October 2011

Feature Article: Do you think you're safe online?

eset

Table of Contents

Do you think you're safe online?

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

Time and again we've discussed how, no matter what sort of antivirus protection people use, they themselves are still the weakest link in cyber-security. Clicking on things, running programs or visiting links they shouldn't, exposing themselves to risks constantly.

At ESET Ireland we're trying to find out why that is the case. And one way we went about it is by trying to establish what Irish computer users even perceive as an online threat and how likely they think it is that something will happen to them. Of course, we expect that our conclusions will be to some extent applicable to a far wider population of users.

We conducted a survey, carried out on our behalf by Amarach research, which presented 852 people of all ages and from all parts of Ireland with the following six statements:

- My computer can be crashed or caused to malfunction by viruses or malware.
- Computer viruses or other malware can infect my computer/ steal data/ cause damage.
- Someone could hack into my email or social media and contact my friends pretending to be me.
- I could be cheated by scam emails or fraudulent social media messages.
- My private information/ credit cards/ identify could be stolen or misused online.
- Someone could access my computer online to steal my data/ turn my computer into a malware or spam dispatching bot.

Then we asked them to rate each of the statements with whether this has already happened or how likely it is to happen and the results were quite surprising.

As it turns out 1 in 4 Irish computer users has already had their computer crashed or otherwise damaged by viruses or malware. 1 in 5 has had their computer infected or data stolen. 14% were hacked or had their social media accounts hijacked. And nearly every tenth person was cheated, had their credit cards or private info abused or their system was used to unknowingly dispatch spam.

What is even more interesting is that over 40% of people believe any of that could easily happen to them. This could mean several things. Either they mistrust their antivirus protection or are aware that their security practices are not adequate compared to the sorts of threats they're facing.

On the other hand less than 4% believe none of those could ever happen to them, while about a third believe it's either not easy or very unlikely that they'd become a victim.

Some more interesting details come from demographics of the surveyed. While males and females were targeted indiscriminately and in equal proportions, it was the younger population (age group 15-24) that experienced most computer crashes, virus infections and online and social media personality theft, while the older population (age group 45-54) had the

most experience of having data stolen or credit cards abused. This can possibly be explained by speculating on how each of these groups use computers. For the young it's mainly gaming, entertainment and social media: thus pirated games, music and movies infect them with malware, while social interactions make them victims of identity theft. Adults, however, tend to shop and bank online more, thus potentially exposing their financial details to abuse.

What conclusions to make from all this? Well, these questions only revealed the attitude people have towards threats and do not really reflect what actions they take to try to prevent them. But one thing is certain. Awareness of online threats has finally reached a point where even if they're fortunate enough not to have been a victim yet, the majority know that a great variety of threats exist out there and that everyone is targeted and could come under attack.

Social Engineering and Social Media

David Harley CITP FBCS CISSP

I usually tiptoe carefully around false positive issues. I understand why people sometimes get infuriated by a high-impact, high-profile FP, but I also know that FPs are to some extent inevitable, that low-impact FP events happen all the time (a bit like those earth tremors that are below the threshold of a human being's natural sensors), and that the real marvel is that in a highly-pressured industry like Anti-Malware, it doesn't happen more often.

So I probably wouldn't normally comment on Symantec's inadvertently blocking access to Facebook, or if I did, it would be with sympathy (and appreciation of their prompt remediation). I couldn't help but be amused, though, at a comment I saw on a private mailing list (hence, no attribution) suggesting that this is actually a correct detection of a site that leaks your private information across the entire Internet, rather than Symantec's Facebook facepalm.

It's an amusing thought, but with a slightly bitter aftertaste. As Ira Winkler remarked at RSA Europe last week, "People don't realize what they are putting out there ... Computers are making people easier to use every day." Though perhaps a suit filed the same day in Mississippi accusing Facebook of violating wiretap statutes, breach of contract, unjust enrichment, trespassing, and invasion of privacy, is symptomatic of a wider scepticism and a not altogether unhealthy paranoia. (I hope, speaking as a professional paranoid.) The Register's Dan Goodin links the suit (chronologically, at any rate) with a blog by Nik Cubrilovic highlighting the fact that Facebook could still identify (some of) your footprints on the web even after you'd logged out of Facebook using persistent cookies.

While Facebook has subsequently addressed the issue (see here and here) to some extent and will probably dodge the class action bullet, the ease with which it slips into the role of Cookie Monster remains discomfiting.

Virus bulletin 2011: fake but free…

ESET had quite a strong representation at Virus Bulletin this year in Barcelona, starting on the first day with Pierre-Marc Bureau presenting his findings about the Kelihos botnet, David Harley and AVG's Larry Bridwell discussion about the usefulness and present state of Anti Virus testing and to the finish day, Juraj Malcho gave an exciting presentation on the current situation in the Anti Virus industry.

On the second day, our Russian researchers Eugene Rodinov and Aleksander Matrosov explained modern bootkits's capabilities for bypassing security features of 64-bit versions of Windows (mainly kernel-mode code signing policy), using the examples of Win64/Olmarik (TDL4) and Win64/Rovnix.

On the last day, before the closing of the conference, Pierre-Marc Bureau took part in a panel discussion on the strategies of tackling botnets,Robert Lipovsky presented the current situation regarding grayware supported software, PUAs and so forth.

The main problem with this type of malware is that it is difficult to verify that they are really malicious or offensive, which, generally a gray list, means that the creators of these softwares complains about why their programs were blocked, even when those are legitimate.

This year we looked at how the grayware situation has evolved in two years, how we are handling the difficult struggle against scareware and potentially unwanted applications, and asked whether there is hope for a "junk-free" internet.

White papers could be downloaded from the following links*:

- Kelihos Botnet, by Pierre-Marc Bureau: http://go.eset.com/us/resources/white-papers/vb2011-bureau.pdf

- Daze of Whine And Neuroses (but testing is fine), by David Harley and Larry Bridwell: http://go.eset.com/us/resources/white-papers/VB2011-HarleyBridwell.pdf

- Fake but free, and worth every cent, by Robert Lipovsky, Daniel Novomesky and Juraj Malcho: http://go.eset.com/us/resources/white-papers/fake_but_free.pdf

** Whitepapers are available courtesy of Virus Bulletin, which holds the copyright of them.*

OSX/Tsunami.A, a Mac OS X Trojan

ESET's research team has discovered a new threat, which was originally designed for Linux, that now can infect Mac OS X. This is a modification of Linux code originally called Linux/Tsunami and currently detected as OSX/Tsunami.A.

The threat is an IRC controlled backdoor that enables the infected machine to become a bot for Distributed Denial of Service attacks. It contains a hardcoded list of IRC servers and channels that attempts to connect to, and then the client listens and interprets commands from the channel.

The backdoor can enable a remote user to download files, such as additional malware or updates to the Tsunami code, and also executes shell commands, giving it the ability to essentially take control of the affected machine.

Two samples of the same code were found in different parts of the world, but with small modifications. Also, ESET's telemetry data indicates that there are very few hosts infected with this malware which indicates that this malware is still in the process of testing.

This threat does not have a big sophistication or complexity, so the risk to Mac users is limited.

For more information, please visit:
http://blog.eset.com/2011/10/25/linux-tsunami-hits-os-x
http://blog.eset.com/2011/10/26/updates-on-osxtsunami-a-a-mac-os-x-trojan

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 5.21%

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/Dorkbot

Previous Ranking: 3
Percentage Detected: 3.12%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely. The file is run-time compressed using UPX.
The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

3. Win32/Conficker

Previous Ranking: 2
Percentage Detected: 2.63%

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.

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.

4. HTML/ScrInject.B

Previous Ranking: 7
Percentage Detected: 2.24%

Generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

5. Win32/Sality

Previous Ranking: 4
Percentage Detected: 2.07%

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

6. HTML/Iframe.B

Previous Ranking: 5
Percentage Detected: 1.89%

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

7. Win32/Autoit

Previous Ranking: 6
Percentage Detected: 1.84%

Win32/Autoit is a worm that spreads via removable media, and some of it 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.

8. Win32/Ramnit

Previous Ranking: 8
Percentage Detected: 1.12%

It is a file infector. It's a virus that executes on every system start.It infects dll and exe files and also searches htm and html files to write malicious instruction in them. It exploits vulnerability on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remotley to capture screenshots, send gathered information, download files from a remote computer and/or the Internet, run executable files or shut down/restart the computer.

9. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 10
Percentage Detected: 0.91%

It 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.

10. Win32/PSW.OnLineGames

Previous Ranking: 9
Percentage Detected: 0.87%

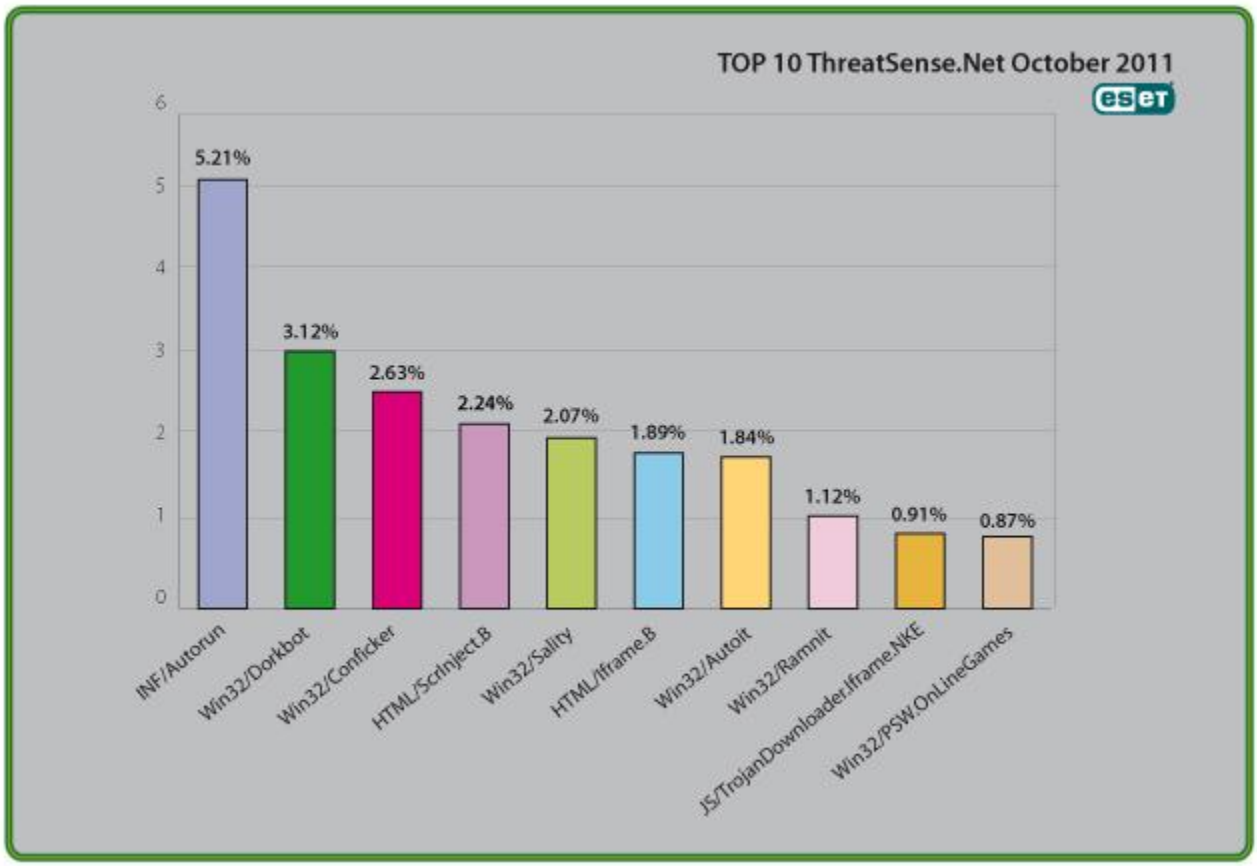
This is a family of Trojans used in phishing attacks aimed specifically at game-players: this type of Trojan comes with keylogging and (sometimes) rootkit capabilities which gather information relating to online games and credentials for participating. Characteristically, the information is sent to a 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

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 5.21% 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