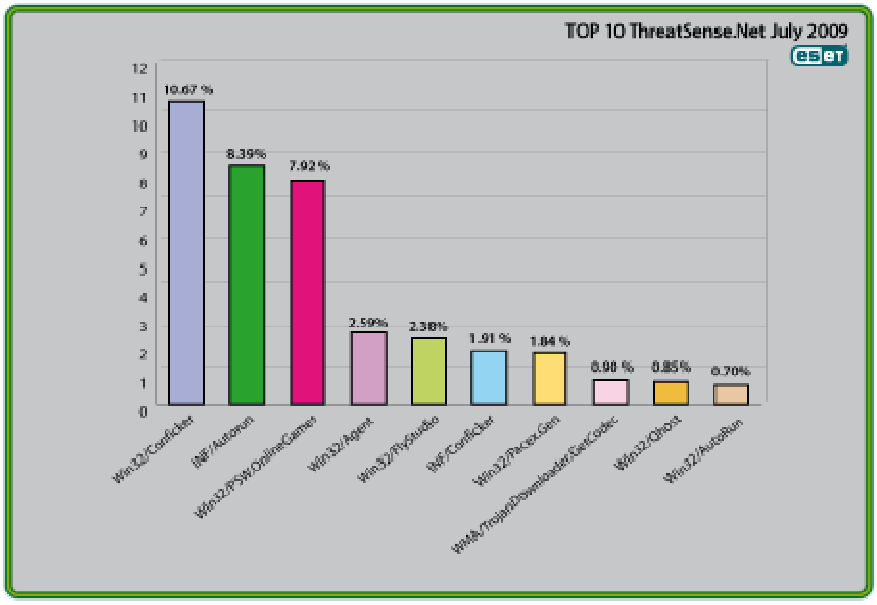
Global Threat Trends – July 2009

Figure 1: The Top Ten Threats for July 2009 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 10.67% of the total, was scored by the Win32/Conficker class of threat.

More detail on the most prevalent threats is given below, including their previous position (if any) in the "Top Ten" and their percentage values relative to all the threats detected by ThreatSense.Net®.

1. Win32/Conficker

Previous Ranking: 1
Percentage Detected: 10.67%

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 Microsoft have announced that it won't be enabled 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 end of October, 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 recent variants seem to have 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.

2. INF/Autorun

Previous Ranking: 2
Percentage Detected: 8.39%

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.

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 7.92%

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 Malware Intelligence 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: 2.59%

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. Win32/FlyStudio

Previous Ranking: n/a
Percentage Detected: 2.38%

The Win32/FlyStudio threat is designed to modify information inside the victim's Internet browser. This threat will modify search queries, with the intention of delivering advertisements to the user. Win32/FlyStudio seems to be targeting users located in China.

What does this mean for the End User?

FlyStudio is a popular scripting language, much used as a development tool in China. However, the malicious code is being reported in other regions too, including North America. This may mean that it has been deployed by another family of malware.

6. INF/Conficker

Previous Ranking: 5
Percentage Detected: 1.91%

INF/Conficker is related to the INF/Autorun detection: it's 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/Pacex.Gen

Previous Ranking: 7
Percentage Detected: 1.84%

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.)

8. WMA/TrojanDownloader.GetCodec

Previous Ranking: 8
Percentage Detected: 0.90%

Win32/GetCodec.A is a type of malware that modifies media files. This Trojan converts all audio files found on a computer to the WMA format and adds a field to

the header that includes a URL pointing the user to a new codec, claiming that the codec has to be downloaded so that the media file can be read. WMA/TrojanDownloader.GetCodec.Gen is a downloader closely related to Wimad.N which facilitates infection by GetCodec variants like Win32/GetCodec.A.

What does this mean for the End User?

Passing off a malicious file as a new video codec is a long-standing social engineering technique exploited by many malware authors and distributors. As with Wimad, the victim is tricked into running malicious code he believes will do something useful or interesting. While there's no simple, universal test to indicate whether what appears to be a new codec is a genuine enhancement or a Trojan horse of some sort, we would encourage you to be cautious and skeptical: about any unsolicited invitation to download a new utility. Even if the utility seems to come from a trusted site (see http://www.eset.com/threat-center/blog/?p=828, for example), it pays to verify as best you can that it's genuine.

9. Win32/Qhost

Previous Ranking: 10
Percentage Detected: 0.85%

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.

10. Win32/AutoRun

Previous Ranking: 8
Percentage Detected: 0.70%

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.

What does this mean for the End User?

The general implications of this particular threat for the end user are much the same as for malware detected as INF/Autorun.

Current and Recent Events

Pick up a P-P-Patch

Patching has been in the news quite a lot this month. A presentation at the Black Hat conference seems to have influenced the timing of an important out-of-band Microsoft patch, partly relating to underlying vulnerabilities in the Active Templates Library. However, this is not just a Microsoft issue. Adobe, who already have their hands full with a queue of Adobe-specific issues requiring patching, have also had to include remediation for the Microsoft ATL issue in their own updates to Adobe Flash Player. David Harley, ESET's Director of Malware Intelligence, commented in one of his blogs on Adobe updating that:

> "Adobe has become almost the target of choice among black hats recently… Perhaps even more significant, though, is the interdependency between applications demonstrated here. In a complex operating environment like Windows, it isn't always practical to consider applications in isolation from each other: the ATL vulnerabilities highlighted at Blackhat affect both Adobe and Microsoft applications, and while the Flash Player update is a Good Thing, you also need the Microsoft update …. While AV vendors are detecting some vulnerabilities proactively, you shouldn't rely on AV detection alone, as exploits can sometimes be tweaked so as to evade detection by specific products.

Web 2.0 or not Web 2.0, that is the question

There have been further, dramatic illustrations of the risks that attend the use of social networking sites. Randy Abrams, our Director of Technical Education, noted that the wife of the Head of MI6, one of the UK's intelligence services, put way too much information up on Facebook (http://www.eset.com/threat-center/blog/2009/07/06/social-networking-or-social-suicide) – even more recently, the MI5 web site was hacked, but I guess we can't blame Facebook for that. Twitter has also had its issues, not least with Avi Raff's Month of Twitterbugs chipping away at its credibility. To its credit, it has attempted to tighten up on security, again, and indeed, we have some twitter accounts on the Research team for those who want to follow our blogs and other activities. No, not the parties we go to: sorry! http://twitter.com/esetresearch is the official team Twitter account, but we also post stuff to http://twitter.com/ESETLLC and http://twitter.com/ESETblog, which have

more followers at the moment. There's also an account http://twitter.com/esetpr that PR contacts will find useful.

Anti-Malware Testing Standards Organization

While there hasn't, for once, been a great deal going on in the public testing arena, there's a lot going on behind the scenes, and ESET is part of it. The Research Team's David Harley joined AMTSO's Board of Directors this month, and is already disappearing behind a flurry of extra tasks. However, ESET regards the work that AMTSO is doing as enormously important, not just for the security industry but also for the benefit of the community at large. Raising the general standard of testing is a vital target, and we're honored and delighted to be able to contribute.

Social Security Numbers and the Art of Password Management

There's been a great deal of interest in a paper for the Proceedings of the National Academy of Sciences called "Predicting Social Security numbers from public data" by Alessandro Acquisti and Ralph Gross, which claims that an SSN is relatively quick and easy to guess if you have other information relating to the individual's place and date of birth. The confusion between identification and authentication that's led to that problem is far too complex to be covered in this short report: however, our blog at http://www.eset.com/threat-center/blog/2009/07/12/theres-security-then-theres-social-security goes into some detail, and a paper by David Harley that expands on the topic is due to appear shortly on the ESET White Papers page at http://www.eset.com/download/whitepapers.php.

As a matter of fact, there are two other white papers due to appear at around the same time, and several more in the pipeline. In the first instance, look out for "Playing Dirty" by Cristian Borghello, and "Keeping Secrets: Good Password Practice" by David Harley and Randy Abrams.

Win32/Waledac and the Dewey Effect

At the beginning of July, ESET got wind of an Independence Day spam campaign by the Waledac gang, who had registered a number of domains that were earmarked to serve copies of Waledac passed off as videos of July 4th fireworks, with the intention of expanding their botnet. The fact that we were able to call attention to it and that so many other security-focused sites like the Internet Storm Center followed up, thus piquing the interest of the media, seems to have made a substantial dent in the effectiveness of the campaign, In fact, the spam campaign started before July 4th, probably in the hope that the spam would reach some potential victims before the warnings did. Since the social engineering ploys used in this spam run very specifically referred to "This year's July 4th firework's shows", it's likely that this backfired to some extent. You don't have to be a security guru or clinically paranoid to be suspicious of a "video" that claims to show events that haven't yet happened. We suspect, however, that the gang will learn from this.

One thing that Win32/Waledac *does* do well, though, is send out spam. ESET's team in Latin America did some testing and estimated that a Waledac-infected computer can send about 150,000 emails a day, which is nearly two emails per second. See Sebastián Bortnik's guest blog at http://www.eset.com/threat-center/blog/2009/07/07/guest-blog-how-much-spam-does-waledac-send.

(And in case you were wondering about the Dewey Effect, check out the Wikipedia page that describes it at http://en.wikipedia.org/wiki/Dewey_Defeats_Truman.

No Wires Attached

Finally, our colleagues in Europe came up with a nice article on the risks around free wi-fi when you're enjoying the summer weather around the city hotspots (wireless hotspots, not nightclubs!), and how you can surf in the sun more safely. Here's an abbreviated version: more information at http://www.eset.com/threat-center/blog/2009/07/28/fly-by-wireless.

- Keep your system and applications updated. Of course, you're already doing this, aren't you?
- Change your passwords frequently: painful though most of us find this, it does limit the extent to which your systems are exposed if something does get through.
- Use different passwords for different accounts and resources, so that if one does leak, it doesn't mean that an attacker has access to everything you own and every service you access.
- Use strong passwords or passphrases.
- Using a profile that doesn't have administrator privileges is likely to restrict the amount of damage an attacker can do if he does get access to your system.
- Back up your data before you take your laptop out. Then, if your laptop is stolen or damaged, then you won't have lost all that information (though you should still change passwords straightaway if the PC is lost.)
- Make sure you your security software is updated regularly and automatically, but don't assume it will protect you from everything. Wi-fi is inherently insecure (WEP even more so) and you need to use common sense as well.
- Disabling the sharing of files or folders, but it's not just the settings on your computer that can save you from the hacker's grasp: you also need to take care which sites you surf. Wherever possible, avoid connecting to websites that involve the transfer of sensitive information, such as online banking and if you must access webmail, use the HTTPS option.

More Information From ESET

ESET Threatblog (TinyURL with preview enabled):
http://preview.tinyurl.com/esetblog

ESET Threatblog notifications on Twitter: http://twitter.com/esetresearch

ESET White Papers Page: http://www.eset.com/download/whitepapers.php

Securing Our eCity community initiative: http://www.securingourecity.org/