

# **SODDImy and the Trojan Defence**

**David Harley BA CITP FBCS CISSP**

**ESET Senior Research Fellow**

Cyber Threat Analysis Center  
ESET LLC, San Diego, CA 92101, US

Email: [david.harley@eset.com](mailto:david.harley@eset.com)

## **CFET 2010**

**4th International Conference  
on Cybercrime Forensics Education and Training**

## **Abstract**

*SODDI is a familiar acronym among those working in cybercrime: it stands for Some Other Dude Did It. There's nothing novel about criminals claiming that some offence with which they are charged was someone else's responsibility, of course, whether it's the victim or some third party. In the specific area of child abuse, it can be difficult to untangle layers of denial [1, 2] but in recent years frequent use has been made of the Trojan Defence, [3] which might be tersely if loosely summarized as "it must have been a virus" (leaving aside for now the technical differences in malware classification). This attempt at a "Get Out of Jail Free" card is not confined to one type of crime (indeed, it's as likely to be heard in workplace disciplinary contexts as in courtrooms), but it is currently particularly associated with child-related offences, at least in popular perception.*

*As always where child abuse is concerned, attempts to negotiate these murky legal waters have been hampered by a strong emotional undercurrent: debate has been polarized between those who believe that the SODDI defence is about as convincing as "the Internet ate my homework" [4], and those who fear that natural revulsion at paedophile activity and eagerness to prosecute those who practice it may lead to the conviction of innocent parties. In fact, as a general rule, the assertion that "malware installed itself, performed some illegal act, then removed itself leaving evidence of the activity behind but no trace of itself", while not technically impossible, is not particularly likely. But most modern malware is primarily a constantly changing delivery mechanism for attacks that themselves change ownership, target, and context according to market forces and the need to evade tracking by law-enforcement and other interested parties. [5]*

*Much has been made of the way in which the Julie Amero case was compromised not only by forensic flaws and inadequate preservation of the chain of evidence, but by the presence ineffective, obsolete security software. [6] Malware and anti-malware have evolved since then, but has forensic understanding of those evolutions increased correspondingly?*

*This paper will review the 2010 threatscape, considering some cases and scenarios that highlight some of the ways in which malicious software has impacted (or could impact in the future) on investigation, whether by law enforcement agencies or in the workplace. But it will also look at some of the psychosocial issues that may distort our ability to apply our understanding of those technologies appropriately in emotionally charged contexts.*

## Introduction

SODDI is a familiar acronym among those working in cybercrime: it stands for Some Other Dude Did It.

In the context of the problem considered here, the Trojan Defence is a subcategory of SODDI that might be tersely if loosely summarized as “it must have been a virus”. We’ll leave aside the technical differences in malware classification in this paper, though a consideration of the way in which the shift from viruses to other forms of non-replicative malware has affected malware forensics might make an interesting discussion for another occasion.

This attempt at a “Get Out of Jail Free” card is not confined to one type of criminal or disciplinary context. In my time with the NHS the author once contacted a hospital staff member and requested that she stop forwarding a well-known hoax over the NHS network. She responded that their IT department had found a virus on her system which had forwarded the hoax. Now that’s an unusual payload... Nonetheless, malware is credited (correctly, in many cases) with lots of strange payloads that go much further than the cascading letters, ASCII animations and chewed up data of the 80s and 90s.

A few years ago the Trojan defence started to pop up in all sorts of cases, but it is currently particularly associated with child-related offences, at least in popular perception.

There’s nothing novel about criminals claiming that some offence with which they are charged was someone else’s responsibility, of course, whether it’s the victim, the voices or some other third party. In the specific area of child abuse, it can be difficult to untangle layers of denial.

## Six Aspects of Denial [1]

- Denial of the Act
- Denial of the Child as Person
- Denial of the Child as Victim
- Denial of Adult Responsibility
- Denial of Consequence for the Child
- Denial of consequences for the offender.

This paper focuses on first stage denial, according to the model posited by Mezey et al: while there may be incontrovertible evidence of the existence of illegal material (assuming the chain of evidence is properly preserved), the defence in the cases considered here rests on the non-participation of the accused in its acquisition. [2]

## The Case for the Prosecution

The 1988 Criminal Justice Act, Section 160 makes it an offence to be in possession of an indecent photograph of a child. But this isn't the only form of pornographic activity that may lead to investigation, whether it's criminal or otherwise. The primary forms are:

- The possession, viewing, downloading, transmission or any storage of paedophilia-related material or any involvement whatsoever with the traffic of such material.
- The trafficking of bestiality-related material
- Trafficking in other "adult" material.

Even where such activities are not actually illegal, they are usually in breach of national and local Acceptable Usage Policies, and liable to investigation. But we'll focus here on examples of child-abuse related incidents.

According to The Register [7], a resident of Wisconsin whose laptop contracted a virus, took it into his local Best Buy store for repair, even though it contained a number of abusive images. The press reported that the technician assigned to repair it found a child-abusive pornographic image displayed as its desktop background, and attempted to replace it because he was working in a public area of the store. Finding more pornographic photos in the "My Pictures" folder he notified his manager, who called the police, and they, apparently, found 67 abusive images on the computer.

You might think it's strange to take a machine with this kind of content to a store for repair, but one-time rock star Gary Glitter was jailed for 4 months in 1999 under somewhat similar circumstances with something like 4000 abusive images on the machine for repair. [8]

Graham Cluley [9] noticed a resemblance between the Wisconsin case and a case from 2005.

Dear Sir/Madam,

We have logged your IP-address on more than 30 illegal Websites.

Important: Please answer our questions! The list of questions are attached.

Yours faithfully,

Steven Allison

Federal Bureau of Investigation-FBI-  
935 Pennsylvania Avenue, NW , Room 3220  
Washington , DC 20535  
Phone: (202) 324-30000

**Figure 1**

Sober-Z is an elderly mass mailer that used messages like the one in Figure 1 to trick victims into opening a malicious attachment. In this instance, a 20-year-old German man got a message claiming that he was being investigated by Germany's Federal Crime Office for "visiting illegal websites." After the individual in question turned himself in, police did indeed find pornographic pictures of children on his computer.

As Shakespeare might have said, the plague's the thing wherein I'll catch the conscience...

## A Novel Approach to Courtship

According to the Times [10] (see Figure 2), Ilkka Karttunen became so obsessed by a co-worker that he tried to break up her marriage in the hope of establishing a romantic relationship with her. He broke into her home and used the family computer to download abusive images of children, then stole the hard drive and sent it anonymously to the police.

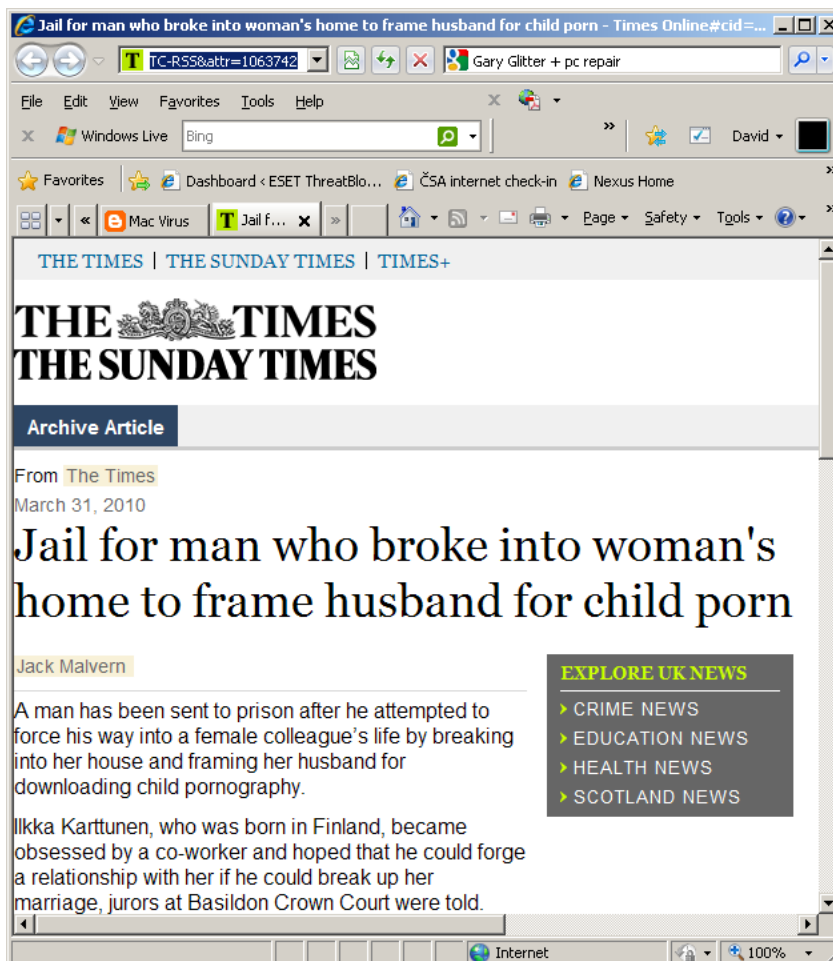


Figure 2

Officers discovered evidence of Karttunen's involvement on a computer in his garden shed, but it's not clear how they came to make that search from the report.

Analysis with specialist software showed that it contained the entire contents of his victim's home computer. In the meantime, of course, the husband had been arrested and denied access to his home and children.

## **Caretaker took insufficient care...**

There is an episode of "Judge John Deed" (a UK television drama known to the unenthusiastic as Judge Dreddful) where the establishment tries to neutralize the pompous crusader by planting child abuse images on his laptop. [11]

According to a story by John Oates in The Register [12], a caretaker in East London pulled a similar stunt against his colleague in the hope of getting his job, and sent police a CD containing 177 child sex abuse images that he claimed came from his co-worker's computer. Police found another 235 images on the co-worker's laptop. However, the culprit was arrested after police traced the mobile phone used to make the original anonymous call.

In fact, there was an epidemic of attempts made by Eastern European "Cyber-extortionists" in the first decade of the 21<sup>st</sup> century to extort relatively small sums by threatening to wipe the hard drives of their victims, or to plant child-abusive images on their systems, so there's more to this than far-fetched TV plotting. Mark Rasch suggested that "the possibility of Trojans and the relative ease with which they could be used to promulgate such an attack made the threats credible." [13].

And indeed, Haagman and Ghavalas remark in a paper published by on the Trojan defence [3] that "storing files on other systems is a common tactic for attackers. Individuals who share copyright protected materials store their contraband on high-speed servers; hackers store their 'rootkits' on compromised systems or other publicly accessible servers." The reference here is to distributed storage of illegal materials in general, in the context of botnets. However, it's perfectly possible that child abuse-related material in particular may be stored in such contexts.

## **So what about the forensics?**

What have we seen so far? Detective work, yes. Psychological analysis, yes.

But there's no particular emphasis on exhaustive, bit by bit analysis of disk images in these accounts, apart from a reference to specialist forensic software used in terrorist cases in the Kartunnen story. However, in 2003, an article by Neil Barrett highlighted a trial in which illegal, pornographic material seemed to have been placed on "an innocent man's computer by a Trojan program

In this case, though, there apparently *was* evidence: a Trojan was found linked explicitly to the paedophile pictures. According to Barrett, the defendant had not accessed the pictures and that he could not have known they were on his computer.

This conclusion was reached even though Devon police found child-abusive images on the accused individual's home PC, and ISP logs seemed to identify him as responsible for the

downloads. However, evidence was found that there *were* Trojans planted on Green's computer that hijacked his browser and logged into porn sites. The prosecution was unable to prove definitively that the files were knowingly and intentionally downloaded, and the charges were therefore dismissed.

## **We Have A (Dos) Problem, Houston.**

Another individual was charged in Southwark Crown Court with carrying out a denial of service (DoS) attack on the computers of the port of Houston, Texas in 2001, after ISP logs traced the attack to his computer.

In this case, a forensic audit of the computer showed no trace of a Trojan. However, he argued that a Trojan *could* have been responsible for the attack, and that the government could not prove its case "beyond a reasonable doubt". The jury was apparently convinced by his expert credentials: he was acquitted in October, 2003. It was a cause of considerable concern in law enforcement and security circles at the time that just the bare possibility of an undiagnosed infection was seen as introducing enough reasonable doubt to dismiss a case. Would we start seeing the Trojan defence causing failed prosecutions in all sorts of unexpected contexts?

Fortunately, this has so far been more of a trickle than an avalanche, and there have been cases where the Trojan defence has failed.

## **Unsuccessful Use Of Trojan Defence: Child Abuse Case**

Barrett has stated [14], referring specifically to child abuse cases, that the Trojan defence has been implausible where experts were able to show that

- Pictures had been viewed and moved around.
- No indication that were loaded as pop-ups
- No indication of spam email
- No evidence of the presence of a Trojan

However, he also cites three possible defences:

- The picture is there for a legitimate reason, as in the possession of an authorized investigator, or the individual has been asked to retain the picture by the police pending investigation. Of course, if they tell you to delete them, there is also some protection if subsequent investigation finds *deleted* images, though there may be some scope for misuse there.
- The system user hadn't seen the picture or had no reason to believe it was in breach of the law.
- The material was unsolicited and not kept for any length of time, a defence that is considered to cover the instance where extreme material is transmitted in spam

(though direct transmission as spam has probably diminished dramatically in recent years).

Barrett suggested that in the event of receiving such spam, you should contact the police or delete them immediately. And indeed, in an earlier phase of his career, the author had to spend a lot of time deterring people from forwarding such material for evaluation, since that would make them a "distributor" and in "knowing possession" of the image.

## **The Child Porn Virus**

In the Red corner: those who believe that the SODDI (Some Other Dude Did It) defence is about as convincing as "the dog ate my homework"...

In the Blue corner: those who are concerned that natural revulsion at paedophile activity and eagerness to prosecute those who practice it may lead to the conviction of innocent parties...

A recent article by Geoff Liesik on "Authorities scoff at 'child porn virus' tale" [15] revisits the schism between the two groups.

The question revolves around the assertion that malware was installed, downloaded illegal material, then removed itself leaving no trace of itself except the residue from its payload, such as pornographic records. (Again, we'll disregard the fact that this issue is much more about malware in general than it is about viruses, technically speaking.)

This defence has been accepted in the past, but a sophisticated jury nowadays is likely to wonder why such a Trojan (which is not technically impossible, though unlikely) would have been installed

The likeliest scenario seems to be that one person might use the technique to "frame" another, as we saw in previous examples: however, an investigator would still be interested in the identity and motivation of the malefactor, as well as the technical and forensic issues of access and programmatic behaviour.

But what if there's no motivation, no deliberate targeted attack?

## **I, Bot**

Botnets are highly adaptive networks of compromised computers [16]. Range, components and structure changes according to need as zombie PCs (infected with a bot or agent software that controls the infected PC) and servers are taken down, and as the attack type and target changes. For example:

- DDoS attacks (for purposes of revenge, extortion, or self-protection of the botnet)
- Use of distributed processes for click fraud, captcha breaking, and for disseminating scams and spams and other malware
- Storage and distribution of other illicit content



So what does “adaptive” mean? Bots and botnets are apt to:

- Change shape
- Self-update
- Change role
- Change the function of the “zombie” PC.

Botnets are a highly dynamic, fluid ecosystem [17]. Zombie systems are switched in and out, and control and function passes from one botmaster to another. Software is updated and replaced, even supplanted by malware from a different source. Potentially, a bot-infected system is an agent for anything that makes money [18], such as those listed in the previous slide. It’s a participant in orchestrated, distributed attacks. It may be used as a command and control server, as a drop box for stolen credentials, as a repository for malware, and other illegal material.

But it’s also a battleground: a vulnerable machine may perform many attacks for many customers of more than one botmaster, and each of those attacks may leave a layer of residue. The remote administrator doesn’t care about what is left from previous attacks as long as it doesn’t affect his ability to make use of the system.

And the system’s nominal owner may have no more idea of what’s happening on “his” system than you and I have of what’s happening sub-microscopically in our own bodies. If he is aware that something is not “right” he may have no idea of how to fix it, or take inappropriate measures such as the use of rogue security software.

Above, we saw a summary of contraindications of Trojan defence [14]. But that summary assumes a far more static environment than the one I’ve just described. Files may be accessed for reasons other than viewing, and they may or may not be moved around. If they’re installed by malware, it’s not unlikely that they’ll be somewhere hidden where they can reside comfortably until an investigator comes along and unearths them. Spam email comes and goes, and may be deleted with no indication left of damage that it’s done. In a world where tens or hundreds of thousands [5] of unique malicious binaries are processed daily, finding evidence of one Trojan on a beleaguered system is not a trivial task.

## **The Case for Scepticism**

Capt. Rhett McQuiston supervises the Internet Crimes Against Children Task Force for the Utah Attorney General's Office. In 2009, he responded [15] to an Associated Press report of innocent people labelled paedophiles as a result of pornographic images installed on their PCs by malware, and suggesting that pedophiles might use infected computers to store and view images and videos.

(Well, there are very recent reports [19] of Facebook being used to store and exchange paedophile material, but a paedophile ring might also employ the services of a botnet crew, as already mentioned. Indeed, social media are starting to look like the new botnet ecology. )

McQuiston stated that his team had had individuals make that claim, but that investigation had always proved otherwise.

That disproof comes in many forms. A confession made during interview isn't really within the remit of this presentation, but forensic examination looks for:

- Review of visits to known bad sites
- Quantity of stored images
- Number of accesses to stored images
- Keywords entered into search engines

McQuiston said, reassuringly, that "we've never once just gone off the images alone and said we're taking someone to jail. Let's hope so.

## **There Is No "Mystery Porn Virus" (Probably)**

But there is a lot of morphing, self-protective malware. Beware of Greek gods bearing bots ...

No report I've seen has mentioned specific malware (most have just said "viruses" and the use of that term in itself makes it hard to estimate how much credence to give to the reports).

The "take home" point here is that *in principle* many malicious programs might have functionality at some point in their life-cycles: for instance, in order to use a victim's machine as a repository for illegal material, and might also have self-protective and morphing characteristics that could compromise forensic analysis in terms of establishing guilt or innocence.

Sophos have reported [20] Zeus samples "crafted to ensure that they only work when executed on one specific machine and from one specific path. Any attempt to execute the sample on a different machine or from a different path will result in early termination of the malware and no impact on the target system"

Zeus is normally associated with banking Trojans, attacks on military sites and possibly even SCADA sites, not paedophile activity. But there are many overlaps and dependencies in the black economy. Coders are not necessarily "contracted" to a single gang, and unexpected dependencies crop up all the time. For example, it's been suggested that the Stuxnet worm used for attacks on certain SCADA installations was able to use Verisign certificates stolen from Jmicron and Realtek [21] because they were acquired in some way from Zeus, which is known to steal certificates [22]. That's just one theory, of course, but it is at least an indication of how little insight we have into the alternative economy.

## A Pinch of Salt Lake City

Joseph Jardine, a Salt Lake criminal defense attorney, on the other hand, suggested [15] that Utah presents particular problems where “so many home computers have only one login and password but are used by multiple people.” I don’t know how Utah compares in that respect to other parts of the US, or indeed the world, but the assertion may hold true in some corporate environments. Certainly, when the author’s role included direct user support, telling customers not to share passwords was a continuing theme, and the audit trail issue was one of the factors behind it.

Jardine also suggested that the need to secure a conviction may override the interests of the accused and raised the spectre of defence and economics, claiming that “...employing his own examiner to review the forensic investigation conducted by authorities...can add \$5,000 to \$10,000 to a client’s legal bill...”

One resident of Wyoming might agree: he is, reportedly, currently serving six years for child porn found in a folder used by a file-sharing program on his computer. He asserts that he used the program to download video games and adult porn, but not child porn.

An investigator testified that his antivirus software wasn't working properly and suggested an infection. She found no evidence that videos on his computer had been viewed or downloaded fully, but the pursuit of that defense was curtailed, when she ended her investigation due to a dispute with the judge over her fees. [23]

A prosecution forensics expert, Randy Huff, on the other hand, maintained that the accused man’s antivirus software was working properly, and that he ran other antivirus programs on the computer without finding an infection.

It pains me to say this, given the industry that has paid my mortgage for some years now, but it’s not unknown for AV to miss malware. Of course, what is more problematical is that the article suggests that establishing whether the AV was working was critical to the success of the prosecution. There’s no suggestion that a more searching forensic analysis was carried out.

The Julie Amero case was not directly concerned with child pornography – the offences of which she was convicted were related to “risk of injury to a minor, or impairing the morals of a child”. But it is somewhat apposite in that it was compromised by significant forensic flaws in procedure, questionable use of investigative technology, and optimistic assumptions of the effectiveness of obsolete security software. [6]

No-one, as far as I'm aware, has found an (untargeted) malicious program that *always* downloads illegal porn to a victimized system. However, if you find that there is *something* installed that is *still* downloading child-related pornography at the time of investigation, *and* you can state with some certainty that "something" is malware rather than a black utility

deliberately installed by the user to facilitate the downloading of illegal material, there may be a viable defence.

Unfortunately, if you find malware that doesn't have that payload, it's still possible to argue that it might nevertheless have had it at *some* point since the machine was infected, because it's highly characteristic of botnets to change the function performed by individual infected machines according to the changing requirements of the botmaster or his customers.

Certainly, that's far too much like a get-out-of-jail-free card for comfort. No-one is in favour of imprisoning the innocent, but it's likely that a lot of guilty people will continue to try to use this approach.

However, the only way of mitigating (*not* fixing) this ambiguity is by absolutely scrupulous forensic examination. Yet maintaining the integrity of the chain of evidence is, though critical, by no means the hardest part of the problem. The only sort of forensic investigation that stands a chance of giving useful information in this scenario involves all sorts of legal, resourcing and administrative complications. To do it properly requires *more* than forensic skill and in-depth knowledge of malware (not to mention a strong stomach and appropriate clearance). Not a job that most people would relish, and one with a notoriously high burn-out rate.

The sort of examination that's hinted at in some recent reports suggests a form of dynamic analysis that involves reproducing the illegal behaviour. Sometimes this may be the only way of gathering evidence, but it's an approach with obvious and murky legal implications.

A more generic legal approach might be to link the fact that at least one of the "victims" cited in recent reports did admit to downloading "adult" porn, which, irrespective of legality or morality, escalates the risk of exposure to malware and to other forms of porn: porn merchants don't care about what they push as long as they don't expose -themselves- to punitive action. So there's an element of reckless endangerment, especially when a victim doesn't have properly functional security software, as may have been the case in that particular instance. But is a long sentence appropriate if the suspect's crimes are too much faith in his security software and an expensive expert witness?

## **Selected Bibliography**

[1] Murphy, W.D. (1990) *Assessment and Modification of Cognitive Distortions in Sex Offenders*, in "Handbook of Sexual Assault: Issues, Theories and the Treatment of the Offender".

[2] Mezey, G. et al. (1991) *A Community Treatment Programme for Convicted Child Sex Offenders: A Preliminary Report*. *Journal of Forensic Psychiatry* 1: 11-25.

- [3] Haagman, D., & Ghavalas, B. (2005) *Trojan Defence: a Forensic View*. Available from: [http://220.231.93.23:8000/collect/EN-digital/index/assoc/HASH815b.dir/1c\(53\).pdf](http://220.231.93.23:8000/collect/EN-digital/index/assoc/HASH815b.dir/1c(53).pdf) (Accessed: 3<sup>rd</sup> July 2010).
- [4] Liesik, G. (2009) *Authorities Scoff at 'Child Porn Virus' Tale*. Available from <http://www.deseretnews.com/article/705343760/Authorities-scoff-at-child-porn-virus-tale.html> (Accessed: 3rd July 2010).
- [5] Harley, D. (2009) *The Game of the Name: Malware Naming, Shape Shifters and Sympathetic Magic*. Available from: <http://www.eset.com/resources/white-papers/cfet2009naming.pdf> (Accessed: 3rd July 2010)
- [6] Phillips, D., Harley, J., & Harley, D. (2007) *Education in Education*. In "The AVIEN Malware Defense Guide for the Enterprise, ed. Harley (Syngress).
- [7] [http://www.theregister.co.uk/2010/05/19/child\\_abuse\\_pc\\_repair/](http://www.theregister.co.uk/2010/05/19/child_abuse_pc_repair/)
- [8] <http://news.bbc.co.uk/1/hi/uk/517604.stm>
- [9] <http://www.sophos.com/blogs/gc/g/2010/05/18/child-porn-desktop-virusinfected-pc-repair/>
- [10] <http://www.timesonline.co.uk/tol/news/uk/article7081986.ece>
- [11] [http://en.wikipedia.org/wiki/List\\_of\\_Judge\\_John\\_Deed\\_episodes](http://en.wikipedia.org/wiki/List_of_Judge_John_Deed_episodes)
- [12] [http://forms.theregister.co.uk/mail\\_author/?story\\_url=/2010/08/05/caretaker\\_plot/](http://forms.theregister.co.uk/mail_author/?story_url=/2010/08/05/caretaker_plot/)
- [13] [http://www.theregister.co.uk/2004/01/20/the\\_giant\\_wooden\\_horse\\_did/](http://www.theregister.co.uk/2004/01/20/the_giant_wooden_horse_did/)
- [14] <http://www.computing.co.uk/itweek/comment/2085900/beware-trojans-bearing-gifs>
- [15] <http://www.deseretnews.com/article/705343760/Authorities-scoff-at-child-porn-virus-tale.html>
- [16] Bradley T. & Harley D. "Big Bad Botnets" in "AVIEN Malware Defense Guide for the Enterprise", ed. Harley, Syngress, 2007.
- [17] Harley D. & Lee A. "Net of the Living Dead: Bots, Botnets and Zombies", February 2008. [http://www.eset.com/resources/white-papers/Net\\_Living\\_Dead.pdf](http://www.eset.com/resources/white-papers/Net_Living_Dead.pdf)
- [18] Schiller C. et al., "Botnets: the Killer Web App", Syngress, 2007
- [19] <http://www.telegraph.co.uk/technology/facebook/7966538/Child-porn-pictures-posted-on-Facebook.html>
- [20] <http://www.sophos.com/blogs/sophoslabs/?p=10519>
- [21] Harley D. "Chim Chymine: A Lucky Sweep?" Virus Bulletin, September 2010.

[22] Harley D., "There's Passwording and there's Security":<http://blog.eset.com/2010/07/20/theres-passwording-and-theres-security>

[23] <http://ricorant.blogspot.com/2009/11/thatll-teach-you-to-run-that-anti-virus.html>