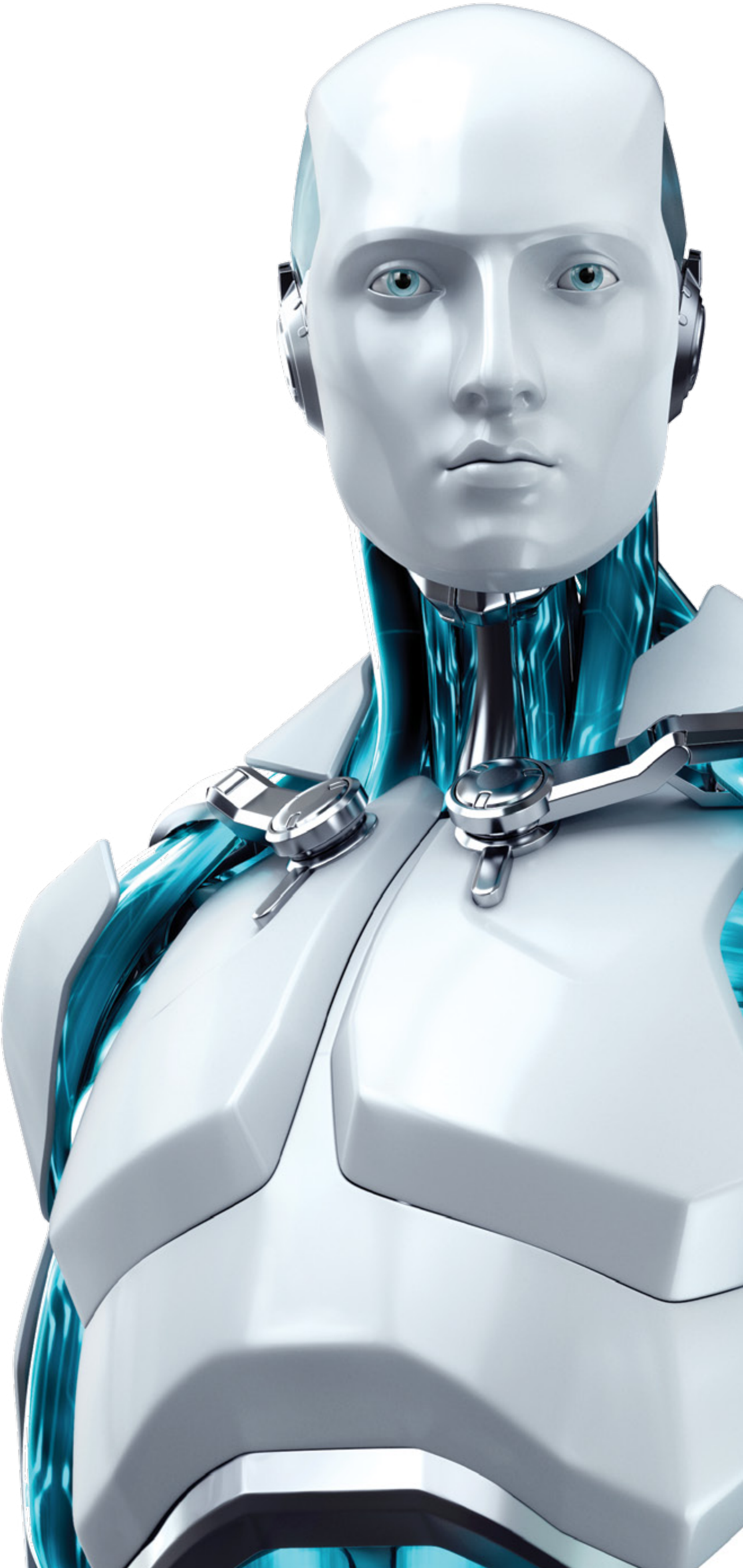
WHITE PAPER

ORIGIN OF THE SPECIOUS[1]: THE EVOLUTION OF MISINFORMATION

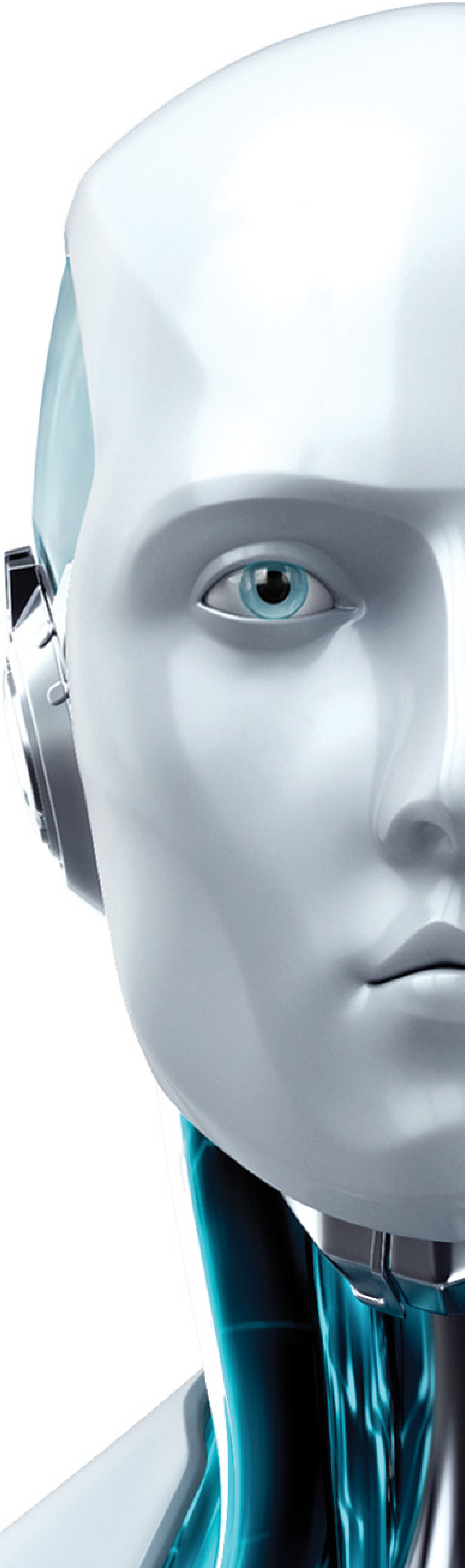
David Harley
CITP FBCS CISSP,
ESET North America



SPRING 2013

ESET Internet Security

Table of Contents



Abstract

Information wants to be free. Unfortunately, false information doesn't spend nearly enough time behind bars, except those bars that specialize in old whines in new bottles. Welcome to the Web 2.0 incarnation of the Misinformation Superhighway. Did you really think that hoaxing had died out?

Introduction

Long before there was a World Wide Web (or, at any rate, anything going by that name), the Internet was largely a playground for academics and the military, and most people still thought spam was just a canned meat. Yet there were already hoaxes and scams (pyramid schemes, Ponzi schemes, lures into premium rate phone services, fake friends and cyberstalkers...[2]). Just as early Internet worms evolved into the mass-mailers of the last decade [3] and then into Facebook clickjacking apps [4], and the pre-WWW world of Usenet and email morphed into social networks and Twitter, so social engineering adapted to the new environment.

Virus hoaxes

"The beauty of this 'meta-virus' is that it took me about two minutes to make it really scary and I didn't even have to write any code." [5]

Mogul's metavirus made a serious point in a humorous way about the ease with which a victim might be tricked into a self-inflicted denial-of-service attack using pure social engineering.

```
The only safe way to protect yourself against this virus is to print all your
files onto paper, erase all the disks on your system with a demagnetizer, buy
fresh software disks from the manufacturer, and type in all your data again.
But FIRST! send this message to everyone you know, so that they will also follow
these steps to protect themselves.
```

But who had the last laugh? It turned out to be a prototype for a family of hoaxes that continued to proliferate into the twenty-first century, albeit mutated into the SULFNBK and JDBGMGR variations on the hoax virus theme [5]. The sweat had hardly dried off Mogul's keyboard before the "Mike RoChenle" hoax showed how effective Mogul's hypothetical attack could be, especially when combined with such impressive technobabble as this:

```
The virus distributes itself on the modem sub-carrier present in all 2400 baud
and up modems. The sub-carrier is used for ROM and register debugging purposes
only, and otherwise serves no other purpose. The virus sets a bit pattern in one
of the internal modem registers, but it seemed to screw up the other registers on
my USR.
```

While the cognoscenti chuckled over spoof variations that joined the back-catalog of widely forwarded but more or less harmless joke emails that take on a life of their own based essentially on their entertainment value, the Good Times hoax virus and its offspring scared the life out of newbies and the naïve with similarly impressive descriptions of infection mechanisms and payloads:

```
If the program is not stopped, the computer's processor will be placed in an nth-
complexity infinite binary loop - which can severely damage the processor if left
running that way too long.
```

Hoaxers are blessed with a conviction that gullibility pervades both ends of the gene pool, and that there is no such thing as a claim so improbable that no one will believe it [6]. Or at any rate suspend disbelief long enough to pass it on "just in case." Unfortunately, they do not seem to be wrong.

Virus hoaxes are not a thing of the past, but they have made the jump to social media. This one [7], for instance, represents a minor variant (textually speaking) of a whole family of hoaxes spread through email over the past two decades.

> WARNING!!!!!!...DO NOT USE THE Christmas tree app. on Facebook. Please be advised it will crash your computer. Geek squad says its one of the WORST trojan-viruses there is and it is spreading quickly. Re-post and let your friends know.

However, this one was spread primarily through Facebook messaging, not through email [3]. Similarly, the ancient Olympic Torch hoax got a new lease of life with the London Olympics in 2012 [8].

Fakirs and fakers

Just as malware authors have largely moved on from hobbyist malware authoring in the pursuit of onanistic self-gratification and bragging rights, to profit centers and business models, so fiction in malware hoaxing could be described as having moved from fantasy to faction. Older generations of hoax virus alerts were merely intended to frighten the recipient into forwarding the alert: as with old-school viruses, replication was a powerful enough motive to keep the game going. More recently, real malware has often been used as the basis for a deceptive alert. Sadly, legitimate security vendors have not been immune to the temptation to use this approach to marketing. But while it's impossible to say whether former hoaxers have joined the malvertising industry, hoax techniques certainly have [9].

Fake antivirus software has benefited hugely thereby (as, increasingly, have other fake applications [10]). Of course, malware distribution and hoax distribution have overlapped for a long time: consider, for instance, the Red Team virus [11], a real if mediocre Windows file infecting virus distributed by email that contained the following text:

```
The "Red Team" virus is a complex new computer virus that spreads via the
Microsoft Windows operating system, and Internet E-Mail. Although it is not the
first virus to spread via E-Mail (that was "Good Times"), the Red Team virus is
unparalelled in its destructive capabilities.
```

But recent generations of malware authors have gone several steps beyond, by generating large volumes of fake programs that "detect" non-existent infections, which can be "disinfected," but at a price [12]. Black-Hat Search Engine Optimization (also known as BHSEO, index poisoning, index hijacking [14]) is a major weapon in the fake vendor's armoury and works at several layers of deception. While it may be related to real events [15] it can also be related to made-up events, supported by links to fake video footage, seeded by Twitter spam (and the occasional Twitter worm [16]) and so on.

Here's an unpleasant instance of fake AV in the social media context. Slashkey's Farm Town [17, 18] was attracting nearly 10 million active players monthly when it was obliged to issue a warning to them:

> If you suddenly get a warning that your computer is infected with viruses and you MUST run this scan now, **DO NOT CLICK ON THE LINK, CLOSE THE WINDOW IMMEDIATELY**. You should then run a full scan with your antivirus program to ensure that any stray parts of this malware are caught and quarantined.

Strangely enough, this event was not connected (except in time and cyberspace) with a Farmville-related virus hoax with a distinct resemblance to an older email virus hoax form [19]:

> RED ALERT!!! Norton has just informed me that the post for Send the 3 spring Eggs at a time is a virus, Rawand Bradosty is a HACKER from Pakistan, do not click on this post it is not legitimate, please copy and repost immediately.

In fact, the Twitter worm cited above represents a transplantation of a phenomenon that has become particularly widespread in other social media contexts, especially Facebook. However, the OMG school of social engineering has also served its time in email malware dissemination. (As in a comment such as "OMG, I can't believe this is true!" being used to trick a victim into opening a malicious attachment or URL.) The point of this kind of attack is to trick the victim into opening a suspicious object by presenting him with an alarming or sensationalist hook.

In Facebook scams like those that accompanied some of 2011's disasters in Japan [19], a link to such amazing (fake) footage generally turns out to lead to a survey scam. These stories also use clickjacking so that when a victim thinks he's clicking on something that will enable him to see the OMG video, he's really been tricked into telling his Facebook friends that he "Likes" the application ("likejacking"), so that they will be recruited into the replication process [15].

This process of transplantation and adaptation to new contexts is a persistent feature of Internet criminality. While email and instant messaging have not become extinct as a vector for harassment, malware and scams such as 419 advance fee fraud (AFF) [20], the more recent social networks have become an important (and in some instances the main) channel for dissemination of disinformation [21]:

- "DeathTweets" claiming the death of some celebrity [22]
- "Londoning" where a hijacked account is used to contact friends of the legitimate account holder asking for financial help (courtesy of Western Union) [23]
- Variations on cyberstalking [24, 25]

It’s yesterday once more

If the threats have proved transferable to new media, is it also possible to transfer some of the detection heuristics and countermeasures of yesteryear to new user populations?

There are, of course, characteristics of hoaxes that are not unique to email. The dictionary/blacklisting approach to detecting social engineering hoaxes and scams has only limited applicability to automated defences [6].

Nonetheless, there are some core messages that might mitigate out-and-out hoaxes, including virus hoaxes, and some common scams.

- It doesn’t make it true if 100,000 people forward a message.
- A warning that states that “there is no cure for this virus” should also be regarded with skepticism. Anti-malware vendors usually address the high-profile, high-impact, fast-spreading malware that most excites the media attention in a matter of hours (or less). It is unlikely that there will ever be a totally undetectable virus, or one from which there is no protection, and if there is, no one will know about it, virtually by definition. There are malicious programs whose effects are so drastic that recovery of data (or, in rare instances, of systems) is impractical (perhaps for reasons of cost-effectiveness); however, such viruses are no more difficult to detect and protect against than any other virus.
- People lie: in email, in blogs, on television, in newspapers and certainly on Facebook. Just because a telephone number, CVE ID, security vendor, person or other entity is quoted in a message, that doesn’t confirm that they’re real, let alone that they’re trustworthy. (This is the sort of circumstantial detail that 419s use to lend their scams authority, too.)
- Bill Gates didn’t get rich by giving his money away to people just to reward them for forwarding email, or tweets, or replicating a Facebook status. No one is going to give you an iPad or donate money to cancer research because you forward multiple emails. Actually, anyone who offers you a free iPad is at best entering you into a draw, and very likely luring you into one of a wide range of scams 26, 27.
- If you receive multiple, possibly slightly inconsistent variations of the core message, that might be because it isn’t true. It certainly isn’t proof that it is true.
- If a message says it isn’t a scam, chain letter, spam, etc., that’s often a good indicator that it is.
- Forwarding chain messages, irrespective of the transmission medium, without checking their validity is dumb. Forwarding unconvincingly presented messages on the off chance that they may be valid is irresponsible and dumb. Forwarding chain messages that you don’t believe yourself is verging on the psychopathic.
- Watch out for any message that has classic chain-letter characteristics:
    - It implements a threat: “Pass this on to everyone you know, otherwise something undesirable will happen.” For example, a virus epidemic, a child’s dying wish won’t be honored, a missing child will not be found, or you will feel excruciatingly guilty about troops fighting in some contested region of the Middle East.
    - It’s undated, or the date is impossible (29-31st April[28]) or unverifiable. A nonspecific date such as “Yesterday” or “just issued by…” isn’t good enough. There are messages with such “evidence” in circulation right now that have been around for many years. Of course, it’s quite possible that a message with a convincing date could still be a hoax. However, that would at least suggest a possible timeframe and give you something to check.

- Messaging from the alleged sources for the information is inconsistent or illogical. For instance:
  - The vendor behind an operating system or an application is unlikely, in real life, to say that a virus causes irreparable damage, and a security company is equally unlikely to describe a malicious code as undetectable—at any rate by its own product.
  - The BBC does not send out radiation alerts by text message, and NASA does not send out warnings of acid rain.
  - National Health Service agencies and police stations in the UK do not send out vague alerts about HIV-infected needles in cinemas as chain mail.
- There is no indication of an expiration date or time-to-live value. One of the more encouraging features of the alert system via Twitter and Facebook apparently proposed [29] by the Department of Homeland Security is that alerts will apparently be sent "far and wide but only...for limited periods of time." Nonetheless, the presence of such a date doesn't prove anything in the absence of other verifiable and supporting evidence.
- No identifiable organization is quoted as the source of the information.

Verifiability

How do we guarantee the validity of referenced sources of further information? Of course, we can't.

URLs can be obfuscated in many ways, and an apparently innocuous URL may simply be the first stage in a series of redirections pointing ultimately to a malicious, inappropriate or at least suspicious site. Many web pages are, of course, sitting on machines that are either frankly criminally owned or compromised and recruited without the knowledge of the owner into a botnet.

Such activity is a staple of twenty-first-century cybercrime, but that aside, it's all too easy to set up a web page without supplying any sort of verification/authentication (sometimes free of charge, so credit card details aren't necessary, and of course stolen credit card details are routinely available from black market forums), so an apparently genuine web page can contain very unreliable information. And misleading websites are the basis of many phishing attacks and not a few other scams [30], a problem that is not mitigated by the continuing tendency for legitimate financial institutions to communicate with customers over security and other issues in ways that are easily spoofed by bad actors [31]. Even security organizations have been known to distribute alerts in the form of chain letters (rarely, fortunately), and such an approach is seen all too often by less security-oriented enterprises as a tempting form of viral marketing [10].

Similar problems exist with other verification measures. There is unlikely to be a digital signature of any sort for authentication in a pure hoax, but the presence of a digital signature is not, in itself, proof of a bona fide alert. Many people don't bother or don't know how to check a digital signature—or, come to that, a CVE ID or a Microsoft bulletin ID.

Reducing attack surface

Short messaging media (Facebook Statuses, SMS, Twitter, LinkedIn messaging and so on) make heavy use of URLs shortened and therefore obfuscated with bit.ly, TinyURL and so on. Where possible, use and encourage others to use links that at least allow preview before opening—http://surl.co.uk actually forces a preview, while http://tinyurl.com and http://bit.ly have options that allow it. Most URL shortening services allow web pages to be previewed by adding a plus sign (+) to the end of the URL.

While social media are often more interested in sharing data than in preserving privacy/data (Facebook seems to be a particularly hot spot for data leakage), they do have information on configuring an account in ways that mitigate vulnerability to attack. For instance:

- http://googleblog.blogspot.com/2009/11/next-steps-in-cyber-security-awareness.html
- http://support.google.com/youtube/bin/request.py?contact_type=abuse&hl=en-US
- http://support.google.com/youtube/bin/search.py?ctx=en%3Asearchbox&query=security
- http://twitter.com/about/security
- http://www.facebook.com/security
- http://www.google.com/help/security/index.html
- http://www.myspace.com/help?p=/safetysite/home
- https://support.twitter.com/articles/76036#
- https://www.facebook.com/about/privacy/your-info-on-fb

Unfortunately, as with all websites, pages are moved or removed, and it can be fairly tricky to find out where they went. It would be cynical, of course, to suggest that social media sites are sometimes a little sensitive about making security information too obvious, not wanting to flaunt possible security issues or do anything that might discourage people from using their services. Then again, the same suspicions could be held with reference to businesses in many other sectors.

While generic security software is generally of limited effectiveness in addressing the social engineering–oriented first stage of attacks that may or may not ultimately lead to some form of malicious binary, security companies with an educational remit often make available resources such as the ESET Social Media Scanner that track some of the trends and specific attacks in this space.

Many potential attacks make use of services that share a user's physical location (geotagging). This goes beyond being careful about using services that allow you to "check in" at a given location [32]: for example sharing photos from a smartphone or iGadget [33]. Though modern digital cameras tend not to include geolocation metadata in a JPG by default, not all smartphones have the same security smarts [34]. However, there is information on resetting a number of common smartphone types at http://icanstalku.com/how.php#disable.

Conclusions

When a resident of Balby in the United Kingdom was alleged to have threatened on Twitter to bomb Robin Hood airport, Doncaster, after his flight was cancelled, South Yorkshire police said, according to the *Independent* [35], that "A 26-year-old Doncaster man has been charged with sending by a public communications network a message that was grossly offensive or of an indecent, obscene or menacing character contrary to Section 127 of the Communications Act 2003."

This author said at the time [36] that "I can't help wishing the opportunity would present itself to bring to book the originators of some of the scaremongering hoaxes that regularly cross my desktop about mythical threats like rattlesnakes in sandpits, gang initiation rites on the freeway, and mysterious warnings about terrorist attacks on a certain future date."

Unfortunately, the nature of the Internet makes such opportunities generally impractical. The identity of a hoaxer is usually concealed behind a mist of anonymity or pseudonymity, or simply undistinguishable from the identities of his victims. While it's sometimes possible (though depressingly uncommon) to bring cybercriminals to justice, it's *very* uncommon for resources to be brought to bear on an attack whose impact is usually psychological rather than financial.

References

1. Wikipedia, On the Origin of Species, 2001, http://en.wikipedia.org/wiki/On_the_Origin_of_Species
2. Daniel J. Barrett, "Bandits on the information superhighway," O'Reilly, 1996
3. David Harley, Robert Slade and Urs E. Gattiker, "Viruses Revealed," Osborne, 2001. ISBN 0-07-213090-3
4. David Harley, "ROFLing around the Christmas Tree," http://www.welivesecurity.com/2010/11/23/rofling-around-the-christmas-tree/
5. Jeffrey Mogul, "Virus Paranoia," RISKS, http://catless.ncl.ac.uk/Risks/6.23.html#subj3.1, 1988
6. David Harley and Randy Abrams, "Whatever happened to the unlikely lads? A hoaxing metamorphosis," Virus Bulletin 2009 Conference Proceedings, http://www.eset.com/us/resources/white-papers/Harley-Abrams-VB2009.pdf
7. David Harley, "Facebook Christmas tree virus: it's still a hoax," http://www.welivesecurity.com/2011/11/27/facebook-christmas-tree-virus-its-still-a-hoax, 2011
8. Olympic hoax reference
9. Graham Cluley, "Christmas Tree App Virus Hoax Spreads on Facebook," http://nakedsecurity.sophos.com/2010/11/22/christmas-tree-app-virus-hoax-spreads-on-facebook/, 2010
10. David Harley, "Security Software & Rogue Economics: New Technology or New Marketing?", EICAR 2011 Conference Proceedings, http://smallbluegreenblog.wordpress.com/2011/05/15/eicar-2011-paper/
11. F-Secure, "Red Team," http://www.f-secure.com/v-descs/redteam.shtml
12. Róbert Lipovský, Daniel Novomeský and Juraj Malcho, "Fake but free and worth every cent," Virus Bulletin 2011 Conference, http://www.welivesecurity.com/media_files/white-papers/fake_but_free.pdf
13. Cristian Borghello, "Free but Fake: Rogue Anti-malware," http://www.eset.com/us/resources/white-papers/Free_but_Fake.pdf, 2009
14. Igor Muttik, "A Tangled Web," AVIEN Malware Defense Guide for the Enterprise, ed. Harley, Syngress, 2007
15. David Harley, "A tsunami is also a crime wave," http://www.scmagazineus.com/a-tsunami-is-also-a-crime-wave/article/199547/, 2011
16. Charlie White, "Tweet Viewer Worm Crawling Around Twitter," http://mashable.com/2011/03/05/twitter-worm/, 2011
17. David Harley, "I thought I'd bought London Bridge, but instead I bought the farm," http://chainmailcheck.wordpress.com/2010/04/12/i-thought-id-bought-london-bridge-but-instead-i-bought-the-farm/, 2010
18. Jeremy Kirk, "Malicious Facebook Ad Redirects to Fake Antivirus Software," http://www.pcworld.com/businesscenter/article/194008/malicious_facebook_ad_redirects_to_fake_antivirus_software.html, 2010
19. David Harley and Urban Schrott, "Blackhat Japanning," Global Threat Trends, http://www.eset.com/us/resources/threat-trends/Global_Threat_Trends_March_2011.pdf, 2011
20. David Harley and Andrew Lee, "The Spam-ish Inquisition," http://go.eset.com/us/resources/white-papers/Spamish_Inquisition.pdf, 2007
21. Richi Jennings, "Facebook shutting down March 15: Yeah, right," http://blogs.computerworld.com/17651/facebook_shutting_down_march_15_yeah_right?ta, 2011
22. Austin Considine, "One Comeback They Could Skip," http://www.nytimes.com/2012/09/20/fashion/celebrity-hoax-death-reports.html?_r=1&adxnnl=1&adxnnlx=1351339723-6QVNV5DS70XWwi2PqH+7Iw, 2012
23. David Harley, http://www.welivesecurity.com/search/?s=londoning&x=17&y=15, 2010–2011
24. David Harley, "Not quite stalking but ugly enough," http://chainmailcheck.wordpress.com/2011/03/16/not-quite-stalking-but-ugly-enough/, 2011
25. David Harley, "Cyberstalking," http://chainmailcheck.wordpress.com/2011/03/16/cyberstalking/, 2011
26. Randy Abrams, "The iPad 2 is Not Free," http://www.welivesecurity.com/2011/03/02/the-ipad-2-is-not-free/, 2011
27. Randy Abrams, "Get a Free iPad on Facebook!", http://www.welivesecurity.com/2011/02/15/get-a-free-ipad-on-facebook/, 2011
28. David Harley, "Chainmail for the Calendar-Deprived," http://chainmailcheck.wordpress.com/2011/02/28/chainmail-for-the-calendar-deprived/, 2011
29. Charlie White, "Homeland Security to Issue Warnings via Facebook & Twitter," http://mashable.com/2011/04/07/terror-twitter/, 2011

30. David Harley and Andrew Lee, "A Pretty Kettle of Phish," http://www.eset.com/us/resources/white-papers/Pretty_Kettle_of_Phish.pdf, 2007

31. David Harley and Andrew Lee, "Phish Phodder: is User Education Helping or Hindering?", Virus Bulletin 2007 Conference Proceedings, http://www.eset.com/us/resources/white-papers/Phish_Phodder.pdf

32. Foursquare, "Privacy 101," https://foursquare.com/privacy/, 2010

33. I Can Stalk U, "Raising awareness about inadvertent information sharing," http://icanstalku.com/how.php, 2010

34. NBC Action News, "Smartphone pictures pose privacy risks," http://www.youtube.com/watch?v=N2vARzvWxwY, 2010

35. Dave Higgens, "Man charged over 'airport bomb hoax' Tweet," http://www.independent.co.uk/news/uk/crime/man-charged-over-airport-bomb-hoax-tweet-1903349.html, 2010

36. David Harley, "Robin Hood Airport hoaxer shoots own foot," http://chainmailcheck.wordpress.com/2010/02/18/robin-hood-airport-hoaxer-shoots-own-foot/, 2010

Author biography

David Harley BA CITP FBCS CISSP is a security researcher/consultant/author/editor with an academic background in social sciences and computer science. He worked 1986–2006 in medical informatics with emphasis on security, notably as manager of the National Health Service's Threat Assessment Centre. Since founding Small Blue-Green World (incorporating Mac Virus and AVIEN) he has worked closely with ESET, where he is Senior Research Fellow. Between 2009 and 2012 he was a director of the Anti-Malware Testing Standards Organization (AMTSO). He is a Fellow of the British Computer Society (now the BCS Institute) and has certifications in security management, audit and ITIL service management.

Harley is coauthor (with Robert Slade and Urs Gattiker) of *Viruses Revealed*, and technical editor and principal author of The *AVIEN Malware Defense Guide for the Enterprise*. He has also contributed chapters to a number of other security-related books, and security articles for Virus Bulletin and Elsevier among others. He often presents papers at specialty security conferences including Virus Bulletin, AVAR and EICAR, and blogs (or has blogged) for ESET's ThreatBlog, *Infosecurity Magazine*, *SC Magazine*, SecuriTeam, Anti-Malware Testing, Mac Virus and Internet Evolution.

If he had any leisure time, he would devote it to the guitar, photography and country walking.