Common Hoaxes and Chain Letters

Volume 1

David Harley, Director of Malware Intelligence | ESET LLC

About the Author

David Harley CISSP, ESET Research Author, is an experienced and well-respected anti-virus researcher, and also holds qualifications in security audit, ITIL service management, and medical informatics. Until 2006 he worked in the UK's National Health Service, where he specialized in the management of malicious software and all forms of email abuse, and managed the Threat Assessment Centre. He has worked as an independent author and consultant to the anti-virus and security industries, and is Chief Operating Officer of AVIEN (Anti-Virus Information Exchange Network).

He was co-author of "Viruses Revealed" and has contributed chapters to many other books on security and education for major publishers, as well as a multitude of articles and conference papers. He was technical editor and lead author of "The AVIEN Malware Defense Guide for the Enterprise", also for Syngress.

Table of Contents

Introduction

This is a listing of hoaxes and chain letters that are commonly reported right now, though it might be expanded to include more varied material, as time allows. Not all hoaxes are chain letters, of course. Come to that, not all chain letters are hoaxes, either, but it's rarely a good idea to forward chain e-mail, even if it doesn't include any deceptive elements.

I used to say "never" rather than "rarely", but some situations do arise where people have an emotional need to participate actively in an issue (for instance, the identification of 2004 Tsunami victims or the search for the missing English child Madeleine McCann) and feel that chain e-mail offers them a way to do that. Unfortunately, it's not a very efficient way, since it results in the same message (whether true, false or in between) being received over and over. Often, a chain letter that *does* attempt to deal with a real issue becomes a total pain because it has become obsolete and irrelevant, yet the letter keeps on circulating.

Fortunately, not all hoaxes pose such ethical and psychological dilemmas. A great many of them are originally the work of hoaxers who make glorify themselves by exploiting the good intentions of other people, by getting them to spread chain mail in the belief that they're doing something that benefits others (such as alerting them to a virus problem). Of course, some hoaxes (or semi-hoaxes) arise out of genuine misunderstandings and misconceptions, or become divorced from the truth as they spread further across the Internet. However, many are started by an individual whose warped self-esteem is boosted each time one of his victims is made to feel stupid when they realize they've been hoaxed.

Recognizing and Handling Hoaxes

Here at ESET our primary focus is on real malware rather than viruses that don't actually exist. However, virus hoaxes and other chain letters are clearly very much an ongoing problem, and these are some of the points that administrators and support units may find it useful to reinforce:

- A story doesn't become truer if 10,000 people forward it as a message.
- Circumstantial detail that may be correct itself can be used as irrelevant pseudo-corroboration of a Big Lie.
- The presence of circumstantial contact detail such as a telephone number doesn't prove that it's a real number or belongs to a real person
- Mention of AOL, Nike, Microsoft, McAfee (even hoax-dubunking sites like www.snopes.com) and so on do not prove that those companies have endorsed the message that mentions them.
- Bill Gates didn't get to be the third richest man in the world by giving his money away to people as a reward for forwarding email.
- If email was that easy to track, there'd be no spam problem. No-one is going to give you a cell phone, a $2000 check, or even donate money to cancer research or a children's charity because you forward multiple emails.
- If a message says it isn't a scam or a chain letter, that's may be a good indicator that it *is*.
- To forward a chain letter without checking its validity is naive. Forwarding a chain letter just in case it might be true is both naive and lazy. Forwarding a chain letter in the hope of its stopping people forwarding chain letters is simply bizarre.
- No security alert should be passed on without authorization and, if there's any doubt, verification by a competent authority.
- Any alert that describes a virus that can't be detected by anti-virus is either a hoax or pessimistic beyond belief.

There are many heuristics (rules of thumb) which can be used with some success to identify common types of hoax:

- They may have the characteristics of a chain letter - "Pass this on to everyone you

know, otherwise something unpleasant will happen."

- They are usually undated, or have no realistic or verifiable date. "Yesterday" or "just issued by..." tells you nothing. Of course, a convincing actual date doesn't prove that it's not a hoax in itself.
- Similarly, there is usually no expiry date on warning, but the presence of such a date doesn't prove anything in itself.
- There is no identifiable organization quoted as the source of the information, or else the organization is one not normally associated with security advice and expertise. These attributions are invariably intended to add what Padgett Peterson has referred to as "credibility by association" and should not be taken on trust. However, this doesn't mean that attribution to a credible source shouldn't be treated with scepticism. Anyone can say "I heard it from someone at ESET" (or Symantec, or SANS, or....).

List Entry Format

Each entry includes a "traffic light" hoax status indicator:

Red = completely fabricated, not a word of truth in it. Do not forward it indiscriminately, even to refute it, but feel free to direct people to this page and other anti-hoax resources.

Amber = not altogether false: in fact, many hoaxes are better described as semi-hoaxes, which carry a grain (or several grains) of truth, but their usefulness has been compromised, deliberately or otherwise, by the introduction of misunderstandings and misconceptions, or downright deception.

Green = True. That doesn't mean it's a good idea to forward it indiscriminately, though. I've never yet seen chain e-mail that was worth forwarding in the form in which it arrived.

Red and amber = status undetermined, but since it found its way into this document, perhaps it would be sensible to assume the worst.

The text of the actual message is shown in Courier (monotype), and interpolated comments are shown in normal body text, but italicized.

"Snopes/Postcard" Hoax

Red = completely fabricated, but with a misleading reference to www.snopes.com, which is an informational site that actually does a very good job of tracking and classifying hoaxes.

Alternative names and keywords: Olympic Torch, Invitation, A Virtual Postcard for you, Merry Christmas, Sector Zero.

> Hi All, I checked with Norton Anti-Virus, and they are gearing up for this virus!

As a matter of fact, Symantec list a very close variant to this hoax in their hoax listings as Olympic Torch: clearly, they are not "gearing up" for a virus that doesn't exist. This assertion is a deliberate deception included to lend authenticity to the hoax.

> I checked snopes.com, and it is for real!! http://www.snopes.com/computer/virus/postcard.asp (last updated 2/13/08)

This is a genuine link, but it doesn't refer to this mythical virus: it refers to a wave of emails sent out in 2007 by (and with the intention of propagating) the Storm botnet (Nuwar, Zhelatin, Peacomm). In fact, the same link actually refers to (as a hoax virus) a version of this message, which they further describe at http://www.snopes.com/computer/virus/invitation.asp

> VERIFY IT FOR YOURSELF. DON'T GET CAUGHT!

Good advice.

> Get this E-mail message sent around to your contacts ASAP.

> PLEASE FORWARD THIS WARNING AMONG FRIENDS, FAMILY AND CONTACTS!

Bad Advice. The next few paragraphs are essentially the same hoax that has been circulating for several years: it's almost identical to the Olympic Torch hoax, apart from the substitution of the POSTCARD for the mythical Torch image.

> You should be alert during the next few days. Do not open any message with an attachment entitled 'POSTCARD,' regardless of who sent it to you.

> It is a virus which opens A POSTCARD IMAGE, which 'burns' the whole hard disc C of your computer.

This virus will be received from someone who has your e-mail address in his/her contact list. This is the reason why you need to send this e-mail to all your contacts. It is better to receive this message 25 times than to receive the virus and open it.

If you receive a mail called' POSTCARD,' even though sent to you by a friend, do not open it.! Shut down your computer immediately.

This is the worst virus announced by CNN. It has been classified by Microsoft as the most destructive virus ever. This virus was discovered by McAfee yesterday, and there is no repair yet for this kind of virus.

This virus simply destroys the Zero Sector of the Hard Disc, where the vital information is kept.

COPY THIS E-MAIL, AND SEND IT TO YOUR FRIENDS. REMEMBER: IF YOU SEND IT TO THEM, YOU WILL BENEFIT ALL OF US

"Do you really know how to forward emails?" Semi-Hoax

Amber = not altogether false, but of questionable value, and undoubtedly a chain letter.

A friend who is a computer expert received the following directly from a system administrator for a corporate system.

This kind of opening is characteristic of many hoaxes and urban legends (we sometimes use the acronym FOAF, for Friend Of A Friend, to describe stories where the person to whom whatever it is actually happened is always someone the sender doesn't know personally, someone a few links down the chain of forwarders). Assumptions here are that:

- *Invocation of expertise and authority, even though the individuals concerned are totally anonymous and may or may not exist at all, corroborates the authenticity of the message. Making it two "experts" rather than one is a nice touch, but doesn't really prove anything at all.*
- *Being a "computer expert" or a system administrator makes you an expert on spam, malware and so on. Actually, many people who may fit the "computer expert" description in some senses and/or do administer systems perfectly competently, nevertheless know less than you might think about the specifics of security. In fact, in my years as a security analyst, sysadmin, and security manager, I came across many instances where IT staff, system managers, support staff, even security specialists, nevertheless distributed or forwarded poor or misleading information, even hoax emails, proving themselves as gullible as anyone else. Remind me to tell you sometime about what Rob Rosenberger calls "False Authority Syndrome", where an individual is assumed to be an expert because he has knowledge in (often) unrelated areas, or even just because he's some sort of celebrity.*

It is an excellent message that ABSOLUTELY applies to ALL of us who send e-mails.

Of course it is and does. I just read it on the Internet, so it must be true in every detail. That was meant to be ironic, by the way.

Please read the short letter below, even if you're sure you already follow proper procedures.

I'm sure of nothing but how little I know. But I'm always ready to learn.

Do you really know how to forward e-mails? 50% of us do; 50% DO NOT.

And 97.6935% of statistics are made up on the spot.

("I'm a poet. And I know it..." OK, it doesn't scan too well, and Milton is probably turning in his grave.

The point, though, is that anyone can make up an unsupported statistic.)

> Do you wonder why you get viruses or junk mail? Do you hate it?

I think that's called a rhetorical question. And rhetoric is what you use to sell an idea to people who are easier to persuade with psycholinguistics than with logic and pure fact. :-/

> Every time you forward an e-mail there is information left over from the people who got the message before you, namely their e-mail addresses & names. As the messages get forwarded along, the list of addresses builds, and builds, and builds, and all it takes is for some poor sap to get a virus, and his or her computer can send that virus to every e-mail address that has come across his computer.

Well, there's some truth in this. A message that's forwarded does contain header information that can include the email addresses of other individual recipients, and it is possible for malware to scan a hard disk for addresses to send itself to, or for spamming purposes. But the steps listed here make virtually no difference in that respect, except to mislead those of us who aren't particularly computer-literate.

> Or, someone can take all of those addresses and sell them or send junk mail to them in the hopes that you will go to the site and he will make five cents for each hit. That's right, all of that inconvenience over a nickel!

Well, taken as a whole, it's a great many nickels. Unfortunately, though, this is far from the only (or even the most common) means by which spammers harvest addresses. So this isn't going to fix the spam problem (or even just your spam personal problem) any more than all the other instant fixes of the past 10-20 years.

> How do you stop it? Well, there are several easy steps:

The 11th Law of Data Smog: "Beware stories that dissolve all complexity." ("Data Smog", by David Schenk, Abacus 1997)

> (1) When you forward an e-mail, DELETE all of the other addresses that appear in the body of the message (at the top).

Well, that's often good netiquette. Many people forward or reply to messages without editing them at all, which can result in unnecessarily long and difficult-to-read messages. However, email addresses are often listed in the body of the message in a form that doesn't give spammers anything to harvest. For instance:

> ––Original Message––

> *From: David Harley*

> *Sent: 07 March 2008 10:28*

> *Subject: bcc test*

> That's right, DELETE them. Highlight them and delete them, backspace them, cut them, whatever it is you know how to do. It only takes a second.

And it leaves the headers intact, so it may not help at all in making the message less useful to spammers. But at least it shortens the message, and, if you're careful about what you delete, may make it more readable.

If you want to strip the superfluous addresses from the headers, the easiest way is to paste the parts of the message you want to forward into a new message. By the way, if you're not familiar with email headers, here's a shortened version of a set of typical message headers (with some of the detail edited).

Received: from A_PC ([xxx.xxx.xxx.xxx])
by mx.google.com with ESMTPS id
d38sm3486984and.17.2008.03.04.07.19.37
(version=SSLv3 cipher=RC4-MD5);
Tue, 04 Mar 2008 07:19:39 -0800 (PST)
Reply-To: <someone@somewhere.com>
From: "Joe Bloggs" <someone@somewhere.com>
To: "'Josephine Bloggs'" <someoneelse@somewhereelse.com>
X-ASG-Orig-Subj: FW: News
Subject: FW: News
Date: Tue, 4 Mar 2008 15:19:30 -0000
Message-ID: <005801c87e0b$25dc6540$4101a8c0@DAVID>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="—-=_NextPart_000_0059_01C87E0B.25DC6540"
X-Mailer: Microsoft Office Outlook 11

> You MUST click the "Forward" button first and then you will have full editing capabilities against the body and headers of the message. If you don't click on "Forward" first, you won't be able to edit the

message at all.

Well, it's true you can't usually edit the original of a message that you've received until you forward it, reply to it etc.

(2) Whenever you send an e-mail to more than one person, do NOT use the To: or Cc: fields for adding e-mail addresses.

What the writer doesn't seem to have remembered is that often you actually want to share address information with other trusted recipients! Also, blind copied mail can actually confuse the recipient.

Always use the BCC: (blind carbon copy) field for listing the e-mail addresses. This is the way the people you send to will only see their own e-mail address.

That isn't automatically a good rule for every occasion. For a start, it's exactly what a lot of spam messages do, which means that some crude filters may automatically reject it. Furthermore, it doesn't make the slightest difference in terms of discouraging spam if you forward mail in sensible quantities to appropriate people.

If you don't see your BCC: option click on where it says To: and your address list will appear. Highlight the address and choose BCC: and that's it, it's that easy.

That depends on which mail client you use, actually. But it does (kind of) happen if you use Outlook, give or take a menu or two and one or two other variables.

When you send to BCC: your message will automatically say "Undisclosed Recipients" in the "TO:" field of the people who receive it.

There's nothing automatic about it. It depends on a number of variables. This may cast doubt on the "expertise" of the person who wrote this. But maybe the point is to appear authoritative, rather than informative?

(3) Remove any "FW :" in the subject line. You can re-name the subject if you wish or even fix spelling.

Hopefully, someone will explain to me how this reduces virus/spam dissemination. What am I missing?

(4) ALWAYS hit your Forward button from the actual e-mail you are reading.

Well, that's one way of getting to edit it, but ALWAYS is a BIG WORD.

> Ever get those e-mails that you have to open 10 pages to read the one page with the information on it? By Forwarding from the actual page you wish someone to view, you stop them from having to open many e-mails just to see what you sent.

That's a netiquette issue. Perhaps this is one of those instances of a hoax mail intended to reinforce "good" practice, but unless we get the chance to talk to the anonymous originator, we may never really know. Certainly it would be nice if people sometimes removed the unnecessary bits of email they reply to or forward, which I presume is the message that this slightly confusing sentence was meant to convey.

> (5) Have you ever gotten an email that is a petition?

Of course I have. A few of them have constituted serious chain letter hassle, and they're not generally a good idea. There's a place for electronic petitions, but not in the form of chain letters, which are hardly ever justified.

> It states a position and asks you to add your name and address and to forward it to 10 or 15 people or your entire address book. The email can be forwarded on and on and can collect thousands of names and email addresses.

That's a rough and ready definition of a chain message. I'll come back to that thought at the end.

> A FACT: The completed petition is actually worth a couple of bucks to a professional SPAMMER because of the wealth of valid names and email addresses contained therein.

So such a petition is (1) a professional spamming exercise (2) only going to make a couple of bucks difference to the spammer? Hmmm…

*However, I **have** seen chain letters that appeared to be intended for address-harvesting purposes.*

> If you want to support the petition, send it as your own personal letter to the intended recipient. Your position may carry more weight as a personal letter than a laundry list of names and email address on a petition. (Actually, if you think about it, who's supposed to send the petition in to whatever cause it supports? And don't believe the ones that say that the email is being traced, it just ain't so!)

Certainly there are problems administering a petition by email: it may be much better to do it by way of a web form, for instance.

(6) One of the main ones I hate is the ones that say that something like, "Send this email to 10 people and you'll see something great run across your screen." Or, sometimes they'll just tease you by saying something really cute will happen. IT AINT GONNA HAPPEN!!!!!

Poor cynical chap. People are always sending me cute stuff. I don't always want them to, but that's another issue.

(Trust me, I'm still seeing some of the same ones that I waited on 10 years ago!) I don't let the bad luck ones scare me either, they get trashed. (Could be why I haven't won the lottery??)

Those "if you don't forward this you'll have bad luck" messages are sometimes referred to as "St Jude letters", after a particular example: Richard Dawkins, among others, has written about them in some detail. They are, in fact, pointless and mildly evil…

(7) Before you forward an Amber Alert, or a Virus Alert, or some of the other ones floating around nowadays, check them out before you forward them. Most of them are junk mail that's been circling the net for YEARS! Just about everything you receive in an email that is in question can be checked out at Snopes. Just go to www.snopes.com/

As it happens, www.snopes.com is an excellent resource. I recommend it. But you need to read the articles properly…

Its really easy to find out if it's real or not.

Unless it's a new hoax (they all have to start from somewhere, and no anti-hoax site has managed to catch every hoax that's around). Furthermore, hoaxers can be quite inventive: it sometimes takes significant research to establish truth or falsity, even for an expert.

If it's not, please don't pass it on.

Even if it is, it's rarely appropriate to pass on a warning to everyone you know. Well-administered corporate institutions usually forbid anyone to pass on warnings themselves unless explicitly authorized to.

So please, in the future, let's stop the junk mail and the viruses.

If only it were that easy…

Finally, here's an idea!!! Let's send this to everyone we know (but strip my address off first, please). This is something that SHOULD be forwarded.

BANG!!!! Credibility blown to blazes... After all that, it's just another chain letter, no different to all the other chain letters the author is railing against.

Err... No. It isn't something that SHOULD be forwarded, thank you. Even if it were much better advice than it actually is, chain letters that turn up again and again don't usually make up in usefulness for the irritation they cause...]

Here's an idea. Let's not forward this after all.

Other Resources

If you can't find information here on a chain letter or suspected hoax, or simply wish to report it, feel free to forward it to hoaxchecker@gmail.com for a "true or false?" response.

There are, of course, many other resources you can try.

About.com Urban Legends page: http://www.urbanlegends.about.com/

Break The Chain: http://www.breakthechain.org/

Chain letter information page (lots of links and information on pyramid-type chain letters) http://www.cs.rutgers.edu/%7Ewatrous/chain-letters.html

Hoaxbusters.org "The Big List": http://hoaxbusters.org/

Korova "Hoax du Jour": http://www.korova.com/virus/hoax.htm

TruthOrFiction.com: http://www.truthorfiction.com/

Rob Rosenberger's hoax and commentary page: http://www.vmyths.com

Urban legends page: http://www.snopes.com/

Corporate Headquarters

ESET, spol. s.r.o.
Svoradova 1
811 03 Bratislava
Slovak Republic.
Tel. +421 (2) 59305311
www.eset.sk

Americas & Global Distribution

ESET, LLC.
610 West Ash Street
Suite 1900
San Diego, CA 92101
U.S.A.
Toll Free: +1 (866) 343-3738
Tel. +1 (619) 876-5400
Fax. +1 (619) 437-7045
www.eset.com

EWPCHCL20080716