinár, Juraj Malcho, Richard Marko, and David Harley, takes a long hard look at the technicalities of anti-malware testing. Pierre-Marc Bureau, along with Joan Calvet and Jean-Yves Marion, LORIA, and Jose M. Fernandez, École Polytechnique de Montréal will present on "Large-scale malware experiments, why, how, and so what?". David Harley also has a paper with Andrew Lee, on "Call of the WildList: last orders for WildCore-based testing?"

The Top Ten Threats: More Information

1. Win32/Conficker

Previous Ranking: 1
Percentage Detected: 10.32%

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: 8.42%

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: 5.15%

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

4. Win32/Agent

Previous Ranking: 4
Percentage Detected: 2.88%

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.

5. INF/Conficker

Previous Ranking: 5
Percentage Detected: 1.80%

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/Tifaut

Previous Ranking: 25
Percentage Detected: 1.49%

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.

7. VBS/StartPage

Previous Ranking: 60
Percentage Detected: 1.22%

VBS/StartPage is a detection applied to various examples of malware that change settings for Internet Browsers (usually Internet Explorer) and redirect the starting page to advertisement websites. These threats can also create icons on an infected PC's Desktop with links to advertisements. VBS/StartPage is very prevalent in Asia and especially in China, if this threat is detected on a computer, it might be an indication that other threats might have infected this system.

What does this mean for the End User?

It's not that usual nowadays for malware to make its presence as obvious, and this isn't brand-new, innovative malware. But that doesn't, unfortunately, mean that it's not a problem for users who aren't using regularly updated antivirus software.

8. Win32/Qhost

Previous Ranking: 8
Percentage Detected: 0.93%

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/Pacex.Gen

Previous Ranking: 6
Percentage Detected: 0.87%

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)

10. Win32/AutoRun.PSW.OnlineGames

Previous Ranking: 85
Percentage Detected: 0.69%

Threats identified with the label 'AutoRun' are known to use the Autorun.INF file. This file is used to automatically start programs upon insertion of a removable drive in a computer.
Trojans identified with the label 'PSW.OnlineGames' have 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?

The implications of this type of threat are similar to those for INF/Autorun (see above) and Win32/PSW.OnlineGames (also above).