February 2013
Feature Article: Academic Vanity Press: Who Gets Scammed?

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Academic Vanity Press: Who Gets Scammed?

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

A version of this article was originally published by the Anti-Phishing Working Group in its eCrime blog.

I'm not a regular denizen of the ivory halls and towers of academia, despite having the title Senior Research Fellow at ESET and being a Fellow of the BCS Institute (the current name for the British Computing Society). However, I've recently become aware of a journal paper submission scam for which even a quasi-academic is apparently a suitable target. At any rate, I recently received a minor blizzard of emails offering me the opportunity to submit a paper to one of several dozen open-access, peer-reviewed online journals, *and* to join them as an editorial board member or reviewer.

People *do* ask me to write, edit or review for them from time to time - after all, my primary job is authoring - but they're usually rather more precise about *which* site or publication they want me to contribute to. They don't let me choose from a variety of publications in disciplines of which I have no experience whatever. Most of them don't expect to pay me for my efforts, but that's fine: people who write blogs and papers that are published by a security company usually also write on behalf of the same company for reputable third parties like the Anti-Phishing Working Group, local press, specialist security magazines, and so on. The third party gets a wider spread of expertise than if it only used in-house staff, especially if the writer is already established; the security company and the author get a wider audience and are seen as a force in the knowledge-sharing research community, not just a marketing operation.

However, in this case it was money that was wanted, not my presumed expertise or reputation. The spammer doesn't seem to know what my field of expertise actually is. And it turns out that if you want to be an editor or reviewer, you first have to submit a paper. The cost of processing the article (copyedit, proofreading, and publication on acceptance) is up to $500 (but would have entailed a very substantial discount if I'd submitted it before January). It turns out that some similar organizations charge 3-4 times that much, though again they often offer impressive discounts.

Welcome to the seamier side of Open Access. Not that OA is in itself fraudulent. In principle, it provides unrestricted access to scholarly, peer-reviewed journal articles. Instead of the reader paying for access (for example, by paying a yearly subscription fee or for individual articles), the business model is largely reliant on the cost of publishing being borne by the author. It's actually quite a complex and varied model, but for many academics and academic departments, publications constitute an essential performance metric, a numbers game that boosts their claim to tenure and gives them an advantage in the job market. Research information is both a core product and a marketing asset, so it can work very well.

However, it may come as no surprise that there are journals whose review process is less rigorous than you'd expect. On the other hand, what may be more surprising is how many Open Access journals have little or no content, or cheerfully include articles from disciplines different to the one indicated by the journal title, or include names on editorial and review boards of people who have never agreed to participate, or whose credentials are seriously misrepresented. I guess it's not a scam if you get what you want out of it: if buying your bibliography by the yard - the way some people buy books for their study - makes your résumé look more attractive, you may consider it

worth the money. But if you obtain and maintain your position by *buying* credibility at the expense of those who earn theirs, doesn't that mean that an academic employer is being cheated, and the academic community as a whole being short-changed? Is there a lot of difference between buying exposure in a dubious pseudo-academic publication and buying your self a degree from an email spammer?

Free Isn't Always Better

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

A different version of this article was originally published on the ESET blog.

ESET Ireland's Urban Schrott has blogged recently that "Research reveals nearly half of all Irish computers depend on free antivirus for protection". That proportion isn't in itself surprising: there are several options for anti-virus products that don't cost anything for home users, and plenty of people who "believe that a free antivirus is equally effective in keeping their computers safe as a full security suite," and more than a few irresponsible 'security experts' suggesting on the basis of spurious statistics and imperfect misunderstanding (hat tip to Kurt Wismer) of modern anti-malware technology that AV is not worth paying for.

Urban notes:

> *"Online security these days goes far beyond just sets of virus definitions as was the case with antivirus a decade ago. The multiple-vector attack nature of modern malware and cybercrime in general forces effective security suites to integrate antivirus, firewall, anti-spam, social media scanners and scam-site detectors, using traditional definition-based malware recognition, combined with proactive, behavioural heuristic detection. That is then also backed up by large teams of security experts and analysts, who monitor the web 24/7 for new outbreaks and new forms of attack as well as offer tech support to their users."*

But his statistics (based on a poll commissioned by ESET Ireland) also throw up some interesting sidelights on consumer habits and attitudes that I'm sure are reflected in other parts of the world.

- 45% of users use free AV, which is a lot better than being one of the 5% using no security software at all (as long as you're using a competent mainstream program and you're not one of the "3% minority … mad enough to use pirated antivirus.")

- Still, it's actually quite encouraging that a good proportion of those surveyed use a licensed security suite or a licensed AV product in combination with other security software. Not only because licence payments for anti-malware keep people like me in steak and Merlot, but because it shows that there are people with a healthy recognition that AV is not sufficient protection.

There's also some demographic analysis indicating that women are more cautious (and likelier to pay for security software) than men, while the youngest age-group is also the most reckless. (This is well in line with other research from the same source.)

Inevitably, one comment posted to the ESET Ireland blog

accused Urban of 'lame FUD', to which he responded trenchantly: "It isn't FUD to say that AV (free or not) doesn't have the same defensive capabilities as a security suite, or that free AV isn't as well supported as its for-fee equivalent. That's the trade-off and we're far from the only ones saying it."

In fact, the AV market is not simply divided into free and commercial scanners. There are a few scanners that are completely free, though I can't think of one I'd recommend. There are scanners that are free for non-commercial use. There are short-life evaluation copies of commercial scanners (and even full suites) like ESET's 30-day trials. There are free web-based scanners (we have one of those, too), though they're not a complete substitute for a full-blown AV product, free or otherwise. There are fully supported commercial scanners that don't have all the bells and whistles of a security suite (best used in tandem with other types of security software such as a personal firewall). And there are full-blown security suites, which provide multilayered protection but are hardly ever free.

While free AV doesn't contribute anything to my steak and Merlot fund, it's a good thing that people are using it: as long as it's a legitimate and competent product, it's a great deal better than no protection at all. But it's a dangerous world out there, and free AV doesn't mitigate as many risks as a full suite, and it isn't as well supported. To claim otherwise is just wishful thinking.

Righard Zwienenberg went into considerable detail on the 'hidden costs' of free AV in Why Anti-Virus is not a waste of money.

Job Scammers Will Take Anyone's Money

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland
David Harley, Senior Research Fellow, ESET North America

It's all too common for job offers to turn out to be some form of 419 or other Advance Fee Fraud (AFF) or a poorly paid work-from-home job. However, sometimes the job offered actually involves participating in money laundering as a money mule, though oddly enough, that's never the job title - that's more likely to be something like 'financial assistant' or even 'financial director'. Unfortunately, it's possible for a naive victim to believe they're working for a legitimate company and not realize that they're breaking the law until the police come a-knocking.

These are global problems, not just an issue in Ireland, but apart from an overwhelming quantity of online banking scams hitting Irish mailboxes, ESET Ireland has in the recent months observed that the cybercriminals are also working particularly hard on exploiting the misfortune of those worst hit by the economic situation, with the same immoral cynicism they apply when promoting fake charities or fraudulent donations during natural disasters.

Official-looking emails, equipped with company logotypes and addresses, are circulating, offering everything from easy and affordable loans, offers to work from home for an online enterprise, to completing financial transactions and taking a cut for yourself. All topics specifically aimed at those that found themselves out of work and regular income.

EMPLOYMENT APPLICATION FORM

First Name _____Middle Name_____ Last

Residential Address_____

City _____State _____ _____Zip _____

Home Telephone Number_____

Personal cell phone Number_____

Gender _____ Marital Status _____

Age _____ Nationality

_____

Please note: Only interested applicants should respond to this offer. IF YOU INTERESTED KINDLY REPLY BACK AT [redacted]

WHAT YOU NEED TO DO FOR US?

My Company needs a financial representative who will serve as our Agent in processing any of our funds made out to us by our CANADA, EUROPE & AMERICAN customers, Why we need you to represent us there is because the payments Takes a long period of time to clear in our banks in UK, and due to Frequent Request and supplies of product we do not meet our demand due to this Failure So that why we seek your time and assistance.

JOB DESCRIPTION

1. Receive payment (America Cheques/EUROPE DRAFT) from Clients which will get to you through a courier service

2. Cash Payments at your Bank

3. Deduct 10% which will be your percentage/pay on Payment processed. 4. Forward balance after deduction of percentage/pay to any of the Offices you will be contacted to send payment to (Payment is to Forwarded By Western Union Money Transfer).

Even if they sound promising enough and will claim to provide the receiver with something, either a loan, a job or a transaction fee, most of these offers will sooner or require the victim to pay some advance fee or provide some delicate personal data, such as bank account or credit card numbers, or they will go straight for the main prize.

How does the scam part usually work then? The victim receives an uncovered cheque or other counterfeit proof of payment to themselves, while they are expected to forward on their actual funds immediately. By the time they get confirmation they didn't actually receive anything from the scammers and that the checque or other proof of payment is worthless, they have already parted with their own money via the untraceable Western Union and the scammers walk away with a hefty profit.

This is a slightly different example, though.

> *I would like to know if you are interested to work from home for us*

This looks like a money mule solicitation, the sort of 'job offer' by which someone out of work might be particularly vulnerable to being conned. And in fact, the victim may actually make some money out of the deal. But it's still bad news for someone who takes up the offer, who is likely to find that sooner or later he'll attract the attention of the police and be left holding the bag, with his bank account closed and his assets frozen, at least until it can be sorted out what proportion of those assets have been acquired through involvement in money laundering. The

sad thing is that the victim may honestly believe he has a legitimate job for a legitimate company, hard though that is to understand for anyone with a modicum of healthy scepticism. Of course that doesn't mean the scammer won't demand some sort of advance fee in order to get a little extra profit, and in fact we see 419 versions that are probably more interested in scamming the recipient than in real money laundering.

Needless to say, the golden rule "If it sounds too good to be true, it probably is" should be applied rather vigorously to most, if not all, such emails. The only goal of the cybercriminals is to make money. Any offers they make, any promises or good deals they offer, all serve their main purpose, to get to some of your money and make it theirs.

Spam filtering should limit the amount of such scams you receive, but some may also arrive through Facebook messages, chat or phone texts. In either case, use common sense if you receive them, do not reply to any of them and warn your friends to be careful too.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 3.32%

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. HTML/Iframe.B

Previous Ranking: 2
Percentage Detected: 2.99%

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

3. Win32/Sality

Previous Ranking: 5
Percentage Detected: 2.17%

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

4. HTML/ScrInject.B

Previous Ranking: 3
Percentage Detected: 1.96%

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

5. Win32/Dorkbot

Previous Ranking: 8
Percentage Detected: 1.81%

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.

6. Win32/Ramnit

Previous Ranking: 7
Percentage Detected: 1.74%

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.

7. Win32/Conficker

Previous Ranking: 6
Percentage Detected: 1.39%

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.

8. Win32/Qhost

Previous Ranking: 4
Percentage Detected: 1.31 %

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.

9. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 9
Percentage Detected: 0.84%

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.

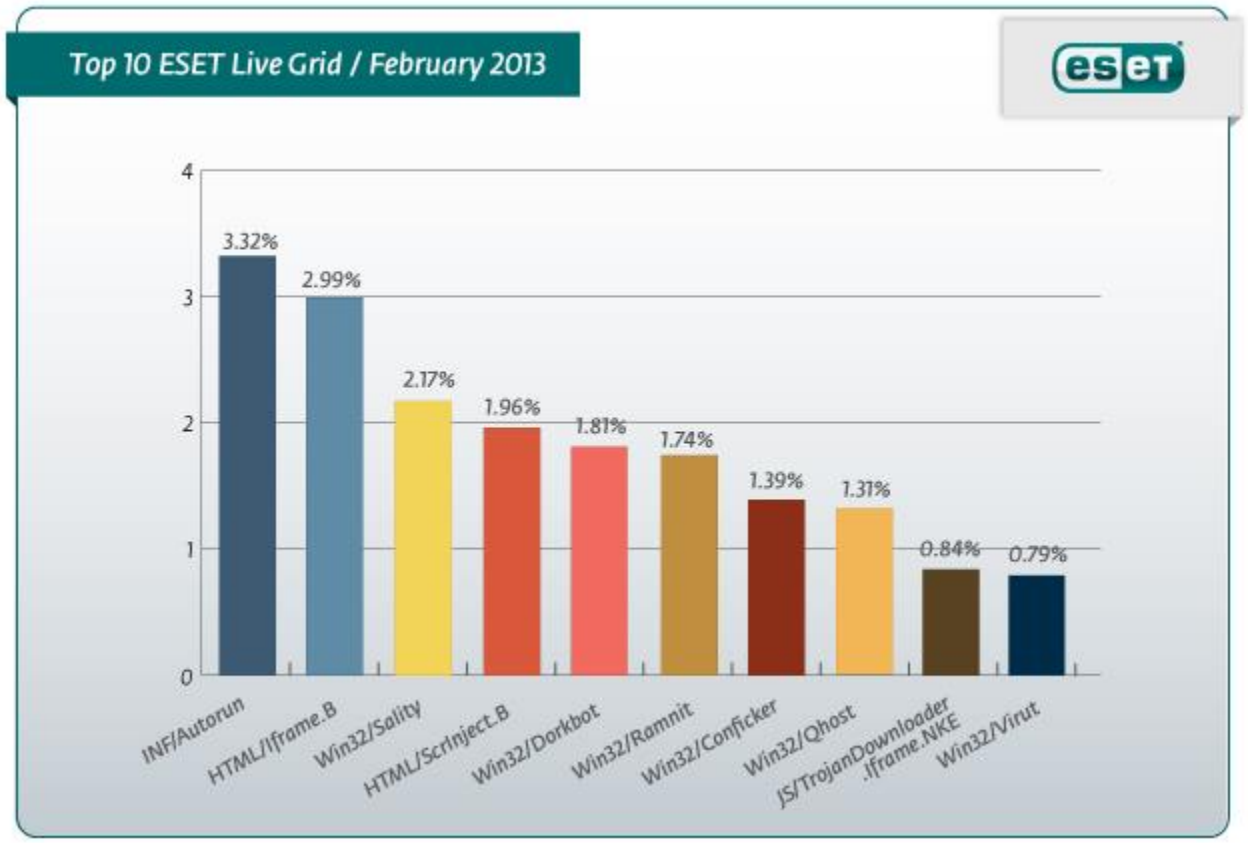
10. Win32/Virut

Previous Ranking: 32
Percentage Detected: 0.79%

Win32/Virut is a polymorphic file infector. It affects files with EXE and SCR extensions, by adding the threat itself to the last section of the files source code. Aditionally, it searches for htm, php and asp files adding to them a malicious iframe. The virus connects to the IRC network. It can be controlled remotely.

Top Ten Threats at a Glance (graph)

Analysis of ESET LiveGrid®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 3.32% of the total, was scored by the INF/Autorun class of threat.



About ESET

ESET®, the pioneer of proactive protection and the maker of the award-winning ESET NOD32® technology, is a global provider of security solutions for businesses and consumers. For over 26 years, the Company continues to lead the industry in proactive threat detection. By obtaining the 80th VB100 award in June 2013, ESET NOD32 technology holds the record number of Virus Bulletin "VB100" Awards, and has never missed a single "In-the-Wild" worm or virus since the inception of testing in 1998. In addition, ESET NOD32 technology holds the longest consecutive string of the VB100 awards of any AV vendor. ESET has also received a number of accolades from AV-Comparatives, AV-TEST and other testing organizations and reviews. ESET NOD32® Antivirus, ESET Smart Security®, ESET Cyber Security® (solution for Mac), ESET® Mobile Security and IT Security for Business are trusted by millions of global users and are among the most recommended security solutions in the world.

The Company has global headquarters in Bratislava (Slovakia), with regional distribution centers in San Diego (U.S.), Buenos Aires (Argentina), and Singapore; with offices in Jena (Germany), Prague (Czech Republic) and Sao Paulo (Brazil). ESET has malware research centers in Bratislava, San Diego, Buenos Aires, Singapore, Prague, Košice (Slovakia), Krakow (Poland), Montreal (Canada), Moscow (Russia) and an extensive partner network for more than 180 countries.

More information is available via About ESET and Press Center.

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 (also available at welivesecurity.com)
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation