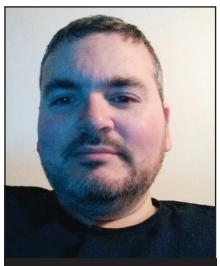
The first 10 years of the Trojan Horse defence


Stephen Bowles


Julio Hernandez-Castro

Stephen Bowles and Julio Hernandez-Castro, University of Kent

Apprehended criminals throughout history have always attempted to put the blame on someone else, a strategy popularly known as a SODDI defence (Some Other Dude Did It). When this defence is used, the act of the crime (*actus reus*) and the guilty mind *(mens rea)* is blamed on another party. A Trojan Horse Defence (THD) is a type of modern SODDI defence, where the *mens rea* and *actus reus* are blamed on a piece of software, known as a trojan.[1]

A trojan is a type of malicious software (globally known as malware) that is either packaged along with a useful piece of software or pretends to be a piece of useful software itself. Once a trojan is activated, which usually goes unnoticed by the user, it releases a payload such as a virus or a backdoor that may allow a remote user to gain access to the system.[2,3] A popular means of infection is for online downloads to be packaged with a trojan, resulting in an infection when the user runs the downloaded application. The more complex trojans – those that capture typed keyboard characters or permit a remote user access to the system – can be used to create a credible legal defence. This is in contrast to simple trojans, which act as a nuisance by deleting files and changing user settings.

The THD is believed to have been first used in 2003, when it appeared in the Charles Schofield case.[4] After a literature review of relevant publications over the past decade, this article discusses court cases where the THD has been used.

The prosecutor's view

In 2004 Susan Brenner and her colleagues wrote a paper that primarily concentrates on the view of the prosecutor. As it was major news at the time, the paper focuses on the Caffrey case, regularly linking points to it. The paper reservedly states that the defence could be "empirically valid". However, especially with recent advancements in malware, it should be stressed that it is entirely possible for a trojan to be the cause of a crime. The paper provides an introduction to four 2003 court cases and then continues on to a discussion of the legal and technical issues regarding the THD.

"The paper suggests that a thorough examination is only needed if malware is found – however it is not that simple. A thorough investigation is always required, partly because a quick analysis might miss things, but also because malware may still be responsible"

The opening statement of the paper's 'Legal issues' section highlights potential problems, where criminals use a THD in their favour or an innocent user is charged with a crime that they did not commit. In the same section's summary, the paper suggests that a thorough examination is only needed if malware is found – however it is not that simple. A thorough investigation is always required, partly because a quick analysis might miss things, but also because malware may still be responsible, even if traces of malware are not found on the machine.

The 'Technical issues' section provides an overview of malware, trojans, 'virtual crime' and the 'bot defence'. While it lacks intricate technical details, it does provide a gentle introduction to terms that all parties in a THD should be aware of. The section also discusses procedures to follow when performing an analysis on a system, as well as what can be done depending on whether traces of malware are found.

Finding out how the digital evidence came to be on the computer is important, and this is highlighted in the summary section. This section also discusses how the digital evidence, such as malware, could have used entry and exit points to get onto the computer, something of which all investigators should be aware. Overall, the paper provides a good introduction into the THD and raises many valid points that prosecutors should thoroughly consider.

The forensics and technical side

A 2003 paper added a thorough discussion about digital forensic techniques and provides intricate details on how a forensic investigation should take place on a Windows- or Linux-based system.[5] Although perhaps dated, many of the techniques and tools mentioned are still valid and used today. The paper primarily focuses on data recovery; however it also discusses viewing logs and tracking the activities of a hacker. The paper

makes a significant point that, in some cases (which we report on later), investigators failed to perform an important step – which is to make a copy of the hard drive and its contents and then proceed to carry out the investigation on that copy. This is important so the evidence is not altered and the investigation can be carried out by other parties.

"It is considerably easier today for a malicious party to modify a malicious program that, when hashed, matches a safe value or a hash of a lesser malware"

A reader should be aware of the current significance that recent developments bring to technology. For example, where the paper suggests using cryptographic checksums MD5 and SHA-1 to check a file system, we suggest that, in light of the multiple security vulnerabilities recently discovered, it would be better to use SHA-1 instead of MD5, or even SHA-2 or SHA-3. Although it has been recently stated that MD5 and SHA-1 are still valid for digital forensics, it is considerably easier today for a malicious party to modify a malicious program that, when hashed, matches a safe value or a hash of a lesser malware.[6] Some authors have highlighted how a hex editor can be used to change the signature of malware, making it, in some cases, no longer recognisable by protection software.[7]

The two-part 2005 paper (Haagman and Ghavalas) discusses techniques to develop trojans and scenarios of trojans compromising a system. The paper also discusses volatile and network evidence, areas barely touched by the previously mentioned 'Issues in Computer Forensics' paper. Evidence that can be collected from a system's memory and evidence from the network, such as activity logs, could be invaluable in a case.

Finally, another recent 2012 paper (Sepec) provides the reader with an insight into the difficulties that forensic examiners face, and the steps they should take. The paper details trojans, their behaviour, how they work and the THD. Although it refers mostly to Slovenian law, the contents remain significant and relevant for other legal systems. In regards to THD cases, the paper mentions four key considerations and although they are not the only ones to take into account, they are nonetheless quite important. In brief they are:

1) Investigators should use several up-to-date investigative programs.
2) Digital evidence is not the only evidence to be considered in cybercrime offences.
3) Expert testimonies on the mental state of the accused is relevant.
4) Consider that the accused might have planted a trojan on their computer system as a defence tactic.

Statistics

A 2004 paper (Carney and Rogers) details an attempted stepwise discriminant analysis of four scenarios, all which resulted in five illicit images of children being created on the system.[8] The goal was to see, "whether an investigator could determine if images were downloaded intentionally or without the owner's knowledge based on characteristics located in the operating and file system". The paper lists seven characteristics of an operating and file system, which it proposes an investigator should look at when performing an investigation. The results from this analysis proved interesting and showed that it might be possible to create an accurate statistical model, although much more work is required in this area before that becomes a reality.

Other authors have looked into plausibility metrics and posterior odds, where they discuss an Operational Complexity Model and an Enhanced Complexity Model (ECM).[9,10] In a personal communication with one of the authors, Richard Overill provided the following summary: "On the basis of the ECM we are suggesting that the Trojan Horse Defence is a rather implausible defence, provided there is an up-to-date anti-virus/malware scanner installed. When compared with other accepted forensic techniques (fingerprints), the Enhanced Complexity Model shows a lower odds ratio against the THD, which implies that this kind of complexity based metric is not as clear-cut as a biometric like fingerprinting or DNA. Also, of course, the biometric identifies an individual whereas the ECM on its own does not; it simply says that it is 198 times more likely that an individual did it rather than a TH."[11]

"Anti-virus software provides very little protection, other than to avoid questions in court as to why there is no anti-virus software installed on the relevant computer"

However, we believe that this approach, while still having some merit, is no longer true, because malware is becoming increasingly equipped with tools to disable or hide from anti-virus software. Although more research is required here, we believe that anti-virus software provides very little protection, other than to avoid questions in court as to why there is no anti-virus software installed on the relevant computer.

Defending against a trojan

The usual defence against a trojan includes anti-malware, anti-virus and firewalls. However, some authors have recently suggested other measures to improve defences against a trojan.

A 2010 paper suggests that an 'Education, Enforcement and Engineering' or 'Triple-E' approach could be taken.[12] For education, the paper suggests changing the perception of people towards hackers, teaching how to use a computer appropriately, and teaching the public safe habits when using a computer system and the Internet. The authors,

relating enforcement to procedures for fact finding and investigations, propose the MDFA (Multi-faceted Digital Forensics Analysis) strategy. MDFA is a range of procedures for collecting and linking characteristics from the four phases of a crime that the authors list as evidence, scene, victim and suspect. The M-N model and Ideal Log are discussed for the engineering part of Triple-E, where both focus on logs (such as audit logs) and the task of building a series of events by synchronising events that could be from different time zones, which can happen because the time on a client may not be the time on a server or the network devices in-between.

"It is important to note that, as mobile technology is becoming dominant, the next THD case could involve a smartphone"

Other papers suggest an intrusion detection system to work alongside other software, which will attempt to detect potentially malicious programs.[13,14] Although these papers take different routes, the general principle is the same – having a system in place that monitors and tracks the execution of programs and the resources they attempt to use. By placing programs into different levels, where one level has higher trust or permissions than another, the system can alert a user if a program is attempting to access something it should not. The concepts discussed here are similar to User Access Control (UAC), a system in use by some of the more recent Microsoft Windows operating systems.

Mobile

When considering the THD, it is too easy to think only of the classical scenario – a home, possibly family-shared, desktop PC. However, it is important to note that, as mobile technology is becoming dominant, the next THD case could involve a smartphone. Although some papers have started to discuss the mobile malware topic, awareness needs to be raised regarding smartphone security.[15]

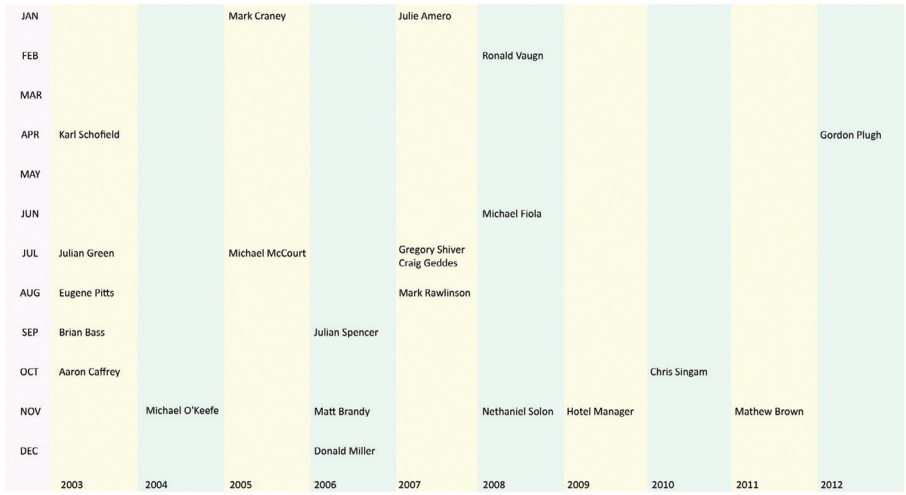


Figure 1: Timeline of cases where the trojan defence (or similar) was used or mentioned.

Court cases

Table 1, along with the timeline shown in Figure 1, provides what we believe to be the currently most detailed and comprehensive list of court cases where the THD (by this or a similar name) has been used. The date within the table corresponds to the conviction or acquittal date. Where it was difficult to accurately gather the date, an educated guess is used, based on time of articles published, news stories or the appeals documents. This section will discuss some of the most notable cases listed in Table 1.

Aaron Caffrey

The first heavily publicised THD case was the 2003 Aaron Caffrey case. The Port of Houston, in the US, suffered a denial of service (DoS) attack, which was traced back to Caffrey's machine. This case is interesting because no evidence of a trojan was found.[16] Furthermore, Caffrey was a member of a hacking group and tools that could have carried out the attack were found on Caffrey's system.[17] During the case, Caffrey made false claims that were not disputed, such as an anti-virus cannot scan every file on a system, which is blatantly false. Even with a possible motive identified, Caffrey was acquitted on the argument that he was being framed by another hacker by means of a trojan.[18]

Eugene Pitts

The 2003 Eugene Pitts case is different from any others, as the type of crime was very different. Pitts was accused of income tax evasion in the US and even though he had a history of troubles, where he was accused in previous years of under reporting income, he was acquitted under the claim that a virus was responsible for modifying his files.[19,20] It was noted, however, that his customers' tax returns, which were on the same system, were surprisingly not affected by the virus at all.

Michael Aaron O'Keefe

This case involves a defendant who apparently created two websites, modelquest and hctweens, to catch paedophiles.[21] Michael Aaron O'Keefe was arrested and accused of advertising, receiving, and possessing indecent images of children.[22] The websites that O'Keefe had apparently created to catch paedophiles were hosting child pornography images, something that O'Keefe said a virus must have done.

Logs were also found that show O'Keefe was posing as a young girl, apparently in an attempt to lure

Date/Place	Victim/Crime/Evidence	Defendant	Result	Notes
2003 April, UK	Possession of 14 indecent pictures of children	Karl Schofield	Acquitted: "unnamed trojan did it"	An analyst found and testified that a trojan was responsible.
2003 July, UK	Possession of 172 Indecent pictures of children	Julian Green	Acquitted	Martin Gibbs, working at Vogon International, found 11 trojans on Green's system.
2003 August, US	Evasion of tax/income tax evasion	Eugene Pitts	Acquitted	It was noticed that Pitts had previous a history of issues; also it was odd that the virus did not affect any customers' tax returns.
2003 September, US	Possession of 2,000+ indecent images of children	Brian Bass	Convicted on five counts	Bass used history remover software, claimed to have a "morbid curiosity" with child porn, but blames a virus for downloading the images.
2003 October, UK	Denial of service attack on the Port of Houston, US	Aaron Caffrey	Acquitted: "trojan did it"	Caffrey was a known hacker, possessed hacking tools, and no evidence of a trojan was found.
2004 November, US	Buying, advertising and owning child pornography	Michael Aaron O'Keefe	Convicted on four counts	Claimed to have created websites to catch paedophiles; blamed the indecent imagery being hosted on a virus.
* 2005 January, UK	Possession of 1,793 indecent images of children	Mark Craney	Convicted on 16 counts	Claimed a virus was to blame.
* 2005 July, US	Possession of 320 indecent images and videos of children	Michael Shawn McCourt	Convicted on two counts	Claimed a hacker put the images on the system using peer-to-peer programs.
2006 September, UK	Possession of 3,000 pictures of child pornography	Julian Spencer	Guilty plea	When arrested, Spencer claimed a virus was to blame.
2006 November, US	Possession of nine indecent images of children	Matthew Bandy	Plea-bargain to avoid going to court	Over 200 viruses and malware were found on the system belonging to the 16 year-old.
2006 December, US	Possession of child pornography	Donald R Miller	Convicted	Unsuccessful claim that a virus downloaded the images, which got mixed in with other, legal pornography.
2007 January, US	Exposing children to illicit imagery	Julie Amero	Initial 2007 conviction was thrown out. Disorderly conduct guilty plea in 2008	Malware caused pop-ups to appear, which Amero struggled to remove. Experts used had questionable expertise.
2007 July, US	Possessing and transporting indecent images of children	Gregory James Shiver	Convicted	During the case, a brief mention that 'pop-ups' or a virus had placed the images on the computer was made.
2007 July, UK	33,000+ indecent images and 1,000+ videos of children	Craig Geddes	Convicted on possession of child pornography	A detective in the case said she had never heard of a virus that could install child porn, even though defendants have been acquitted before on this reason.
* 2007 August, South Africa	1,159 indecent images of children	Mark Rawlinson	Convicted on 330+ counts	Believed to be the first use of the THD in South Africa.
2008 February, US	Two counts of possession and one count of receiving child pornography	Ronald Vaughn	Convicted on all three counts	A post-trial attempt at the THD was made, but failed, as evidence was found on multiple systems with the only common user being Vaughn.
* 2008 June, US	Government work laptop contained indecent pictures of children	Michael Fiola	Acquitted after investigation proved innocence	Forensic examiner Tami Loehrs found the system was infected months before it was given to Fiola, by the state. Malware visited 40 child porn websites a minute.
2008 November, US	Receiving and possession of child pornography	Nathanial Solon	Convicted after initial guilty plea was withdrawn	Apparently an expert hired by Solon found evidence that could prove his innocence. There are claims that the judge behaved oddly, such as walking out without reason for a trivial matter.

* 2009 November, UK	Child pornography	Hotel Manager	Apparently cleared as a result of a trojan/ virus	Reportedly Chris Watts, a forensic investigator, helped clear the hotel manager on charges of child pornography.
* 2010 October, UK	Possession of 30 indecent images of children	Chris Singam	Acquitted	Defence team hired a digital forensic investigator who found evidence of malware. The police examination was not performed by an expert.
2011 December, US	Possession of indecent images of children	Matthew Brown	Charged on two counts	Brown claimed a trojan downloaded videos, while he only viewed 100 indecent images of children.
2012 April, US	600+ indecent images of children	Gordon J Plugh	Guilty plea	A THD claim was made but later withdrawn.

Table 1: Cases where the trojan defence (or similar) was used. Dates with asterisks are estimated.

paedophiles.[23] Within this case, evidence of malware that allowed a remote user to gain access to the defendant's system was found. As there was no evidence that O'Keefe ever made any effort to inform or help law enforcement of his actions or motives, the claim that he was trying to catch paedophiles was not believed.

Julie Amero

Julie Amero's case is an example of the serious miscarriages of justice that have occurred in some THD cases. Here, the simplest forensic techniques were not used, the computer experts used had questionable knowledge and made false claims, and events were blown out of proportion by parents and prosecutors, as it is highly questionable if any damage was done to the pupils who saw the pornographic pop-ups.[24,25]

During the case, Amero's system was not scanned for viruses or malware, and for what little investigation did happen, it did not follow best practices, as the investigator worked off the hard drive rather than making a copy.[26] This case helps show why parties involved must be careful, as the stress of the case has been blamed for the miscarriage of Amero's unborn child.[27]

Matthew Bandy

The 2006 Matthew Bandy case is another clear miscarriage of justice. Detectives in Bandy's case did not seem aware of the steps that should be taken, which included requesting a digital forensic analysis, and as a result multiple mistakes were made.[28] After being named a paedophile, a digital forensic investigation found that the anti-virus software was disabled, there was no firewall, and there were a myriad of infections and running malware, some of which had the capabilities to place pornography on the system.[29] This case ended in a plea-bargain, but had it gone to a jury, the result would have been again unpredictable, as we have seen in other cases with the jury, even when the evidence is nearly identical.

Craig Geddes

Craig Geddes' 2007 case is very similar to other THD cases where the defendant was acquitted, although in this particular case Geddes was convicted. Geddes asked, "Can a virus do that?", the answer to which is yes. But during the case the opposite was stated.[30] Detective Constable June McKay, of Strathclyde Police computer crime unit, said that they had never heard of a virus that could place child porn on someone's system.[31] This is a worrying claim by a computer crime detective, especially several years after similar cases. Other dubious claims include incorrect statements regarding changing IP address. During the case, no evidence was shown of any digital forensic investigation, making Geddes' innocence conceivable.

Mark Rawlinson

Although information on Mark Rawlinson's case is scarce, it is worth mentioning as it is believed to be the first use of the THD in South Africa.[32] Cases outside of the UK and US are not as well documented, but the THD can happen and does get used in other countries, of which Rawlinson's case is an example. Rawlinson's THD claim failed and he was convicted of possessing over a thousand illicit images of children on his system.

Michael Fiola

Michael Fiola's 2008 case stands out by its remarkable conclusion. Fiola was arrested and lost his job, as indecent images of children were found on his laptop. Unlike other cases, such as Amero's, a digital forensic investigation was conducted by a qualified forensic examiner. The other major difference with other cases is that the laptop in question was a government issued computer, from the Department of Industrial Accidents in Massachusetts, US, where Fiola was working at the time.

The results from the forensic investigation found that the laptop was infected with malware months before it was given to Fiola. It was also found that the malware in question was visiting 40 child porn websites a minute. Although Fiola was acquitted with this evidence, the department never offered an apology or his job back.[33,34,35]

Nathaniel Solon

Nathaniel Solon's 2008 case seems to be another miscarriage of justice example.[36] Solon's case initially followed a

path similar to other cases, which led to acquittals. The same digital forensic investigator from Amero's case was involved in Solon's, where some evidence of a virus that could have downloaded the pornography was found but no evidence of the material being viewed by Solon was found.[37,38] The findings were seemingly ignored and as a result Solon was convicted only because of the material found on his system. A later appeal claimed that the behaviour of the judge swayed the jury, who disregarded the investigator's findings and was unhappy with the fees.[39]

Recent developments

With the huge increase in cyber-criminals using ransomware, the future looks grim.[40] Ransomware is a type of malware, often the payload to a trojan, that is used by cyber-criminals to hold a user to ransom.

In 2013, Jay Riley's system was infected with ransomware that pretended to be from the FBI and asked Riley to pay a fine. After Riley asked the police if there was any warrants out for him and volunteered for a search, he was arrested, because indecent images of children were found on his system.[41] As well as possession, Riley was also charged on "1 count of indecent liberties with a minor", as one of the images was of a 13-year old girl from Minnesota, roughly 1,000 miles away from Riley in Woodbridge, Virginia, US.[42,43] It is possible that Riley travelled that distance, but it is also likely that the malware planted those images.

In 2014, Marcel Datcu, a 36 year-old man from Romania, hanged himself and his four year-old son in his home after a piece of ransomware infected his computer.[44,45] A note left for his wife stated that a warning appeared on Datcu's computer demanding a payment of 70,000 lei. This incident shows that not enough of the general public are aware of ransomware and the fake messages apparently coming from authorities. It also shows how serious the effect of ransomware can be on people's lives.

Conclusions

This article has discussed the THD, the cases where it has been used, and related published material over the past decade, since its first use in 2003. By compiling an exhaustive list of cases, this work has shown that there are many occasions where serious miscarriages of justice have occurred. There have also been cases where clear and obvious mistakes have been made, either in the forensic investigation (or lack thereof) or from incorrect evidence given by incompetent experts.

As with many SODDI cases, the THD brings new challenges to the table, some that still need to be addressed by the forensic community. There should never be a worry that an innocent person has been put into jail or branded a criminal. Hopefully lessons would be learned from mistakes from the previous decade, so cases in the following decade will not see the same errors made.

Future work

Forensic techniques: It is possible that a criminal might successfully use the THD in their favour. To help combat this, forensic techniques need to improve and evolve. Not only this, but investigators need to know how they can investigate such a case. As a future work, a list of techniques and methods could be compiled, which can be followed by an investigator in a THD case. This work may help highlight additional steps, methods or techniques that could be used, that have not been considered before.

Court cases, match-and-learn, and data mining: Table 1 contains currently the most comprehensive list of THD cases; however, it is likely there are more that are currently not listed there. By researching cases, perhaps using data mining tools, it might be possible to not only add to that table but also create a set of match-and-learn profiles, which might predict the outcome of a THD case. As we have seen, this may not be easy, as often the defining and unpredictable factor in a THD case is the prosecution, jury or judge, rather than the evidence found.

About the authors

Stephen Bowles is a recent graduate of the University of Kent with a first class honours BSc. He is keen to progress in the computer security field, either in industry as a practitioner or in research to pursue a PhD.

Dr Julio Hernandez-Castro is a computer security lecturer at The School of Computing, University of Kent, UK. He was previously senior lecturer at Portsmouth and associate professor at Carlos III University in Madrid, Spain. His interests are cyber-security, cybercrime, steganography and steganalysis, malware and securing the Internet of Things.

References

1. SW Brenner; B Carrier; J Henninger. 'The Trojan Horse Defense in Cybercrime Cases'. 2004.
2. E George. 'UK Computer Misuse Act – the trojan virus defence: Regina v Aaron Caffrey, Southwark Crown Court, 17 October 2003'. Science Direct. Accessed Jan 2015. www.sciencedirect.com/science/article/pii/S1742287604000337.
3. D Haagman; B Ghavalas. 'Trojan defence: a forensic view'. 2005.
4. M Sepec. 'The trojan horse defence-a modern problem of digital evidence'. 2012.
5. S Bui; M Enyeart; J Luong. 'Issues in computer forensics'. 2003.
6. V Schmitt; J Jordaan. 'Establishing the validity of MD5 and SHA-1 hashing in digital forensic practice in light of recent research demonstrating cryptographic weaknesses in these'. 2013.
7. F Daryabar; A Dehghantanha; H Broujerdi. 'Investigation of malware defence and detection techniques'. 2012.
8. M Carney; M Rogers. 'The trojan made me do it: a first step in statistical based computer forensics event reconstruction'. 2004.
9. R Overill; J Silomon. 'A complexity based forensic analysis of the trojan horse defence'. 2011.

10. R Overill; J Silomon; K-P Chow; Y Law. 'Quantitative plausibility of the trojan horse defence against possession of child pornography'. 2011.
11. Personal communication from Richard E Overill, 29 Oct 2013.
12. D-Y Kao; S-J Wang; F Fu-Yuan Huang. 'Sote: strategy of triple-e on solving trojan defense in cybercrime cases'. 2010.
13. M Moffie; W Cheng; D Kaeli; Q Zhao. 'Hunting trojan horses'. 2006.
14. W Sun; R Sekar. 'Practical proactive integrity preservation: a basis for malware defense'. 2008.
15. R Di Pietro; F Lombardi; S Rossicone. 'Modelling mobile resource security'.
16. J Leyden. 'Caffrey acquittal a setback for cybercrime prosecutions'. The Register, 17 Oct 2003. Accessed Nov 2013. www.theregister.co.uk/2003/10/17/caffrey_acquittal_a_setback/.
17. Y Danidou; B Schafer. 'Trusted computing and the digital crime scene'. 2011.
18. 'The trojan made me do it'. About.com. Accessed Apr 2014. http://anti-virus.about.com/cs/allabout/a/caffrey.htm.
19. S Brenner. 'Trojan horse defense'. Cyb3rcrim3, 17 Jun 2006. Accessed Nov 2013. http://cyb3rcrim3.blogspot.co.uk/2006/06/trojan-horse-defense.html.
20. 'Computer virus blamed as man cleared of tax evasion and fraudulent returns'. Sophos, Aug 2003. Accessed Nov 2013. www.sophos.com/en-us/press-office/press-releases/2003/08/va_virustax.aspx.
21. D McCullagh. 'Police blotter: child porn blamed on computer virus'. CNET, 3 Nov 2006. Accessed Dec 2013. http://news.cnet.com/Police-blotter-Child-porn-blamed-on-computer-virus/2100-1030_3-6130218.html.
22. 'Former Atlanta teacher sentenced to 17 years prison following a child pornography conviction'. 2005.
23. US v O'Keefe. No.05-11924, Court of Appeals, 11th Circuit. 2006.
24. A Kantor. 'Case against Julie Amero needs to be deleted'. USA Today. Accessed Dec 2013. http://usatoday30.usatoday.com/tech/columnist/andrewkantor/2007-03-16-julie-amero-update_N.htm.
25. L Beyerstein. 'Questionable conviction of Connecticut teacher in pop-up porn case'. AlterNet, 18 Jan 2007. Accessed Dec 2013. www.alternet.org/story/46925/questionableconvictionofconnecticutteacherinpop-upporncase.
26. L Daniel. 'Julie Amero – wow, just wow'. ExForensis, 12 Sep 2008. Accessed Dec 2013. http://exforensis.blogspot.co.uk/2008/09/julie-amero-wow-just-wow.html.
27. 'Nationwide awareness of Julie Amero injustice grows'. MyLeftNutmeg, 14 Feb 2007. Accessed Dec 2013. www.myleftnutmeg.com/showDiary.do?diaryId=5793.
28. 'In child porn case, technology entraps the innocent'. Fox News, 16 Jan 2007. Accessed Nov 2013. www.foxnews.com/story/2007/01/16/in-child-porn-case-technology-entraps-innocent/.
29. 'Justice for Matt'. Accessed Nov 2013. Site now inactive. www.justiceformatt.com.
30. C Rutherford. 'Man had thousands of child porn images'. Daily Record, 17 Sep 2010. Accessed Dec 2013. www.dailyrecord.co.uk/news/local-news/man-thousands-child-porn-images-2422584.
31. 'Civil servant blames hackers for child pornography'. STV News. Accessed Dec 2013. http://news.stv.tv/scotland/196397-civil-servant-blames-hackers-for-child-pornography/.
32. 'Court dismisses pornographer's unique plea'. SPAMfighter, 18 Sep 2007. Accessed Nov 2013. www.spamfighter.com/News-9064-Court-Dismisses-Pornographers-Unique-Plea.htm.
33. 'Michael Fiola and the ticking time bomb'. Odd Time Signatures, 17 Jun 2008. Accessed Nov 2013. www.drumsnwhistles.com/2008/06/17/michael-fiola-and-the-ticking-time-bomb/.
34. 'Framed for child porn by a PC virus'. Fox News, 9 Nov 2009. Accessed Nov 2013. www.foxnews.com/story/2009/11/09/framed-for-child-porn-by-pc-virus/.
35. R Koman. 'A life destroyed: state employee acquitted of child porn charges'. ZDNet, 18 Jun 2008. Accessed Dec 2013. www.zdnet.com/blog/government/a-life-destroyed-state-employee-acquitted-of-child-porn-charges/3866.
36. 'Federal court dismisses child porn appeal'. Gillette News Record, 4 Dec 2013. Accessed Apr 2014. www.gillettenewsrecord.com/news/wyoming/article88a07072-5d11-11e3-9deb-001a4bcf6878.html.
37. T Morton. 'A case of Internet innocence?' Billings Gazette, 17 Apr 2010. Accessed Apr 2014. http://billingsgazette.com/news/state-and-regional/wyoming/a-case-of-Internet-innocence/articlea349b81c-4a9f-11df-815e-001cc4c03286.html.
38. T Morton. 'Casper man convicted of child porn makes final appeal'. Billings Gazette, 25 Oct 2011. Accessed Apr 2014. http://billingsgazette.com/news/state-and-regional/wyoming/casper-man-convicted-of-child-porn-makes-final-appeal/article\5fd72516-dd92-5174-8e32-f3bb3b1f12c9.html.
39. T Morton. 'US Supreme Court denies Solon child porn appeal'. Casper Star Tribune, 9 Oct 2010. Accessed Apr 2014. http://trib.com/news/local/u-s-supreme-court-denies-solon-child-porn-appeal/article 04fff8cf-146d-5f27-9d5a-27e6878090a6.html.
40. M Ward. 'Ransomware creation kit "sought by cyber-thieves"'. BBC, 11 Dec 2013. Accessed Dec 2013. www.bbc.co.uk/news/technology-25314442.
41. D Kaplan. 'Man falls for FBI "ransomware" attack, turns self into cops for possessing child porn'. SC Magazine, 25 Jul 2013. Accessed Dec 2013. www.scmagazine.com/man-

falls-for-fbi-ransomware-attack-turns-self-into-cops-for-possessing-child-porn/article/304600/.

42. C Farivar. 'Man gets ransomware porn pop-up, goes to cops, gets arrested on child porn charges'. Ars Technica, 27 Jul 2013. Accessed Feb 2014. http://arstechnica.com/tech-policy/2013/07/man-gets-ransom-ware-porn-pop-up-turns-self-in-on-child-porn-charges/.
43. W Peacock. 'Alleged pedo's computer gets locked by virus, turns himself in'. FindLaw, 29 Jul 2013. Accessed Feb 2014. http://blogs.findlaw.com/technologist/2013/07/alleged-pedos-computer-gets-locked-by-virus-turns-himself-in.html.
44 'Police ransomware threat of huge fine forced family to commit suicide'. Hacker News, 13 Mar 2014. Accessed Mar 2014. http://thehackernews.com/2014/03/police-ransomware-threat-of-huge-fine.html.
45. D Gilbert. 'Romanian man kills himself and four-year-old son because of malware on computer'. International Business Times, 13 Mar 2014. Accessed Mar 2014. www.ibtimes.co.uk/romanian-man-kills-himself-four-year-old-son-because-malware-computer-1440144.

Resources

- 'Brian Alan Bass registered sex offender'. Homefacts. Accessed 22-March 2014. www.homefacts.com/offender-detail/OKA540C480C3A6546C397294F3F7393C50/Brian-Alan-Bass.html.
- D Chaikin. 'Network investigations of cyber at-tacks: the limits of digital evidence'. 2007.
- 'Child porn pervert's court u-turn'. Croydon Guardian, 21 Sep 2006. Accessed Dec 2013. www.croydon-guardian.co.uk/news/931208.child-pornpervertscourtuturn/.
- 'Computer virus causing some to be framed for child porn'. Naples News.
- J Welham. 'Fatally flawed'. Operation Ore: The Gamble Connection, 21 Oct 2010. Accessed Mar 2014. http://operationorethegambleconnection.blogspot.co.uk/2010/10/fatally-flawed.html.
- N Trougakos. 'Federal jury convicts man of porn charges'. NewsOK, 11 Sep 2003. Accessed Nov 2013. http://newsok.com/federal-jury-convicts-man-of-porn-charges/article/1945437.
- M Braun. 'Federal jury finds enterprise man guilty in connection with child pornography'. The Southeast Sun Enterprise, 2 Aug 2007. Accessed Nov 2013. www.southeastsun.com/newscrime/article_312d8aa0-f935-5226-88fb-8442c0c22ca1.html.
- 'Former corrections officer sentenced to 46 months in federal prison for receipt of child pornography'. . Department of Justice, 7 Dec 2006. www.justice.gov/psc/docs/PR-Miller-12_7_06.pdf.
- 'Former Fresno county sheriffs sergeant sentenced to 14 years in prison for receiving and possessing child pornography'. Department of Justice, 17 Jul 2008. Accessed Dec 2013. www.justice.gov/opa/pr/2008/July/08-crm-624.html.
- 'Former Rochester resident pleads guilty to receipt of child pornography'. FBI, 2 Apr 2012. Accessed Dec 2013. www.fbi.gov/buffalo/press-releases/2012/former-rochester-resident-pleads-guilty-to-receipt-of-child-pornography.
- J Leyden. 'How malware frames the innocent for child abuse'. The Register, 9 Nov 2009. Accessed Dec 2013. www.theregister.co.uk/2009/11/09/malware_child_abuse_images_frame_up/.
- M Morris. 'Man gets 35 years in child porn case'. Computer Crime Research Centre, 21 Jul 2005. Accessed Mar 2014. www.crime-research.org/news/21.07.2005/1377/.
- FS Monterosso. 'Protecting the children: challenges that result in, and consequences resulting from, inconsistent prosecution of child pornography cases in a technical world'. 2010.
- Shiver v US. Civil Action No.1: 11cv179-MEF, Dist. Court, MD Alabama. 2013.
- 'Solicitors clerk claims virus put child pornography on his laptop'. Croydon Guardian, 14 Sep 2006. Accessed Nov 2013. www.croydonguardian.co.uk/news/918603.solicitorsclerk-claimsvirusputchildpornographyon-hislaptop/.
- R McMillan. 'Spyware case finally closed for teacher Julie Amero'. Computerworld, 21 Nov 2008. Accessed Dec 2013. www.computer-world.com/s/article/9121218/SpywarecasefinallyclosedforteacherJulieAmero?intsrc=newstshead.
- 'Susan Spencer insists husband pleaded guilty to child porn to save her from jail'. Croyden Advertiser, 10 Dec 2010. Accessed Nov 2013. www.croydonadvertiser.co.uk/Woman-insists-husband-pleaded-guilty-child-porn- charges-save-jail/story-11361338-detail/story.html.
- A Carvin. 'Teacher faces 40-year prison sentence because of filtering folly?' Learning.now, 16 Jan 2007. Accessed Dec 2013. www.pbs.org/teachers/learning.now/2007/01/teacherfaces40yearprisonse.html.

I Ibanga. 'Teacher: wrong computer click ruined my life'. ABC News, 27 Jan 2009. Accessed Nov 2013. http://abcnews.go.com/GMA/story?id=6739393.

- 'The detection of online child abuse in UK'. UK Essays. Accessed Mar 2014. www.ukessays.com/essays/criminology/the-detection-of-online-child-abuse-in-uk-criminology-essay.php.
- 'The trojan horse defence'. Computer Forensics. Accessed Oct 2013. www.computerforensics.ca/upload/1849trojanhorsedefence.pdf.
- 'Trojan horse defence results in child porn acquittal'. Out-Law, 25 Apr 2003. Accessed Nov 2013. www.out-law.com/page-3505.

- 'Trojan virus defense fails'. Cybercrim3, 31 Dec 2012. Accessed Nov 2013. http://cyb3rcrim3.blogspot.co.uk/2012/12/trojan-virus-defense-fails.html.
- United States v Shiver. No. 07-15425, Court of Appeals, 11th Circuit. 2008.
- US v Bass. No.04-6049, Court of Appeals, 10th Circuit. 2005.
- US v Brown. Case No.10-20233, Dist. Court, ED Michigan. 2012.
- US v McCourt. No.06-1018, Court of Appeals, 8th Circuit. 2006.
- US v Miller. No. 06-5187, Court of Appeals, 3rd Circuit. 2008.
- US v Miller. No. 08-4278. 2010.
- US v Plugh. Docket No. 07-2620-cr (L), Court of Appeals, 2nd Circuit. 2009.
- US v Vaughn. CR. No. F.05-00482 OWW, Dist. Court, ED California. 2008.
- T Broughton. 'Viruses blamed for pornography found on PC'. IOL News, 12 Sep 2006. Accessed Nov 2013. www.iol.co.za/news/south-africa/viruses-blamed-for-pornography-found-on-pc-1.293277.

The dangers in our trail of digital breadcrumbs


Tracey Stretton


Luke Aaron

Tracey Stretton and Luke Aaron, Kroll Ontrack

What do Apple, eBay, Snapchat, Target and LinkedIn have in common? All of you with accounts at any of the aforementioned companies should know the answer to the question, as you will have likely been asked to change your password in the recent past, or at least read about it in the news. With varying degrees of exposure (in some cases quite literally) the users of these services have all suffered some form of data breach in recent history.

In a single attack on the US retailing giant Target, the credit and debit card details of an estimated 40 million people were stolen and made available on the black market to cyber-criminals able to exploit stolen data for financial gain. You cannot hear these stories without wondering 'what information am I leaving online that people may access?'.

Need to communicate

The truth is we all leave a huge amount of personal data online. We worry about government surveillance and snooping yet 'trust' a corporate giant such as Facebook with personal information that is very sensitive – every private message you've written, every photo you've liked and every video you've watched. In fact, we go further – we tell them our relationship history, our thoughts, feelings, aspirations, worries and of course all of this information plus every disparaging message you may have written about your boss is logged, stored and made available to others for a price. The human need to communicate appears to trump concerns about privacy.

"We are giving away so much data on social media sites now that good old-fashioned data theft is perhaps no longer the major risk when it comes to data loss"

And as we can see from the above list, just because a company is big and conceivably has infinite resources available, certainly doesn't mean your data is safe with it. Until last year Instagram was able to share your private information with Facebook and Facebook was able to sell information to advertisers without seeking your permission or offering compensation. That has apparently not differed following changes to Instagram's privacy policy.

Of course, we haven't even mentioned yet the risks attached to social media accounts that you no longer access (hand's up – who doesn't even know if they still have a MySpace or Bebo account and wouldn't know how to login to it if they did?) And there are new chat tools, location-based dating apps and apps like Whisper that allow you to send messages anonymously, to contend with as well. According to news reports, Whisper was recently accused of tracking the approximate location of some of its users who opted out of geolocation services even though its privacy policy stated that access to location-based information was "purely voluntary".

The bottom line is that we are giving away so much data on social media sites now that good old-fashioned data theft is perhaps no longer the major risk when it comes to data loss.