February 2012

Feature Article: Cybercrime and Punishment

ESET

Table of Contents

Cybercrime and Punishment

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

I spent a couple of days in February at the National Cyber Crime Conference in Sheffield, UK.

I was invited there to talk about those PC support scams that have been raising my blood pressure for a while. (That's a topic I'll be returning to sooner rather than later.) While I very much enjoyed the opportunity to raise the issue with such a highly influential group of law enforcement representatives, it was also a great opportunity to indulge my natural curiosity as to what the recent political announcements on measures to counter cybercrime mean in practice, in the part of the world I actually live in.

If you're interested in the bare bones of the conference put on by the Association of Chief Police Officers (ACPO) and the Police Central e-crime Unit (PC^{e}U), you can get the basic info about the central event – that is, the formal rolling out of three regional e-crime hubs in Yorkshire & Humber, the North West, and the East Midlands – from articles by Dan Raywood and/or John Leyden. I want to talk about some of the detail, though. (I made a *lot* of notes, so I'll probably be back with commentary on some of the other issues that caught my attention.)

In a depressed economy in a (fairly) liberal country (i.e. one where law enforcement's primary concern is not necessarily the maintenance of the political status quo), the public sector is at least as susceptible to budgetary restriction and cost/benefit analysis and monitoring as anyone else, being expected to perform miracles of efficiency. So it's not surprising that the cost effectiveness of the PC^{e}U was a topic that came up time and time again in presentations. And cost-effective it does indeed seem to be: a major driver here is the reduction of financial harm to the UK economy, and the target of saving £504 million pounds in four years looks not only achievable, but on course to be very comfortably exceeded. The unit's Financial Harm Reduction Report claims a harm reduction figure of £140 million over the period 1st April – 30th September 2011, the equivalent of 1:35 ratio of cost to harm reduction. In other words, the unit achieved a little less than 28% of its four-year performance target in six month.

I don't claim to have looked in detail at all the calculations that underpin the report, but it's a fascinating insight into investigations into criminal operations like the Ghostmarket forum, a late and unlamented resource for those with an unhealthy interest in activities such as carding, auction scamming, and even bomb making. An investigation (Operation Pagode) into that group claims a conservatively estimated Police Costs to Harm Reduction Ratio of 1 : 73. Operation Dynamophone, an investigation into banking and credit card phishing, claims a 1 : 19 ratio, while the more generic Operation Papworth claims an extraordinary ratio of 1 : 6622.

But it's not *all* about cold financial analysis: a motif that occurred time and time again in the course of the conference was that 'cybercrime is not victimless crime'. I've no idea how or if the attacks by 'ColonelRoot' on the web hosting company 'Punkyhosting' were factored into the calculations relating to the Organized Criminal Group behind Ghostmarket, but the use of material from Andrew Laws' blog gave a very appropriate expression to the voice (literally – Andrew wasn't there in person) of just one victim, talking about how he was affected personally both by the attacks and by the subsequent trial of Zachary Woodham and Louis Tobenhouse. As AV researchers, we tend to focus on the bits and bytes of malware and other attack methodologies: it's not a bad thing to be reminded occasionally that the real-world impact on victims is a matter of psychological and personal financial damage, not just

prevalence statistics and cost/benefit analyses.

A persistent motif of the conference was the need to raise awareness and understanding. Firstly, in the context of mainstreaming: that is, "raising the bottom bar" by giving non-specialist police training in and better understanding of the field, so that they are better equipped to handle investigations – it seems to be a given that cybercrime (or crime with an IT dimension, to avoid getting too entangled in definitions), is where the money is, certainly at all levels of fraud, and already dwarfs what we might call conventional or street crime. And, of course, to improve the quality of the advice they're able to give the general public.

It's a short step from there to educating the public. In the security industry, there are many very bright people who believe that if education was going to work, it would have worked by now. They're right: education is not going to fix this. And they're wrong: technology isn't going to fix it, either. Get Safe Online, about which Tony Neate talked at some length, is an initiative co-sponsored by government, law-enforcement and the commercial sector (notably the security industry), and seems to be prioritizing helping the man-in-the-street to take some of the responsibility for his own safety by raising his awareness of risk and understanding of how he can reduce that risk through better understanding. If you see that approach as an acknowledgement of a failure of resourcing, policy or technology, get over it. A very high percentage of Internet crime could be reduced purely by the application of common sense and a little knowledge of the (wicked) ways of the online world, and Get Safe Online is providing some well-thought-out resources for distributing that knowledge.

A survey quoted by Neate indicated that 34% of the survey population felt they knew the basics of infosecurity, and 35% feel that it's primarily their own responsibility to look to their own safety. That in itself seems to me to demonstrate the size of the challenge, but also shows just how necessary it is to try to meet that challenge. Security *can't* be purely the responsibility of the government, the police, the security industry, the ISPs, the public sector, private industry, or any permutation thereof.

And if you think it's odd that someone with longstanding ties to a company marketing technological approaches to consumer safety should be advocating generic educational approaches, perhaps I can direct you to Securing Our eCity, an example of a somewhat similar initiative in the US with which ESET North America has been heavily engaged for some years now.

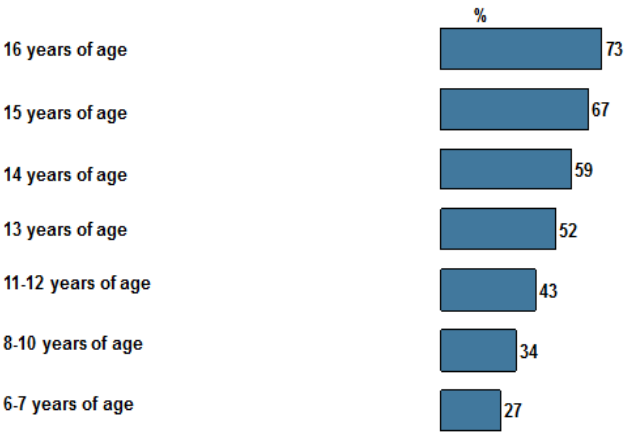
Has the web become a nanny for Irish parents?

Urban Schrott, ESET Ireland

Imagine the Internet is like a large city. Like any large bustling city, with everything fun and useful it offers, the Internet also has its shady streets and underpasses full of criminal and malicious activity. But while most parents are concerned where their children would go alone in a busy city, they seem much less concerned about where they go online.

That is why we have commissioned a survey from Amárach Research, to find out how Irish parents supervise their kids' activities online. The results, based on a sample of over a thousand people, surprised us a bit.

Question: Is your child left unsupervised online?
The graph shows how many parents of children of a certain age said YES.



We asked if children of different age groups (ranging from 6 to 16) were left unsupervised online, and it turns out parents seem to supervise less and less as the children age. So the youngest group of 6-7 years of age were only left unsupervised in 27% of the cases, then supervision drops incrementally to 73% being unsupervised in the 16 years age group.

While this seems to make sense in the usual state of affairs of bringing up children and handing over responsibility as they mature, in the case of being online, it is perhaps worth pointing out that the Internet has bad neighbourhoods and shady corners for every age group (adults not excluded). You have possible paedophiles out there preying on the youngest and most vulnerable, but also illegal music, movies and software downloading and pornographic websites with their malware loads infecting the computers of the older ones. And then if they do online shopping as well and have their credit cards compromised … well you get the picture. Not to mention the older children age groups also probably spend most time online, and should therefore be especially educated about things such as Facebook privacy, safe online shopping and malware threats.

Most parents will probably say *"But my child knows much more about computers than I do!"*, so how to stay on top of what's going on? At ESET Ireland we're aware that online security isn't just a battle between evil malware and good security software, but that it is instead a complex mix of measures, practices and awareness as well. So here's what we suggest:

- Know the dangers out there and talk about them with your family. Explain to your children which things are dangerous and how to avoid them.
- You should know what your children do with the computer. Do they download pirated material and run cracked software and shop online on the same computer? Do they surf dangerous websites?
- You should know who they talk to when online. Is it only friends and acquaintances or also unknown people, engaging them in potentially unwanted activities.
- Special attention should go to Facebook and other social media privacy. How posting inappropriate content can get one in trouble and how to avoid cyber bullying.
- Think about installing Parental Control software which lets you monitor and limit computer use, as well as block many categories of offending websites and programs.

Stay safe online. Think before you click. More information on current threats at
https://www.facebook.com/eset.antivirus.ireland

The month in social networks

ESET'sResearcher Cameron Camp looked at the privacy implications and security settings of Pinterest, the rapidly expanding social network for sharing one's interests in his article "Pinterest.com security – step by step how-to".

In this post Cameron explains some of the options at the time of singing up:

- Methodology of singing up (similar to the early days of Gmail).
- Settings of Facebook interface.
- Revision of social network's privacy settings.
- Explanation of the settings of the integrated "pin it" button.

So if you're interested in having a profile in Pinterest, we suggest you to check this post and follow its recommendations.

One of February's highlights is Valentine's Day and ESET took special note of scams involving this theme, documented by researchers at ESET Latin America in a report that was translated into the blog. This post called Valentine's Day Scams: For the love of money covers the different techniques for the implementation of those scams:

- **Malware in social networks**: Social networks are a major vector for attacks using social engineering.
- **Black Hat SEO**: After social networks, search engines are the primary means used by the attackers to lure users to malicious sites.
- **Fake Greetings Cards**: Cybercriminals are well aware of this, which is why they circulate fake cards and fake weblinks purporting to point to such cards
- **Privacy and Theft information**: there are many applications associated with social networks (especially Facebook) that take advantage of their victims' romantic susceptibilities to trick them into giving them access to far too much information.
- **"Russian Bride"**: For many single people, this is a date on which they too are more susceptible to romantic feelings and advances. So it's not surprising that we also tend to see greater volumes of emails trying to deceive them

Also regarding Valentine's Day, Stephen Cobb wrote "Cookie-stuffing click-jackers rip off Victoria's Secret Valentine's giftcard seekers". This post explains how attackers implement some innocent-looking links as part of fraudulent activities such as cookie-stuffing and click-jacking. Some concepts are explained:

- **Cookie stuffing:** is an abuse of affiliate marketing cookies intended to mark a visit to a website that an affiliate has initiated, and for which that affiliate will get paid if the consumer performs pre-defined tasks, like requesting more information.
- **Click-jacking:** can be narrowly defined as deceiving a user into clicking on things they did not intend to click on, or clicks which lead to pages or actions other than those the user expected when clicking.

Stephen also wrote an article entitled "How to improve Facebook account protection with Login Approvals" which explains the "Login Approvals" feature added recently to Facebook. This article also describes the entire process of activating this feature and how to correctly configure it.

Carberp: the Russian Trojan banker now aims Facebook users

David Harley and a Russian research colleague, Aleksandr Matrosov, explain that the most widely spread banking trojan in Russia is now trying to steal money from Facebook users. ESET researchers noted that Win32/Carberp used bootkit components from malware called Ronix, which was also the subject of scrutiny in February.

The article specifies different kind of information about this threat such as:

- Fake Facebook Lockout
- Demanding e-Cash
- Faking Facebook
- Web-Injects
- Carberp Detection in Russia
- Global infection statistics
- Bypassing DDoS Prevention Systems

The complete description can be read from Facebook Fakebook: New Trends in Carberp Activity.

Also, there was a related post to new trends in Carberp Activity is Rovnix Reloaded: new step of evolution which explains the new developments of this threat. This is detected as Win32/Rovnix.B trojan, this appears to be the first bootkit to employ VBR (Volume Boot Record) infection.

Different topics to secure endpoints

At ESET we tend to think end user education is a big part of securing endpoints. The importance of providing security guidance to users was stressed on different articles.

- Stephen Cobb's post entitled Security awareness, security breaches, and the abuse of "stupid" reflects de importance of education and gives some examples of users thoughts, such as:

  Think of Facebook as a place to share things with a few select friends, but have not adjusted their "share" settings accordingly.

  Under-estimate the number of people who are willing to take advantage of their fellow human beings.

- In addition to this, David Harley explained in his article "Your Children and Online Safety" the importance of supervision of children on the web by their parents. In his article David focuses on some inferences:

  - Know (and discuss) the dangers. I'd suggest that

with younger children, learning about safety issues could be a family project where parents and children could learn from each other.

- Issues such as piracy aren't just moral issues (important though moral issues are): they have dangerous practical implications, too.

- The web (and especially social media sites) is about social interaction with people you or your children may never have met. The idea of Facebook as a paedophile's playground may be overstated, but it's not fiction.

- David also wrote two articles sharing his observations from the ACPO National Cyber Crime Conference held recently in the UK. These articles are online and yo can read them: Cybercrime, Cyberpolicing, and the Public and Cybercrime and Punishment.

- Cameron Camp wrote on his article entitled "Google responds to Android app Market security with stronger scanning measures" about the process of scanning for potentially malicious software. In response to recent reports that malicious apps may have made their way into the official Android Market, Google has responded by announcing a new program to more proactively scan the Market and developer accounts for seemingly malicious apps and highlights and/or remove them before users experience trouble.

- Arye Goretsky considers the security aspects of another mobile platform in his article Windows Phone 8: Security Heaven or Hell?

Recent ESET publications

ESET researchers are often invited to write for other publications. Here's a selection of articles that have appeared elsewhere this month.

Virus Bulletin

David Harley: "Living the Meme" (available to subscribers only)

Hakin9

David Harley, Aleksandr Matrosov, Eugene Rodionov: "When I'm x64: Bootkit Threat Evolution in 2011"

Network Security

David Harley: "AMTSO: the Test of Time?" This article appeared in January's Network Security but is now available from Elsevier as published (including formatting, proofing and graphics) here, or there is a no-fee pre-edit copy available (by permission of the publisher) from the AMTSO blog here.

SC Magazine Cybercrime Corner:

- U.K. MPs bite the cyber bullet...
- Towards a safer internet
- My not-so-funny valentine

(ISC)2 Blog

David Harley: Android, Malware and Rehabilitation

Infosecurity Magazine:

David Harley: Malware: a Matter of Definition

The Top Ten Threats

1. HTML/ScrInject.B

Previous Ranking: 1
Percentage Detected: 3.93%

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

2. INF/Autorun

Previous Ranking: 2
Percentage Detected: 3.77%

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.

3. HTML/Iframe.B

Previous Ranking: 3
Percentage Detected: 3.38%

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.

4. Win32/Conficker

Previous Ranking: 4
Percentage Detected: 1.93%

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.

5. HTML/Fraud.BG

Previous Ranking: n/a
Percentage Detected: 1.64%

HTML/Fraud.BG is a trojan that steals sensitive information by displaying a dialog window asking the user to take part in a short survey and the goal of the malware is to persuade the user to fill in. The trojan attempts to send gathered information (such as telephone number and e-mail) to a remote machine.

6. JS/Kryptik

Previous Ranking: 35
Percentage Detected: 1.30%

JS/Kryptik is generic detection of malicious obfuscated JavaScript code embedded in HTML pages. JS/Kryptik usually redirects the browser to a malicious URL or implements a specific exploit.

7. Win32/Dorkbot

Previous Ranking: 5
Percentage Detected: 1.18%

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.

8. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 7
Percentage Detected: 1.07%

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.

9. Win32/Sality.NBA

Previous Ranking: 8
Percentage Detected: 0.84%

It's a variant of Sality, 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

10. Win32/Spy.Ursnif

Previous Ranking: 10
Percentage Detected: 0.66%

This is a spyware application that steals information from an infected computer and sends it to a remote location, creating a hidden user account, in order to allow communication over Remote Desktop connections.

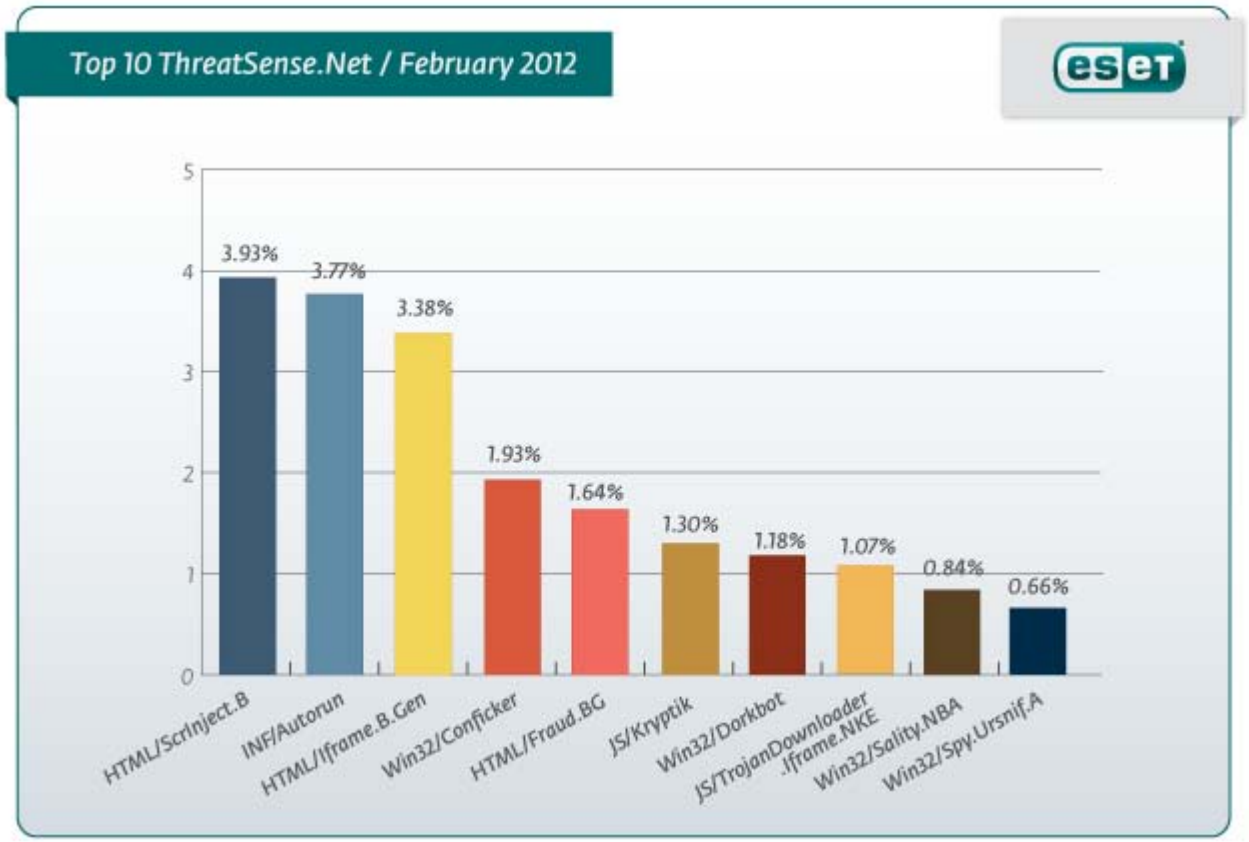
While there may be a number of clues to the presence of Win32/Spy.Ursnif.A on a system if you're well-acquainted with esoteric Windows registry settings, its presence will probably not be noticed by the average user, who will not be able to see that the new account has been created.

In any case it's likely that the detail of settings used by the malware will change over its lifetime. Apart from making sure that security software (including a firewall and, of course, anti-virus software) is installed, active and kept up-to-date, users' best defense is, as ever, to be cautious and proactive in patching, and in avoiding unexpected file downloads/transfers and attachments.

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 3.93% of the total, was scored by the **HTML/Scrinject.B** 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