



February 2015

Feature Article: Hoaxes and Facebook



## Table of Contents

Hoaxes and Facebook.....	3
ESET Corporate News .....	7
The Top Ten Threats.....	8
Top Ten Threats at a Glance (graph) .....	11
About ESET .....	12
Additional Resources.....	12

## Hoaxes and Facebook

David Harley, ESET Senior Research Fellow

[A version of this article originally appeared on the [IT Security blog page](#).]

The security industry doesn't generally take hoaxes per se very seriously. There are exceptions, such as during the spate of virus hoaxes that plagued us during the 90s, which impacted to some extent on the credibility of the anti-virus industry (not least by claiming that the 'viruses' in question were not detected by anti-malware programs, a gambit also used more recently by tech support scammers).

As an example of social engineering: technical security solutions are generally of limited effectiveness in countering psychological manipulation. As a means of distributing malware, or of persuading potential victims to run malware, of course, they are all too effective. As a tool of fraudsters, too. But some hoaxes spread widely but don't do much apart from give the hoaxer some malicious self-satisfaction at convincing himself that everyone else is stupid, make the victim feel stupid if he realizes he's been duped, and irritate people who get tired of seeing the same garbage time and time again. And irritability is a minor issue for people who spend their working lives trying to reduce the impact of heavy-duty criminal activity such as banking Trojans and APTs: is it really that important if people put up a legally meaningless privacy statement that [misses the point](#) by warning Facebook that their content is their own?

My view is a little different. Over the years, I've spent a lot of time seeing at first hand that outside the malware analysis lab, something that simply doesn't exist can have serious real-world consequences. Perhaps that's because it's only fairly recently (since 2006) that I've provided consultancy for security vendors

rather than working for people who *buy* security products. In the 90s, I spent much of my time in a medical research organization restraining people from panicking about non-existent viruses like Good Times, or from pounding overstretched email facilities in order to get money from Bill Gates or free phones from Nokia or to make money for cancer research. In the early 2000s, I sometimes spent as much time as a security manager in the UK's National Health Service countering mailstorms warning against the non-existent *sulfnbk.exe* and *jdbgmgr.exe* malware as I did trying to implement and maintain countermeasures against real malware, and trying to prevent mail services buckling under the weight of emails spreading hoaxes relating to children orphaned by the 2004 tsunami. After I left the NHS I even [started a blog](#) about hoaxes and psychological manipulation as part of a masterplan for seriously reducing their impact. Unfortunately, I never got around to implementing the main plan, and now I've forgotten what it was. Maybe I'll get back to it sometime when I don't have to worry about making a living. But since I was assimilated (resistance was useless) into the security industry, [I've been writing](#) at least as much about fraud and deception as I have about bits-and-bytes security threats: well, my academic background is in social sciences as well as computer science.

Let me [quote myself](#).

*If someone shares misinformation with you on the bus or in a bar, it may have relatively little impact on the community at large. But I've often described social media as the natural supplement to or even replacement of email as the hoaxer's weapon of choice, and because the last thing social media are noted for is restricting the flow of information (or misinformation), they could well be described as a weapon of mass deception.*



And, yes, I was thinking about Facebook in particular: it's by no means the only social media service misused by spammers, scammers, hoaxers and fraudsters, but it does have a huge user population. Happily, it seems that FB has cottoned on to the fact that deluges of false information do not afford its users universal delight. A couple of days ago [the service announced](#) that it was taking measures to reduce the impact of misinformation on its news feeds by adding an annotation to posts 'many people' have reported as being hoaxes, or have deleted subsequently (on the assumption that they have done so because they were told the information was false). However, as far as I know, no information has been given on what algorithm is used to ascertain how many is 'many'. I wouldn't have thought that all that many people would have considered it necessary to warn their friends that an article on Scientists Demonstrate Irrefutably the Existence of Santa Claus wasn't true, but what do I know?

Facebook's definition of a hoax includes scams and 'deliberately false or misleading news stories', but FB is quick to point out that it isn't going to be 'removing stories people report as false' or 'reviewing content and making a determination on its accuracy.' That's hardly surprising, considering the sheer volume of content that's shared on Facebook and its siblings, but the point here is that Facebook is anxious not to be seen as [a publisher rather than a platform](#) and therefore held legally responsible for content that its users share among themselves.

So how much impact will it have? On WeLiveSecurity, [Alan Martin interprets](#) a suggestion from [Wired](#) that people might flag a post not in accordance with their political beliefs as false, as abuse: I'd actually regard it as more a case of an inability to separate subjective from objective – and maybe all of us share that, to a degree and depending on context – but it's certainly possible that a politically (for instance) contentious article (or

other link) might be flagged by Facebook as false (and/or receive less exposure in News Feed) because of the number of Facebook users who've objected to it. If Facebook isn't actually deleting such items, the option may remain for other FB users to make up their own minds, though FB itself admits that heavily flagged items won't show up so often in newsfeeds. Even before this development, it wasn't actually very clear how News Feed selects what is shown, unless you happened to come across something like [this FB article from 2013](#), which told us:

The News Feed algorithm responds to signals from you, including, for example:

- How often you interact with the friend, Page, or public figure (like an actor or journalist) who posted.
- The number of likes, shares and comments a post receives from the world at large and from your friends in particular.
- How much you have interacted with this type of post in the past.
- Whether or not you and other people across Facebook are hiding or reporting a given post.

So the latest tweak is not so different from what already happens, as regards its impact on what content actually gets to your feed. (The major difference is in the way some posts are actually flagged.) Indeed, the degree to which Facebook [manipulates news feeds](#) was the cause of a great deal of controversy not so long ago, when it became known that the company had [manipulated 700,000 news feeds](#) for experimental purposes.



It's for these reasons that I find it infuriating when people complain when no-one seems to have noticed one of their posts, by the way: it's perfectly possible the post in question never got to their friends' and acquaintances' feeds. On the other hand, if Facebook does manage to significantly reduce the number of times a hoax is re-posted – either by manipulating the feed or by flagging it as a possible hoax – that might at least encourage more people not to repost uncritically, without checking.

An interesting point that the Guardian (among others) [has mentioned](#) concerns satirical content. Facebook doesn't believe that 'satirical content intended to be humorous, or content that is clearly labeled as satire' is likely to be reported as false, which is no doubt good news for sites such as The Onion and its readers. [Wired raises the issue](#) of 'clickbait mills', some of which claim to be satirical, but don't make it clear that their stories are 'satirical'. I'm not sure how many 'satirical sites' that publish only untrue stories with no obvious wit or functionality could accurately be described as clickbait mills, but there are certainly [all too many](#) that don't seem to have any purpose other than to attract clicks. And there are certainly contexts in which clicks mean profits.

[An article by Rob Waugh](#) offers a number of suggestions for identifying Facebook hoaxes, and the main identifiers are probably worth summarizing here, though they don't cover all cases:

- 'ANY story where you're asked to share before seeing it': because that's almost invariably clickbait of a kind we've been seeing for years.
- 'Any 'news' story with mermaids or living dinosaurs': or other improbabilities like the Santa Claus story.

- 'Incredibly violent video news reports': scammers have always capitalized on the worst aspects of human psychology, including many kinds of voyeurism. '...and do you have a picture of the pain?'
- 'Outrageous news stories about Facebook itself': like the constantly recurring stories that it's shutting down next week, or about to start charging subscribers, and so on.
- 'The report about the dying girl who begs you for "Likes"': presumably a variation on [those unpleasant requests to Like a photograph](#) so that Facebook will subsidize treatment of a seriously ill child.
- 'The report on the incredible 'hack' which will let you see who looked at your Facebook page': or turn your Facebook page pink (I've always wanted to do that!), or offer a Dislike button.

Here are some more examples of out-and-out scams from the [Facecrooks site](#):

- Apps that are supposed to tell you who has looked at your profile or prevented you from looking at theirs. (Apps with this functionality aren't possible).
- Offers to test and keep iGadgets.
- 'Free' game credits.
- 'Free' travel tickets, gift cards, vouchers and so on.
- 'Exclusive' breaking news stories.



- Any post starting OMG or 'Shocking'. (I think that's a bit sweeping, but there's no doubt that there is a lot of dubious content using that sort of hook to grab attention and draw the reader into a survey scam or something of the sort).
- Fake celebrity stories. (These spread very fast via Twitter, too).

Facebook can be fun and even useful. But you really shouldn't assume that links and stories are safe, accurate, or even legal just because some of your friends are re-posting them.

\*Phil Ochs: 'Crucifixion'.



## ESET Corporate News

### [ESET's Next-Generation Business Security Products Now Available Worldwide](#)

ESET® announced the global availability of its completely re-engineered and redesigned suite of [IT security products for business](#). Following months of in-depth worldwide business user research, ESET identified the top security priorities of IT administrators and CIOs and developed a new suite of IT security products to address them. After intensive design, engineering, development and testing, the all-new business suite from ESET is now available to organizations of all sizes, across industries and around the globe.

ESET's IT security products for business provide maximum proactive protection while maintaining a low impact on company infrastructure, as well as offering a wealth of new features, such as Botnet Protection, Exploit Blocker, Anti-Phishing and Anti-Theft.

At the core of the new product offering is ESET Remote Administrator. This platform-independent, remote management console has been rebuilt to enhance usability, improve security, and lower the overall cost of implementation and management. It boasts a built-in task management system to minimize downtime, while enabling actions to be performed automatically based on dynamic group membership.

The new user interface for ESET business security products simplifies the tasks of monitoring, configuring and controlling network activity to ensure the organization is forewarned and protected against unwanted and malicious actions.

### [ESET Releases New Version of Social Media Scanner](#)

ESET® released an all new version of [ESET Social Media Scanner](#) for Facebook and Twitter. Offering a completely re-designed graphic user interface (GUI) and improved detection capabilities, the scanner is used by more than 150,000 users and has detected more than 28,000 malicious links on Facebook and 10,000 threatening links on Twitter to date.

The new version of ESET Social Media Scanner includes improved detection of harmful links and an intuitive design, making it easy to use across mobile platforms. The automatic scan function runs regularly in the background and provides users with real-time protection against malicious content.



# The Top Ten Threats

## 1. Win32/Adware.MultiPlug

**Previous Ranking: 3**  
**Percentage Detected: 2.89%**

Win32/Adware.Multiplug is a Possible Unwanted Application that once it gets a foothold on the users system might cause applications to display pop-up advertising windows during internet browsing.

## 2. HTML/Refresh

**Previous Ranking: 1**  
**Percentage Detected: 2.42%**

HTML/Refresh 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.

## 3. Win32/Bundpil

**Previous Ranking: 2**  
**Percentage Detected: 2.24%**

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address from which it tries to download several files. The files are then executed and HTTP is used for communication with the C&C to receive new commands. The worm may delete the following folders:

- \*.exe
- \*.vbs
- \*.pif
- \*.cmd
- \*Backup.

## 4. JS/Kryptik.I

**Previous Ranking: 8**  
**Percentage Detected: 1.72%**

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



## 5. Win32/TrojanDownloader.Waski

**Previous Ranking: N/A**  
**Percentage Detected: 1.46%**

Win32/TrojanDownloader.Waski is a Trojan that uses HTTP to try to download other malware. It contains a list of two URLs and tries to download a file from the addresses. The file is stored in the location %temp%\~miy.exe, and is then executed.

## 6. HTML/ScrInject

**Previous Ranking: 4**  
**Percentage Detected: 1.36%**

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

## 7. Win32/Sality

**Previous Ranking: 5**  
**Percentage Detected: 1.34%**

Sality is a polymorphic file infector. When executed registry keys are created or deleted related to security applications in the system and to ensure that the malicious process restarts each time the operating system is rebooted.

It modifies EXE and SCR files and disables services and processes implemented by and associated with security solutions.

More information relating to a specific signature: [http://www.eset.eu/encyclopaedia/sality\\_nar\\_virus\\_sality\\_aa\\_sality\\_am\\_sality\\_ah](http://www.eset.eu/encyclopaedia/sality_nar_virus_sality_aa_sality_am_sality_ah)

## 8. LNK/Agent.AV

**Previous Ranking: 6**  
**Percentage Detected: 1.20%**

LNK/Agent.AV is a link that concatenates commands to execute legitimate code while running the threat code in the background. It is similar in its effect to the older autorun.inf type of threat.



## 9. Win32/Ramnit

**Previous Ranking: 7**  
**Percentage Detected: 1.19%**

This is a file infector that executes every time the system starts. It infects .dll (direct link library) and .exe executable files and also searches htm and html files so as to insert malicious instructions into them. It exploits a vulnerability (CVE-2010-2568) found on the system that allows it to execute arbitrary code. It can be controlled remotely to capture screenshots, send information it has gathered, download files from a remote computer and/or the Internet, and run executable files or shut down/restart the computer.

## 10. INF/Autorun

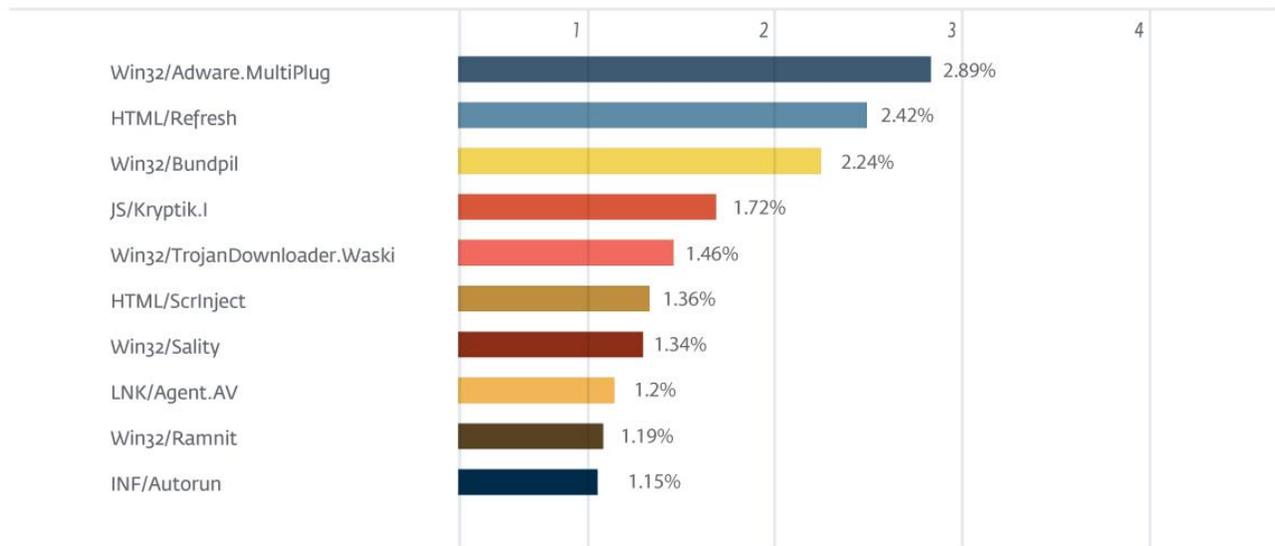
**Previous Ranking: 9**  
**Percentage Detected: 1.15%**

INF/Autorun is a generic detection of versions of the autorun.inf configuration file created by malware. The malicious AUTORUN.INF file contains the path to the malware executable. This file is usually dropped into the root folder of all the available drives in an attempt to auto-execute a malware executable when the infected drive is mounted. The AUTORUN.INF file(s) may have the System (S) and Hidden (H) attributes present in an attempt to hide the file from Windows Explorer.

## 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 2.89% of the total, was scored by the Win32/Adware.MultiPlug class of treat.

TOP 10 ESET LIVE GRID / February 2015





## 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](#)
- [WeLiveSecurity](#)
- [ESET Podcasts](#)
- [Independent Benchmark Test Results](#)
- [Anti-Malware Testing and Evaluation](#)