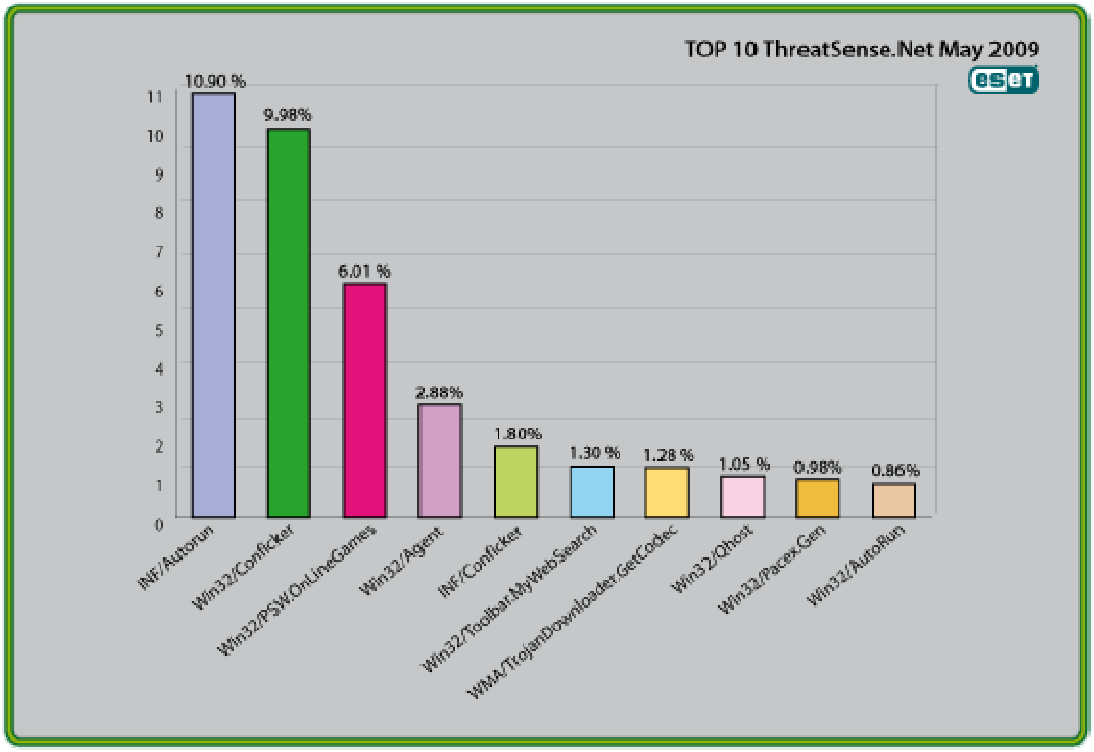
Global Threat Trends – May 2009

Figure 1: The Top Ten Threats for May 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 10.90% of the total, was scored by the INF/Autorun 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. INF/Autorun

Previous Ranking: 2
Percentage Detected: 10. 90%

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.

2. Win32/Conficker

Previous Ranking: 1
Percentage Detected: 9.98%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent, already fixed 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 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

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 6.01%

This is a family of Trojans 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. 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 ranged against them. The ESET Malware Intelligence team considered this issue at more length 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?

Creating random filenames is another approach to making it harder to use filenames as a way to spot malware, and has been used many times over the year. While it can help on occasion, it shouldn't be relied on. We'd suggest that you should be particularly wary of anti-malware packages that appear to use filenames as a primary identification mechanism, especially when they use advertising hooks like "Our product is the only one that detects nastytrojan.dll."

5. INF/Conficker

Previous Ranking: 6
Percentage Detected: 1.80%

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 earlier.

6. Win32/Toolbar.MywebSearch

Previous Ranking: 9
Percentage Detected: 1.30%

This is a Potentially Unwanted Application (PUA). In this case, it's a toolbar which includes a search function that directs searches through MyWebSearch.com.

What does this mean for the End User?

This particular nuisance has been a consistent visitor to our "top ten" lists for many months.

Anti-malware companies are sometimes reluctant to flag PUAs as out-and-out malware, and PUA detection is often an option rather than a scanner default, because some adware and spyware can be considered legitimate, especially if it mentions (even in the small print of its EULA or End User Licensing Agreement) the behavior that makes it potentially unwanted. It always pays to read the small print.

7. WMA/TrojanDownloader.GetCodec

Previous Ranking: 7
Percentage Detected: 1.28%

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.

8. Win32/Qhost

Previous Ranking: 8
Percentage Detected: 1.05%

This threat copies itself to the %system32% folder of Windows before starting. It then

communicates over DNS with its command and control server. 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: 16
Percentage Detected: 0. 98%

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. Some threats aimed at online gamers may therefore be detected as Pacex, rather than as PSW.OnLineGames, as there is some overlap between these two threats. This suggests that the overall percentage of threats falling into the PSW.OnLineGames category is still even greater than its already high score suggests. 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.)

10. Win32/Autorun

Previous Ranking: 10
Percentage Detected: 0. 86%

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

Another Patch Tuesday

Another month, another Patch Tuesday, when Microsoft finally addressed a number of security issues with PowerPoint, though Mac users will have to wait a bit longer for a patch. Microsoft (and others) have shown a tendency towards complacency as regards recent Excel and PowerPoint vulnerabilities. While these have been mostly used for small scale targeted attacks aimed at individuals rather than mass mailouts of malicious sites, such an attack directed, for instance, against a government or military employee could affect many, many people. Such attacks for purpose of international espionage have been commonplace in the past few years.

We've pointed out many times that while we rarely see old-style macro viruses these days, there are many other document-borne threats: zero-day attacks, embedded executables and malicious links, and so on. PDF's have been a particularly common target (as discussed several times at the CARO workshop – see the "Spring Conferences" section), and it's good to see that Adobe finally addressed some of the most recent vulnerabilities to affect Adobe Reader and Acrobat. Adobe now proposes to release security updates on a regular quarterly basis. According to Brad Arkin, who manages Adobe's proactive and reactive security teams, the benefits to the rest of the world will include "more timely communications regarding incidents", and faster patching, simultaneous across affected platforms. We're not sure exactly how that's going to work, but at least it's making an effort. Now if they'll only address some of the other issues we've been flagging in the Threat Center blog at http://www.eset.com/threat-center/blog/, some of the sting will be taken out of a very serious, ongoing problem.

Spring Conferences

It has been another busy month for the Research Team. We were represented at the Infosec conference in the UK at the end of April/beginning of May, where David Harley presented a seminar on good and bad practice in anti-malware testing in the Business Strategy track (see http://www.infosec.co.uk/page.cfm/Action=Seminars/CategoryID=2 for more information). The following week, Pierre-Marc Bureau (and Juraj Malcho from the lab in Slovakia) made a well-received presentation at the CARO workshop in Budapest on the MS08-067 vulnerability exploited by a number of malware types, but

especially Win32/Conficker. Other topics of interest included discussions of (other) vulnerabilities and exploits affecting Microsoft and Adobe users, and a fascinating (if controversial) talk about vulnerability issues that could arise from the use of "in-the-cloud" technologies by security companies.

CARO (the Computer Antivirus Research Organization) has been working behind the scenes in anti-malware research for nearly 20 years now, but has been running annual specialist workshops for several years now that attract intense interest in the research community. AMTSO (the Anti-Malware Testing Standards Organization) is a lot younger (it was formally established a year ago in 2008), but has been making dramatic progress towards changing the landscape in anti-malware testing, and the two organizations have been closely linked in some respects. So the day after the CARO workshop finished, many of us were back at the same venue for another AMTSO workshop.

These workshops are far more of a collaborative working event than a presentation-based information sharing event. On this occasion, two more Best Practices papers were approved: one on testing "in the cloud" security products, and one on validating samples. These topics are both more interesting and more important than you might think.

Testing a product that uses "in the cloud" technologies poses enormous practical problems for some kinds of testing, because it involves either maintaining or disabling an open channel to the internet. An open channel, as with most forms of dynamic testing, involves an increased risk of "leaking" malicious software outside the testing lab, causing risk to people and systems in the outside world. Disabling an open channel involves technical challenges, but is vital in testing heuristic detection of unknown threats.

The members also approved the process document for requesting and handling review analyses. This means that it is now possible for companies or individuals to request an expert analysis from AMTSO regarding a test or review, which will evaluate how successfully the review conformed with the AMTSO principles of testing at http://www.amtso.org/uploads/AMTSO_Principles_-_FINAL_31_Oct_2008-1.pdf. This is an important step towards encouraging testers to adopt best practices, though there is a risk that some testers might see this as threatening, a way for a security company to use AMTSO as a gun-for-hire to shoot down a review in which they did badly, and building in safeguards against such misuse is not altogether straightforward.

However, David Harley, Director of Malware Intelligence at ESET and himself a member of the Review Analysis Board, says "If the Board goes after every faulty test, it's going to be very busy... Personally, though, I wouldn't be interested in pursuing vendettas by proxy or publicising poor testers unnecessarily by publishing reviews that would otherwise sink into deserved ignominy. What I'd really like to see is testers proactively checking their methodology against the AMTSO principles, rather than waiting to be beaten over the head with an analysis because they failed to conform. Encouragingly, I'm starting to see signs of this happening."

All the documents currently available from AMTSO can be found at http://www.amtso.org/documents.html. Subscribers to Virus Bulletin (http://www.virusbtn.com) will be able to read a review of the CARO and AMTSO workshops by David Harley in the June issue.

David and Randy went on to EICAR in Berlin, where they jointly presented David's paper on "Execution Context in Anti-Malware Testing": there were quite a few other papers on testing and an optimistic panel session promising cooperation between AMTSO and EICAR, which would be a significant step forward. More information is available at http://www.eicar.org.

In addition, Randy was at Interop in Las Vegas (a major trade show), Pierre-Marc was at Confidence in Krakow (a small event but very important to research specialists), and David was at Channel Expo in the UK (presenting on testing yet again, but also having some interesting and useful conversations with channel partners and resellers).

Securing Our eCity

ESET has been sponsoring an exciting initiative in San Diego called "Securing Our eCity", to which several members of the Research team have contributed time and resources. See http://www.securingourecity.org for resources, and http://www.securingourecity.org/news.php for news and information on the initiative. Randy Abrams, ESET's Director of Technical Education, blogged "Securing Our eCity is an initiative that ESET and other public and private sector organizations have formed to help provide quality education about cybercrime and how to defend against it.... this coalition of concerned organizations has been able to create free courses on how to better educate and protect yourself from cybercrime. In late May an early June we are offering several free presentations on cybercrime." It's intended to develop this initiative by extending it to other cities in due course.

For more information on the Research team and what they've been up to, check out the Threat Center Blog at http://www.eset.com/threat-center/blog/.