May 2013
Feature Article: Facebook, Scepticism, and the Antisocial Media

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Facebook, Scepticism, and the Antisocial Media

David Harley CITP FBCS CISSP ESET Senior Research Fellow

[A version of this article originally appeared on the ChainMailCheck blog.]

You may be surprised to know that Facebook's automated monitoring of the content posted by its subscribers is quite stringent. Certainly it shocked me slightly that when I mentioned – in distinctly unflattering terms – a domain well-known for its frequent misuse by spammers and scammers, Facebook not only stopped me from posting the comment, but assumed my account had been compromised and suspended it until I logged back in and changed my password. Sadly, this doesn't mean that Facebook is always going to stop you from writing, liking or sharing inappropriate content.

Recently I came across an article on Trial by Facebook – Dangerous Trends by Craig Charles Haley. Haley makes some good points about the use and misuse of vigilantism in the social media, though such ugliness as 'Fred Bloggs is a hacker' hoaxes (see also the It's a wonderful hoax article on We Live Security), the malicious victimization of individuals such as joe jobs (no relation to Steve – a joe job is an attack, not a person), orchestrated online bullying, and so on, were around in some form long before Facebook and Twitter started to rule our lives. He cites a number of recent examples of people who were mistakenly victimized, and offers a sensible high-level guide to distinguishing fact from rumour.

In fact – and Haley does hint at this – the issue goes far beyond the question of how to distinguish between fact and uncorroborated stories. It's about how people behave in an environment that allows them to express themselves in front of huge virtual audiences while remaining themselves to some extent anonymous or pseudonymous. And I'm not just talking about hackers and cybercriminals here, but the average Internet user. For example:

- People who in their everyday offline life would never dream of stealing a book or a CD, but might nevertheless not see a problem with a pirated PDF or MP3, or putting a photograph on their blog page that was copyrighted by someone else.

- People who would be suspicious if someone came up to them in the street and asked to borrow their front door key but are all too willing to give away their passwords.

- People who don't see a problem with sharing commercial software with their friends and family.

Not that anonymity or the use of a pseudonym is invariably malicious or undesirable, but in situations where human beings perceive themselves as being less accountable for their behaviour than in a room with a few of their peers, they don't always behave admirably. Much is made in the Age of the Internet of 'crowdsourcing' and 'the wisdom of crowds', but we seem to have forgotten the historical lessons of the 'Madness of Crowds'.

It sometimes surprises me how often I've referred to Mackay's book on 'mob psychology', first published in 1841, when writing about the psychosocial aspects of IT security, but his examples are constantly re-echoed in contemporary events. A shorter and more scholarly contemporary analysis by my friend Mich Kabay on Anonymity and Pseudonymity in Cyberspace:

Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy offers an excellent introduction to many of the psychological drivers underpinning social behaviour on the web. (However, he was probably more focused on frankly antisocial behaviour than the greyer areas where you or I might sometimes cross a line in cyberspace that we wouldn't cross in 'real life'.)

While the Radio Times isn't generally the first place I'd look for security-related commentary, a recent article by Justin Webb (Radio Times, 27th April – 3rd May 2013) also makes some interesting points about the way in which a healthy scepticism can give way to a less healthy refusal to believe anything that challenges views they already hold. (He cites Nate Silver's *The Signal and the Noise: The Art and Science of Prediction* which I haven't read, but sounds like something I possibly *should* read.)

Hat tip to my colleagues at ESET Ireland for bringing the site to my attention. And while I generally keep my security-related writing and my attempts at a more literary style separate, I can't resist including a link to a poem I wrote in the 1980s called Rumour, which seems strangely apposite. Curiously, it turned up in a pile of papers I was sifting through as I wrote this piece, so I added it to a more appropriate blog page.

In the Radio Times article Webb also quotes Senator Daniel Moynihan as telling Americans that 'they were entitled to their own opinions, but not to their own facts.' That's a little ironic, in that while Moynihan may well have said something to that effect in 1994, the same quote has been attributed to James R. Schlesinger in 1973. Well, many of us have had the experience of coming up with what we believed to be a good original thought (or even a mistaken thought*) only to find that someone else had much the same idea. And the essential value of this particular thought is not devalued by a slight uncertainty about its provenance. It does demonstrate, though, how easy it is to absorb and disseminate information that may not be altogether accurate.

Another example I've seen several times recently is the attribution of the quotation 'Tact is the knack of making a point without making an enemy' both to Sir Isaac Newton and to the much more contemporary Howard H. Newton. While the phrasing of the aphorism suggests Howard H., I've given up trying to find a verifiable source – i.e., exactly *when* or *where* either Newton actually made the remark. It seems that there are many, many rent-a-quote pages that simply copy material from each other rather than checking with a verifiable source.

*I have in mind an anecdote by Richard Dawkins about how both he and E.O. Wilson, apparently totally independently, mistitled papers by Hamilton about his theory of kin selection. The papers were called, according to Dawkins – I haven't read them! – 'The genetical evolution of social behaviour', but both Wilson and Dawkins cited it as 'The genetical theory of social behaviour'. In Dawkins' own words (in the end-notes to Chapter 11 of *The Selfish Gene*), 'Wilson and I had independently introduced the same mutant meme!'

Support Scam Cold-Calling: the Next Generation

David Harley CITP FBCS CISSP ESET Senior Research Fellow

[A version of this article originally appeared on the ChainMailCheck blog.]

A recent post by Jerome Segura describes how he received such a call and played along to see how far it would go. Much of the process he describes may be familiar to you: for example, the use of Event Viewer and Prefetch to convince the victim that

there are problems on his Windows PC that need addressing. However, Segura also describes a trick along the same lines, but that I haven't seen used before, using the system utility MSCONFIG.

The story here seems to be that each service shown as "Stopped" in the Status column is symptomatic of a system problem or of malware. In fact, while the System Configuration utility can certainly be used to help with troubleshooting, the fact that a service is shown as "Stopped" simply means that it isn't running. It certainly doesn't prove the existence of a problem. Different utility, same kind of misrepresentation.

A further interesting feature mentioned in Segura's account is that while the scammers were eager to 'prove' to him that his system was under threat by running (and misusing) no less than three system utilities, they seem to have been insistent that they could not 'help' him until he actually asked them to do so. Segura suggests that 'I think this might be another technique used to cover themselves, as in I willingly asked them to help me' and I think he's probably right. That suggests that even if recent legal countermeasures aren't by themselves driving the scammers off the scene, they are at least being more cautious, in the hope of mitigating any later accusations of actively fraudulent behavior.

Segura made an audio recording of the conversation and posted it on YouTube, so if you find his blog interesting, you might want to check that out too.

While the backroom boys in Kolkata still seem to be researching simpleminded ways to misuse system utilities to mislead potential victims, there are indications that some convergence between active malware and support scam social engineering may be underway. If you read a recent post by Jean-Ian Boutin for ESET, you'll be aware of an attempt to combine the use of unequivocal malware (a program that combines fake AV functionality with a basic screenlocking capability à la ransomware) with support scamming, by driving the victim to contact a 'helpline'. Once the victim makes the call, the con is much the same as in the cold-calling scams we're already so familiar with, but now the scammer can say that the victim called asking for the service, thus sidestepping legal countermeasures based on legislation that proscribes unsolicited cold-calling. Whether this lateral arabesque would stand up to close judicial scrutiny remains to be seen, but it's clear that *someone* is putting some serious effort into prolonging the scam's lifecycle. (If you haven't read Jean-Ian's post yet, I heartily recommend it.)

Meanwhile, Virus Bulletin's Martijn Grooten, with whom I've had many a productive chat on matters relating to support scams, recently drew my attention to what might just be another variation on the theme. For Ars Technica, Jon Brodkin reported on The spammer who logged into my PC and installed Microsoft Office, hinting at a possible connection with support scams. To me this reads less like a call centre scam than a lone operator trying to make a few bucks by installing Office, using a keygen to sidestep Microsoft's licensing process, but it does suggest both an alternative support (black) market and an alternative solicitation approach – "Itman Kool2" looks for customers using SMS spam and a Yahoo mail account. It's consistent with the new 'you called us, we didn't call you' approach, and it's consistent with the common support scammer practice of charging for installing an evaluation version of security software. Will we see them making more use of these channels to get the victim to come to them? I don't know, but I'll be keeping an eye open.

Here are a couple of the papers Martijn and I, together with Steve Burn and Craig Johnston, put together last year for the 2012 Virus Bulletin and CFET conferences: between them, they

offer a pretty comprehensive view of the support scam issue, at least as we understood it at the time.

- FUD and Blunder: Tracking PC Support Scams
- My PC has 32,539 errors: how telephone support scams really work

ESET Corporate News

ESET's First News Portal

ESET announced the launch of WeLiveSecurity.com - a comprehensive source of internet security news, tips and insights. WeLiveSecurity marries ESET's global network of expert security researchers and their technology expertise accompanied by various consumer related articles providing security tips and education, delivering a platform that appeals to novices and expert security professionals alike.

Two Impactful Malware Uncovered

ESET uncovered and analyzed a targeted campaign that tries to steal sensitive information from different organizations, particularly in Pakistan (with limited spread around the world). During the course of ESET investigations, several leads were discovered that indicate the threat has its origin in India and has been going on for at least two years. Also ESET researchers, together with their counterparts at web security firm Sucuri, have been analyzing a new threat affecting Apache webservers, the most well-known and widely-used webserver in the world. The threat is a highly advanced and stealthy backdoor being used to drive traffic to malicious websites carrying Blackhole exploit packs. Researchers have named the backdoor, Linux/Cdorked.A and it is the most sophisticated Apache backdoor seen so far.

New ESET Office

ESET opened a new office in Germany. A new operations hub in the country is part of the company's overall sales strategy in the German speaking region. The newly formed company will continue to expand its 3500 strong reseller network in Germany and to strengthen its presence in retail and e-commerce. The newly created company, team of 39, will be managed by Miroslav Mikuš, ESET Deutschland Country Manager.

ESET CEO Speaking to Bloomberg's TV

During the Central European Bank meeting in Bratislava on May the 2nd 2013, ESET CEO Richard Marko spoke on Bloomberg Television's "The Pulse" and explained how an ECB rate cut may have impacted his business and examined the availability of credit to European companies. There's a video of the interview available at Bloomberg website.

Events worldwide May/June

During May, ESET has been present worldwide at the following events:

- May 6th Interop Conference, in Las Vegas, US.
- May 14th AMTSO, in Bratislava, Slovakia.
- May 16th CARO, in Bratislava, Slovakia.
- May 24th PhDays, in Moscow, Russia.
- May 28th CONFidence, in Krakow, Poland.

Furthermore, during June ESET's representatives will be attending to different events such as the World Partners

Conference, which will take place from June 3rd to the 7th, in Albufeira (Portugal), where ESET executives and partners will present their new strategies in the brand, product and research area.

In addition to the World Partner Conference, ESET is going to participate in BiTS, also in Albufeira from June 8th to the 11th, which is an internal event with testing organisations and testers.

On June 15th, the First Conference event will start in Bangkok, and it will go on until the 21st, where security practitioners will show how they are collaborating and sharing threat intelligence to tackle security incidents.

Finally, Recon from June 23rd to the 25th in Montreal (Canada), which is a computer security conference on reverse engineering and advanced exploitation techniques.

The Top Ten Threats

1. WIN32/Bundpil

Previous Ranking: 6
Percentage Detected: 3.68%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address, and it tries to download several files from the address. The files are then executed and the HTTP protocol is used. The worm may delete the following folders:

*.exe

*.vbs

*.pif

*.cmd

*Backup.

2. INF/Autorun

Previous Ranking: 1
Percentage Detected: 2.80%

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.

3. HTML/ScrInject

Previous Ranking: 2
Percentage Detected: 2.62%

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

4. Win32/Sality

Previous Ranking: 3
Percentage Detected: 2.59%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.
It modifies EXE and SCR files and disables services and process related to security solutions.
More information relating to a specific signature:
http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

5. HTML/Iframe

Previous Ranking: 5
Percentage Detected: 2.19%

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.

6. Win32/Dorkbot

Previous Ranking: 4
Percentage Detected: 2.18%

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.

7. Win32/Conficker

Previous Ranking: 9
Percentage Detected: 1.95%

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/Ramnit

Previous Ranking: 7
Percentage Detected: 1.62%

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. Win32/Qhost

Previous Ranking: N/A
Percentage Detected: 1.43 %

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.

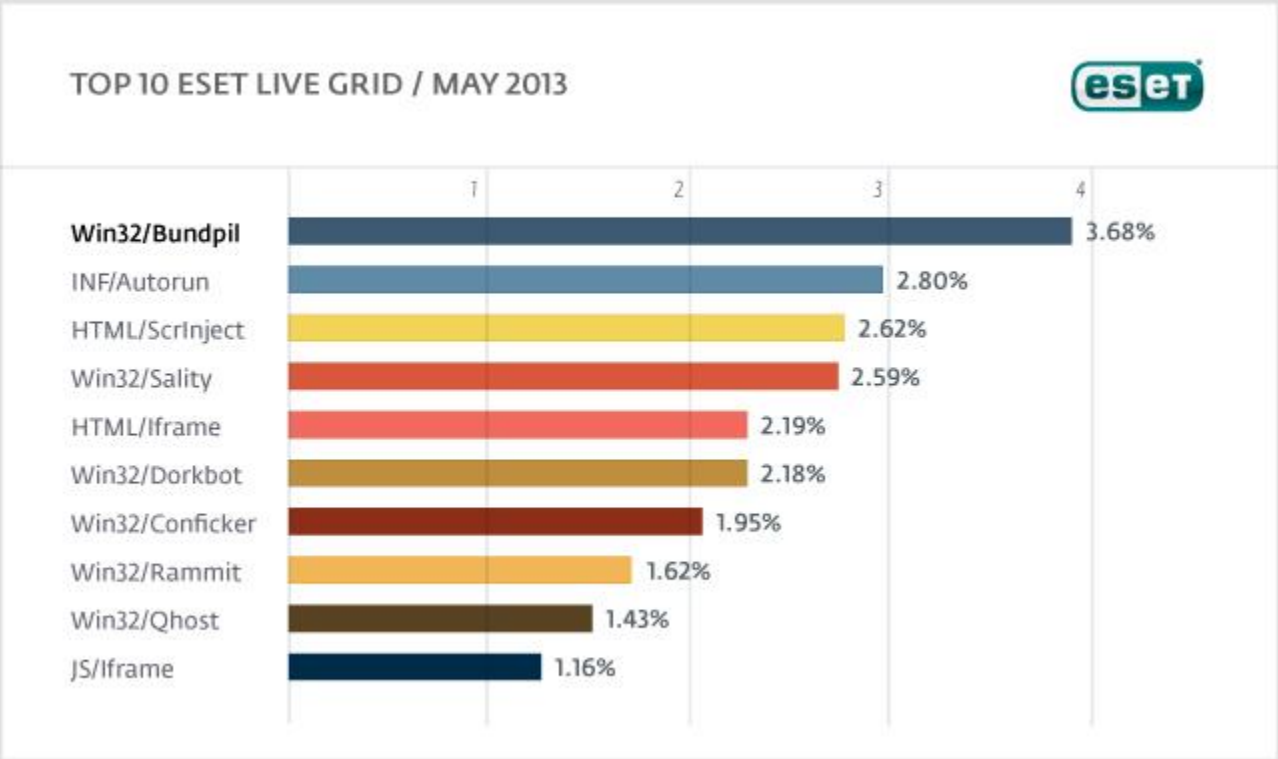
10. JS/Iframe

Previous Ranking: 10
Percentage Detected: 1.16%

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.

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 3.68% of the total, was scored by the Win32/Bundpil class of treat.



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