



Global threat report

May 2011

Feature Article: Don't be silly online, please

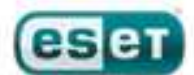




Table of Contents

| | |
|--|----|
| Don't be silly online, please | 3 |
| Facebook privacy: security concerns | 4 |
| Cybersecurity symposium in San Diego | 4 |
| Return of the password reset attack | 5 |
| The Top Ten Threats | 5 |
| Top Ten Threats at a Glance (graph) | 9 |
| About ESET | 10 |
| Additional resources | 10 |



Don't be silly online, please

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

Why are people sometimes so silly when it comes to computer security? With all the warnings, with all the factual data on damage done, they still don't take computer security seriously, even at a basic level. "That's dangerous? I didn't know," is what they tell me. It's as if they were driving a car blindfolded on the assumption that an accident couldn't ever happen to them anyway. Here are two recent anecdotes from people I know that made me think.

Once your friends learn that you're into computer security, they'll ask you all kinds of questions. The other day a friend rang me asking for help. He said that he urgently needed to install a pirated version of a program, but that his ESET antivirus program was preventing him from doing it. And he wanted to know how to disable the antivirus. At first I thought he was joking, but sadly he wasn't. Think of your antivirus as a sort of virtual airbag, preventing (or at least mitigating) damage to you and your vehicle in the event of a car crash. In this case we have a driver asking how to disable the airbag when he's driving on the wrong side of the road... Unfortunately many people still just see the antivirus as that pesky thing that is preventing them to do all the fun but risky stuff with the computer.


We all know pirated software is illegal, but we also know many people don't care about that. But apart from the issue of legality, from a security analyst's perspective this is a seriously naive view of human nature.

Why do you think pirates make licensed software freely available for people to download? Out of the goodness of their hearts? They have nothing better to do, so they go through the

trouble of cracking software protection and giving it to people just for the kicks? If you believe that, you probably also sincerely believe there's a pot of gold at the end of the rainbow. Well, there do seem to be people who sincerely believe that information wants to be free and that artists, musicians, authors and software publishers should not expect to be paid for their time and labour. (Try that argument with your plumber or your lawyer...) The truth is, though, that while you may get hold of entirely functional pirated software, there's also a good chance that, unknown to you, you will also get a little something extra with it. A trojan, a keylogger, a rogue antivirus installer, or something equally desirable: a little piece of malware that can turn into a big problem when cybercriminals use it to start stealing money from you. And often, they steal a lot more than buying the licensed software would have cost you.

The second anecdote concerns a friend who walked into a cyber-cafe abroad, in order to check his mail and social networks. He found an available computer and realized that the previous user had forgotten to log out of his Facebook account. Believing this was a one-off mishap; he kindly logged him out and then checked another computer. But on that machine, someone else had also left the machine still being logged in. And he found two more machines with the same problem. What if my friend had been a bad guy and had taken the opportunity to change those people's passwords and abuse their profiles? As it was, he merely notified them they need to be more careful, and then logged them out. Many public computers don't have logging out and other security features enabled when you close the browser. So it's up to the computer user to be extra careful and to make certain he has logged out of all the services he has logged into and take other commonsense measures like deleting his browsing history.

So, while the bad guys are coming up with infinite ways of



targeting people online with scams, swindles, infections, theft, and so on, we are appealing to all computer users at least not to be silly, and to use common sense and some basic secure behavior when dealing with sensitive things such as malware and password protection.

While we haven't published much specific to safe use of publicly-available computers (cyber cafes, kiosk computers, library facilities, and so on) – which sounds like a project worth spending some time on – David Harley did put together a blog series last year on safe computing in general: see <http://blog.eset.com/?s=cyber-bullets> or the subsequent paper [“Ten Ways to Dodge CyberBullets.”](#)

Facebook privacy: security concerns

If Facebook was a country, it would be the third largest one in the world (<http://blog.eset.com/2011/05/04/osama-bin-laden-is-alive-and-well-on-facebook>). All those Facebook users are exposed to the many social networking risks and nuisances that are regularly reported nowadays. Paul Laudanski's wrote a [comprehensive blog article](#) which is a timely and essential guide to a better and safer management of a Facebook account.

As Paul points out, breaches can and do occur, and the only way to truly protect the information is to not have it online. However, that would be a sort of defeat to the purpose of social networking. The best thing to do is to understand the risks and take all reasonable measures to protect oneself against scams and identity theft.

Cybersecurity symposium in San Diego


[Securing Our eCity](#) (SOeC), originated in the city of San Diego, California (USA), has celebrated a new event that brought together various people connected with this interesting cyber security education initiative, which for more than two years it has been expanding.

On May 17th, all day, over a hundred people attended to the first of two annual symposiums organized by SOeC. ESET was there to attend conferences of various specialists in education, technology and cyber security sectors including governments, businesses and nonprofit organizations.

The presentations were all related to the initiative, such as the problems raise public awareness on cyber security, the same approach I business and the role of governments around the theme. Among the featured speakers were: Ernest McDuffie, leader of the national education initiative of the prestigious cyber security NIST (National Institute of Standards and Technologies), Ruben Barrales, CEO of the Chamber of Commerce San Diego Regional, Nathan Fletcher, California legislature, Darin Andersen, Chief Operating Officer (COO) of ESET North America and Duane Roth, CEO of Connect, an organization dedicated to supporting entrepreneurs.

The symposium featured three panels of experts: one focused on the problem especially in small and medium enterprises, the other on the laws and regulations relating to the business, and one on the need to prepare leaders who have the ability to handle the issue the future.

There were also two workshops, one of which was security at the household level, and the other on the resources required to



create a framework in information security within an organization. The event ended with an awards ceremony and delivery of annual awards to executives in information technology.

Return of the password reset attack

Randy Abrams, director of technical education, ESET

Most people know about the Sony PlayStation Network/Qriocity Service breach by now. Probably most of those people know that they need to change those account passwords when they can access the network again. Many people might be aware that if they used the same password in other places, they need to change those passwords as well. Sony doesn't seem to know if credit card details were breached, so many people are cancelling the credit cards used in conjunction with their Sony accounts.

The insidious threat that many people may miss is the compromise of the answers to password reset questions. That was some of the data that was reportedly compromised in the breach, and has perpetual consequences if you do not change your security reset answers on other sites as well.

The way the password reset attack works is that a hacker tries to log into your account. It may be an email account, a social networking account, a blogging account, or another type of online account. The hacker clicks the link for "I forgot my password" and is challenged with security questions. Having obtained the answers from the Sony data breach, the hacker knows the answers to the reset questions and is now able to commandeer your accounts, depending on the mechanism that particular sites use in conjunction with the security challenge questions.

If you are one of the victims of the Sony breach, do not overlook the significance of the challenge questions. You need to determine each site you are signed up with, and if they use any of the same security challenge questions that were used on the Sony site. Failure to change the answers may leave your other accounts vulnerable to cybercriminals performing password reset attacks.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 6.58%

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.

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.

2. Win32/Conficker

Previous Ranking: 2
Percentage Detected: 3.61%

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&lng=en.

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. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 1.92%

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.

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/Sality

Previous Ranking: 4
Percentage Detected: 1.88%

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

5. HTML/StartPage.NAE

Previous Ranking: 17
Percentage Detected: 1.78%

HTML/StartPage.NAE is a trojan which tries to promote certain web sites by modifying the window's registry. The program code of the malware is usually embedded in HTML pages. The aim of this malware is to change the website that is first opened when running Microsoft Internet Explorer (only affected browser). This way it promotes a specific website, and the owner of it profits of the increasing amount of visitors. This specific variant of HTML/StartPage redirects the affected users to the following website: <http://duzceligenclik.com>

6. JS/Redirector

Previous Ranking: 11
Percentage Detected: 1.59%

JS/Redirector.NID is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages of compromised legit websites. As indicated by its name, it uses a JavaScript, usually obfuscated, to make the redirection to the malicious website. By doing this, it tries to download and execute malicious software on the clients computer, a distribution technique widely used.

7. HTML/Iframe.B.Gen

Previous Ranking: 7
Percentage Detected: 1.59%

Type of infiltration: Virus

HTML/Iframe.B.Gen is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.

8. Win32/Autoit

Previous Ranking: 5
Percentage Detected: 1.28%

Win32/Autoit is a worm that spreads via removable media, and some of its variants spread also thru MSN. It may arrive on a system as a downloaded file from a malicious Web site. It may also be dropped by another malware. After infecting a system, it searches for all the executable files and replace them with a copy of itself. It copies to local disks and network resources. Once executed it downloads additional threats or variants of itself.

In order to ensure that the worm is launched automatically when the system is rebooted, the worm adds a link to its executable file to the system registry.

9. Win32/Bflient

Previous Ranking: 8
Percentage Detected: 0.85%

Win32/Bflient is a worm that spreads via removable media and



contains a backdoor. It can be controlled remotely and ensures it is started each time infected media is inserted into the computer.

10. Win32/Autorun

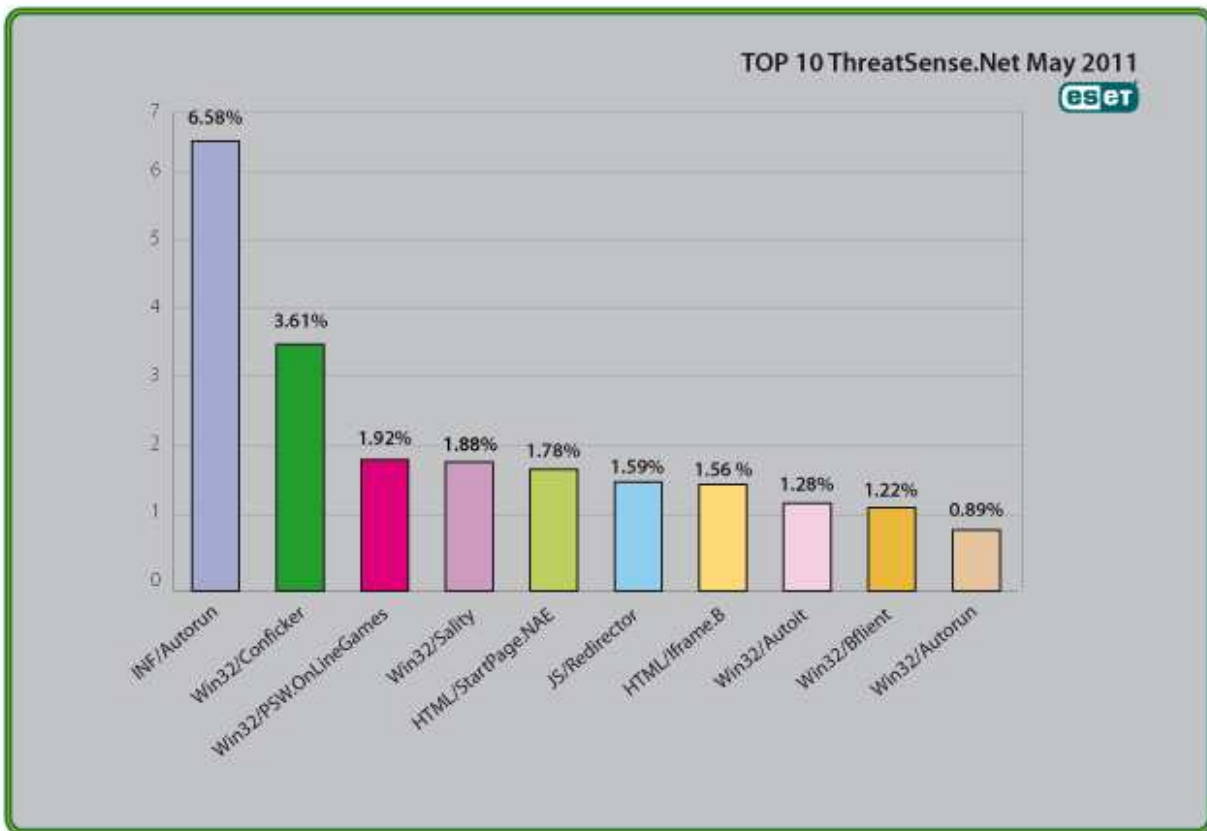
Previous Ranking: 6
Percentage Detected: 0.96%

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. The file itself doesn't represent a threat, but combined with a binary file it turns into a deploying feature.



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 6.58% of the total, was scored by the INF/Autorun class of threat.





About ESET

ESET is a global provider of security software. The ESET NOD32® Antivirus and ESET Smart Security products are consistently recognized among the most comprehensive and effective security solutions available today.

Additional resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the [ESET Threat Center](#) to view the latest:

- [ESET White Papers](#)
- [ESET Blog](#)
- [ESET Podcasts](#)
- [Independent Benchmark Test Results](#)
- [Anti-Malware Testing and Evaluation](#)