Global threat report

November 2011
Feature Article: Breaking up online is hard to do ... for the Irish

Table of Contents

Breaking up online is hard to do ... for the Irish

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

Fifty ways to leave your lover? Although a tiny 1% would post hostile remarks on their ex's social media, and 8% would remove them as a contact altogether, letting go is not easy for 1 in 4 Irish people. Over 25% stay friends and follow each other's profiles even after breakup.

The networked world's social habits are changing. As email revolutionised business communication, so social networking has profoundly changed how people interact privately, and even how they start and end relationships.

Due to our expert interest in the ways online keeps getting abused and exploited in negative ways, social media – and the multitude of interactions, combined with blurred privacy awareness it entails – is a constant target of analysis and study. Technically any unlawful activity that uses computers is considered cybercrime and therefore comes under our magnifying glass. In recent times cyber-bullying, online threats and insults and similar phenomena are growing in frequency, causing increased concern and prompting taking steps, such as the proposed “panic buttons” for those being threatened.

That’s why ESET Ireland has commissioned a survey carried out by Amárach Research on 850 people, to reveal how Irish people react online and on social media after the emotionally stressful event of a relationship breakup.

The results are rather encouraging in that **only 1% showed hostile or offensive behaviour** (that could potentially result in legal action). Some **8% would hold a grudge** and delete their ex’s contact, while **11% would remain friends** even online, with another **15% regularly or occasionally checking** their ex-partner’s profile. If we combine the last two, we can come to a conclusion that letting go is not easy for 1 in 4 Irish people. Do they jealously stalk their ex’s profile to see if they’re interacting with someone new? Do they dread spotting a new “in a relationship” status? Or are they indifferent and just keep contact out of courtesy?

Some interesting regional characteristics were revealed by the demographic breakdown of the survey. For instance, the people of Munster hold the biggest grudges, as 11% of them deleted an ex immediately, while in Connaught and Ulster they seem to be the most forgiving with only 4%. Age is also a big factor. The youngest age group 15-24 is most active and dynamic online and came into all the above categories in percentages up to 26%, while the oldest were very passive and no more that 6% of 55+ fell into any of the categories above.

The majority – over 70% of people surveyed – has either never broken up, doesn’t use social networking or last broke up before social networking was a factor. We do however want to offer some advice for the unfortunate victims of that 1% of less stable ex-partners.

Most social media offer an option to block anyone from contacting you. That should be your first choice if unwanted behaviour occurs. Most social media also offer a report option, where an offender can be reported to the social media administrators and if they’re found to be regular offenders they may be banned from using that social media service. In the extreme case of receiving direct threats, blackmails or other hostile behaviour, it is best to contact your local Garda station (or the equivalent police presence in your own country), as they do also deal with online crime and they will offer you advice or take appropriate action.

Support Scams and Facebook: you don’t have to Like them

David Harley, ESET Senior Research Fellow

There seems to be another burst of unwanted attention from cold-calling scammers offering to rid you of malware and other problems that you don’t really have, and a few of my recent blogs at ESET and for SC Magazine have commented on those. However, Martijn Grooten of Virus Bulletin drew my attention to some of the techniques used by sites offering some form of PC support to give their sites more credibility. I’m not saying that all support sites are scammers, of course, but in the course of some investigations carried out by Martijn, Steve Burn and myself, it became obvious that some sites are backing up their activities with claims that are of doubtful legality.

Facebook Likes and cold-call scams focuses in particular on a company with some disquieting features apart from the indications that it does “cold call” people offering help with problems that they may not have.

eFIX’s web page lists an office in Glasgow under the name eFIX Ltd, at 8901 Marmora Road, Glasgow, D04 89GR. However, a search at Companies House, while it did turn up several entries with somewhat similar names, didn’t find one in Glasgow, and the address is a fake. In fact, the same address turns up in a great many other contexts (design consultancies, music, accountancy, even a buffet service), suggesting the use of some kind of template/boilerplate. This also suggests that it’s not only PC support companies that are suspiciously shy about their real whereabouts.

eFIX also claims to be headquartered in London and has a UK 0800 contact number, but its web site turns out to be registered by Impeccable Solutions, in Gurgaon, Haryana, India. In fact, the registration information is practically identical to that of the US-oriented Fusoft, and the two sites seem to share an awful lot of boilerplate content. However Fusoft *does* actually state that it is based in Gurgaon, though it lists a US 0800 number for contact. A little googling suggests that the same registrant is associated with other support sites: investigation continues, but the registration of multiple, similar sites suggests a site that expects to be taken down in the near future. And in fact, one of the characteristics of the current rash of support scams is that as fast as dubious sites and domains are taken down, they reappear with different names.

eFIX claims to be “several years” old, but the site seems to have been created at the end of September 2011. It might, of course, have been operating prior to the web site, but that leaves several other anomalies and inconsistencies unexplained.

One of eFIX’s Facebook pages largely consists of testimonials – or reviews – as to how good the service is. These are messages going back to the 3rd of October and appear to be from genuine Facebook users, though there is a suspicious similarity of tone, phrasing and misspelling about most of the entries that does not seem kosher. However, some entries clearly suggest that *someone* is using the eFIX FB page to reinforce a cold-calling fraud campaign.

Fusoft.org’s Facebook page turns out to consist of pointers to blog sites like http://fixinternetbrowser.blogspot.com/ and http://windowsxptechsupport.blogspot.com, whose blog articles scrape content from sources such as CNET, though the source is generally acknowledged. (Not always the case with other sites we're looking at right now, where “original material” sometimes turns out to be pasted in from older and unrelated sources and resources.)

This line of investigation set us off looking at other support sites still under investigation where the content may be more original, but the quality of the advice leads to the suspicion that the idea is less to provide a proven step-through process than to create difficulties that will persuade the victim to follow the copious links to “computer technical support providers” or “Dell technical support” or “Linksys support”, all of which lead to the same support site.

Flaky marketing techniques are easier to track than unequivocal wrongdoing (definitions of which tend to vary according to region!). However, what *is* clear is that there are a lot of companies and sites out there offering support, and even if they *aren’t* the same people making scam cold-calls – which in some cases seems pretty unlikely – they are basing their appeal to visitors to their web sites on bona fides that are pretty difficult to verify. It’s not that difficult to set up one or more new Facebook accounts and pages: unfortunately, there’s no simple and foolproof way of telling which accounts might be “dummies” set up purely to promote a product or service. Even where an account looks genuine and well-used, it’s perfectly possible that the victim of a rogue service has been persuaded to “Like” it as part of the scam, and anyone *could* fake a testimonial using stock photos and made-up names. Unfortunately, it also seems likely that we’re increasingly going to find Facebook pages and blog pages with scraped or even frankly deceptive content similarly used to add credibility to web sites whose authenticity doesn’t stand up to scrutiny. But it’s harder to trace and verify the accounts behind social media sites than it is a registered domain, and even those have their challenges.

If nothing else, this investigation should make you think twice about taking for granted the veracity of performance statistics, contact details, “Likes” and “independent reviews”: it might even ring alarm bells if a company suggests that you “Like” its Facebook page after it telephones to tell you that you have a virus.

The Internet is a wonderful thing, and even Facebook has its attractions, but not verifying the reliability of information found online can be seriously naive. If anything, it’s *easier* for a scammer to deceive you online than in the real world. Even a genuine Facebook user can be misled into misleading his or her friends.

Further links:

- http://www.crn.com.au/News/274273,indian-partner-fingered-for-microsoft-pc-support-scam.aspx
- http://securitygarden.blogspot.com/2011/09/microsoft-removes-gold-certified.html
- http://nakedsecurity.sophos.com/2011/09/21/microsoft-dumps-partner-telephone-support-scam/
- http://it.slashdot.org/story/11/09/21/2237207/Microsoft-Dumps-Partner-For-Fake-Support-Call-Scam
- http://blog.eset.com/2011/07/19/support-desk-scams-clsid-not-unique
- https://www.infosecisland.com/blogview/15066-Cyber-Criminals-Just-Came-A-Callin-At-My-House.html
- http://blog.eset.com/2011/06/24/giving-cold-callers-the-cold-shoulder
- http://www.microsoft.com/Presspass/press/2011/jun11/06-16MSPhoneScamPR.mspx

- http://www.virusbtn.com/virusbulletin/archive/2011/01/vb201101-hello

- http://www.iia.net.au/index.php/all-members/869-get-ready-for-icode-in-force-1-december-2010.html

- http://www.symantec.com/connect/blogs/technical-support-phone-scams

- http://nakedsecurity.sophos.com/2010/11/04/sick-of-call-centres

- http://blogs.protegerse.com/laboratorio/2010/11/16/llamadas-desde-el-falso-soporte-tecnico/

- http://www.eset.com/us/resources/white-papers/Hanging-On-The-Telephone.pdf

- http://blog.eset.com/2010/06/23/support-scam-info-some-more-links

- http://www.securityweek.com/fake-av-fake-support

ESET’s 10 tips for a safe holiday shopping online

The holiday season is coming and ESET has put together 10 tips for safer holiday shopping online. Even more holiday shopping will happen online this year than last and that means more scammers will be looking to do some shopping of their own, possibly at your expense. This might involve using **your** credit card and bank account to fund **their** gift-buying, or perhaps capturing and selling your personal information so they have some extra holiday cash.

Here are some of the tips that Cameron Camp and other ESET researchers have put together to help savvy cyber-shoppers avoid getting scammed while hunting for the best holiday deals online:

1. **Tune your shopping machine:** Like the tune-up your car might be getting before a long drive to deliver holiday gifts to relatives, your laptop may need a little attention before going online for some power shopping. Give it some love, and improved protection, by updating and patching your browser, operating system, and anti-malware suite. Patching will help you avoid malware infections and scams, and keep you running smooth throughout the season, and it’s free.

2. **Stick with familiar faces:** Buy from websites that have established a reputation for doing what they say, providing accurate descriptions of merchandise and delivering it in good shape and on time. When you’re getting down to the wire with shipping deadlines, the last thing you need is friends and relatives getting the wrong gifts, which could be worse than no gifts at all.

3. **Be wary of AMAZING deals:** If it looks too good to be true, it probably is, particularly if it’s an amazing offer on one of the hottest products of the season. Such deals can be very tempting, but it really is safer to avoid following links that offer goods, services, or gift cards at impossibly cheap prices, they are just too risky. Not all discount vendors are scammers, but ask yourself if the promised savings are worth the gamble (or Google the offer and/or vendor to see what others are saying).

4. **Insist on secure transactions**: When you are in the

ordering process on a website check to make sure it is using SSL, the standard in secure transactions that shows up in several ways. You should be able to see **https** or **shttp** in front of the web address instead of http. There may also be a lock or key symbol in the browser window as well. Using SSL encrypts the exchange of information, such as your credit card, so eavesdroppers cannot read it. When in doubt, a quick search in Google for the word "scam" or "fraud" along with the site name should tell you if that site has a history of problems.

5. **Think before you act**: Watch out for URGENT deals that arrive in unsolicited email or purport to be from friends on social networking sites. Exercise extra caution if the message uses broken English (or whatever your native language might be) or if it doesn't seem quite right for some reason. If you think the deal is real, open a browser and type the name of the website directly into the address bar. This will keep you from getting swept away by scam links to fake websites built by cyber crooks that harvest your information and spirit it off to the underworld (the black market in stolen identity data).

To take a look at the rest of the 10 tips for safer holiday shopping online, you can visit ESET's Blog "Cyber Monday Safety: 10 tips for safer holiday shopping online" or if you want to print them and share them with your friends and family, you can access a PDF version of The ESET Guide to Safer Cyber-Shopping: 10 Tips for Happier Holidays

Evolution of Win32Carberp: going deeper

This month our laboratory in Russia discovered a new modification in the Win32/TrojanDownloader.Carberp Trojan family, one of the most wodely spread malicious program in Russia.

The criminals behind Carberp are one of the biggest groups related to banking fraud. The average income of the group is about several million US dollars a week and, as we can see in the evolution of Hodprot, they invest a lot of money in the development of malware technologies. An example of this is that the Carberp Trojan has now bootkit functionality, although is still working in test mode.

After analyzing this new version of the threat, it has been discovered that this bootkit is almost identical to Rovnix bootkit, but the installer has been changed. In this case, it installs the bootkit and tries to exploit several vulnerabilities to escalate its privileges. It also removes various hooks from a list of system routines just before installing the Trojan or bootkit to evade sandboxes and other monitoring software.

For more information you can read David Harley's extensive post on the Evolution of Carberp.

Cyber criminals behind 96% of attacks on Irish websites

The Irish reporting and information security service (IRISSCERT) revealed at their conference in Dublin, that they received 441 security incidents reports in 2011, 92% of which related to Irish websites being broken into by criminals to host phishing sites to target unsuspecting users.

As you have read in one of this month's feature articles, ESET Ireland has also been conducting it's own research and one research project led to the following results:

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

The scale of this problem could be reduced by improvements to user behavior, however research indicates that Irsh computer users are reluctant to behave safely online. Some 34% of surveyed computer users said they ignore alerts from their antimalware software.

One the positive side, research project revealed the password habits of users in Ireland were above the global average. At least a third of Irish computer users have set up passwords that include a suitable mix of letters and numbers, rather than just a simple sequence of letters or numbers. However, among a fifth of those surveyed (even more in Connaught and Ulster) use of overly simple passwords was still widespread.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 4.38%

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://blog.eset.com/?p=94 ; http://blog.eset.com/?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: 2
Percentage Detected: 3.43%

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. HTML/ScrInject.B

Previous Ranking: 4
Percentage Detected: 2.40%

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

4. HTML/Iframe.B

Previous Ranking: 6
Percentage Detected: 2.24%

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.

5. Win32/Conficker

Previous Ranking: 3
Percentage Detected: 2.20%

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://blog.eset.com/?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.

6. Win32/Autoit

Previous Ranking: 7
Percentage Detected: 1.53%

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.

7. Win32/Sality

Previous Ranking: 5
Percentage Detected: 1.03%

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

8. Win32/Ramnit

Previous Ranking: 8
Percentage Detected: 0.97%

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: 9
Percentage Detected: 0.79%

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: 10
Percentage Detected: 0.75%

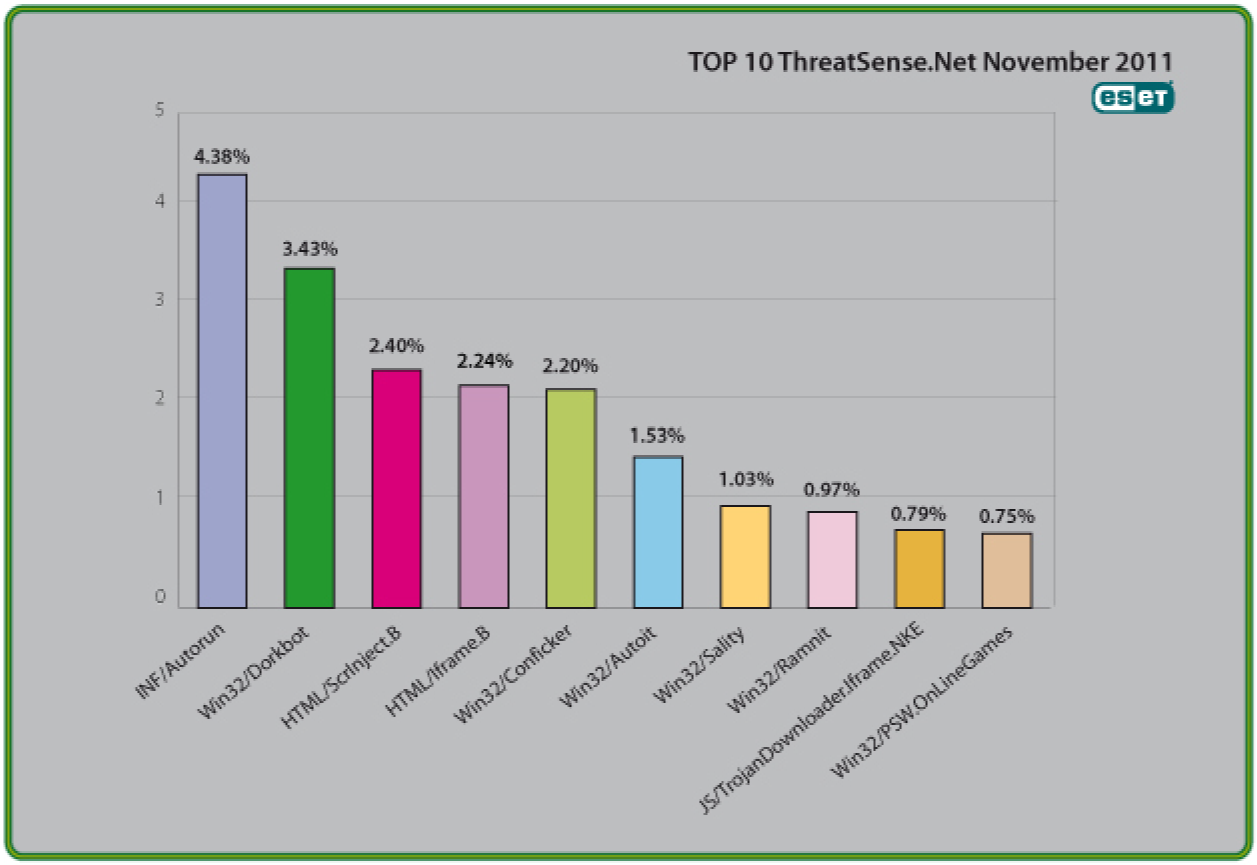
This is a family of Trojans used in phishing attacks aimed specifically at game-players: this type of Trojan comes with keylogging and (sometimes) rootkit capabilities which gather information relating to online games and credentials for participating. Characteristically, the information is sent to a 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 4.38% 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