ARTICLE:

THE TROJAN HORSE DEFENCE – A MODERN PROBLEM OF DIGITAL EVIDENCE

By **Miha Šepec**

The Trojan horse defence is an important aspect of the investigation of crimes involving digital evidence. In raising this defence, the accused claims that they are not responsible for some or all of the digital evidence that forms the offence, but by someone else who has abused their computer system with a Trojan horse or other malicious code. The prosecution must refute such claims with certainty, otherwise the court (or the jury) will have to find the defendant innocent of the crime.

To avoid the Trojan horse defence, law enforcement agents will also, in addition to presenting digital evidence (which must not only prove the existence of a crime, but also the absence of malicious codes and other offenders who could be involved in the offence), use traditional forms of evidence, such as physical evidence, witnesses, motive, and the computer knowledge of the accused. The stronger the connection between digital and other forms of evidence, the lower the probability of using a Trojan horse defence as a diversion with the intent to confuse the court and the jury.

The article presents theoretical and practical dilemmas of a Trojan horse defence, offering some solutions for law enforcement agents when dealing with such a defence within the context of Slovenian criminal law.

Introduction

Using the Trojan horse defence, the defendant admits that the crime was committed through his computer system, but denies that he was the perpetrator of the offence. He asserts that somebody else must have committed the crime using malicious software, or placed it in his computer system. The prosecutor must prove that the crime was not committed by malicious software or some other perpetrator using this software, which can be difficult. The purpose of this defence is often to create doubt in the minds of the jury and the judge. The defence will be hard to refute and will often suffice for an acquittal on the basis of reasonable doubt.

At first glance it is obvious that this is an extremely difficult issue that requires the cooperation of various experts – criminal lawyers that know the legal system, but are restricted in terms of technical know-how; and digital evidence specialists, who have technical and expert knowledge, but often lack knowledge of the legal system. The development of technology has brought us thus far, as a participant at the conference entitled *Current Issues in IT Security in Freiburg 2009* noted: 'At a conference on IT security in one of the largest criminal justice and criminological research institutes in the world, none of the participants dares to argue that he is an "IT security expert"!'[1]

It is necessary to adopt a multidisciplinary approach when dealing with a Trojan horse defence. Such an approach will include classical methods of law enforcement (interrogation, observation, searching for motive, testimony and other physical evidence), as well as new forms of digital evidence (the existence of a Trojan horse on the defendant's system, the possibility of infection of the information system, the probability that another person committed the offence through a

1 *Aleš Završnik, 'Report on the conference "Current Issues in IT Security", Freiburg 2009', Journal of Criminalistics and Criminology Studies, Volume 60, issue 2, 2009, 181-184, at 181; web site of the journal: http://www.mnz.gov.si/si/medijsko_sredisce/revija_za_kriminalistiko_in_kriminologijo/; web site of the conference: http://www.mpicc.de/ww/en/prs/aktuelles/veranstaltungen/security09.htm.*

malicious code).

This article presents the characteristics of the Trojan horse defence, problems of proof and how this defence tactic can be avoided in practice.

The definition of a Trojan horse defence

It should be noted that the term 'Trojan horse defence' is not an established legal term, but comes from a number of digital evidence specialists that wrote texts on the topic some time ago. The Trojan horse defence is the classic defence of passing the blame on a third person – 'The Wrong Person Defence' or 'SODDI defence' (some other dude did it).

In this defence, the defendant must offer at least some evidence that there is a possibility that a third party was liable for the commission of the criminal act. However, as Griffin writes, in many states of America this can be prohibited unless the defence establishes a direct and convincing connection with a third party and the crime that has been committed. Such evidence may be excluded if the only objective is to mislead the jury.[2]

The defendant invariably cannot establish a connection with the third party when claiming a Trojan horse defence. It is only possible to establish the probability of a third party using malicious codes (as Trojan horses) through his computer system: 'Ironically the anonymity of the threat, which is usually fatal to the assertion of a SODDI defence in a prosecution for real-world crimes, works to the defense's advantage.'[3]

There are no special rules of evidence in Slovenian law.[4] The defendant can argue any kind of defence he wishes, without limitation. In the Slovenian criminal system, the burden of proof is always on the prosecution. The prosecution must prove that the crime was not committed by a third party manipulating the defendant's computer system through malicious code. A variety of malicious codes in a computer system may be responsible for a legitimate Trojan horse defence. The most common forms of malicious code are Trojan horses and bots. These are discussed in brief below.

Trojan horses

Trojan horses, as the name suggests, are seemingly innocent programs that contain hidden features (for example, by allowing the hacker to obtain access to the computer system). They act like viruses, thus requiring some preliminary activity by the recipient in the form of execution of files or by visiting a web site, which contains a Trojan horse.[5] Trojan horses belong to a group of programs commonly called 'malware' by the technical community, which are defined as a set of instructions to execute a process in a foreign computer system as instructed by the attacker. These programs are often unwanted, harmful and hidden.[6]

The success of the Trojan horse will partly depend on the level of protection in the computer system. The characteristic of a Trojan horse is that the software often has an apparently innocent function, such as showing the time and weather on the desktop, but in the background the program has a secondary function – this is called the 'Back Door'. This allows the writer of the Trojan horse software to execute certain functions, such as to gain access to the computer system, to obtain files from this system, or install other malware on the system.[7]

A Trojan horse generally does not spread and does not degrade the performance of the computer system into which it is placed. In their simplest form, a Trojan horse requires a degree of naïveté from the user, who executes an unknown file. However, modern and more sophisticated forms of Trojan horses are becoming more difficult to identify and locate, as Bilar notes: 'anti-virus software does not prevent all forms of malicious software from penetrating computers and networks – some malicious software will not be identified by anti-virus software'.[8]

The efficiency of the Trojan horse is evident by the fact that Germany is using them for on-line investigations (die Online-Durchsuchung), which is a form of covert telecommunication surveillance (Die Quelle-Telekom munikationsüberwachung).[9] The use of Trojan horse software programs, called 'der Bundestrojaner', and other programs for this purpose was limited by the German

2 *Lissa Griffin. 'Avoiding Wrongful Convictions: Re-examining the "Wrong-Person" Defense' 39 Seton Hall L. Rev. 129 (2009).*

3 *Susan W. Brenner and Brian Carrier, with Jef Henninger, 'The trojan horse defense in cybercrime cases', 21 Santa Clara Computer & High Tech. L.J. 1 (2004), p 17.*

4 *Ana Burgar and Klara Miletič, 'Slovenia' in Stephen Mason, gen. ed., International Electronic Evidence (British Institute of International and Comparative Law, 2008).*

5 *Jonathan Clough, Principles of cybercrime, (2010, Cambridge University Press).*

6 *Samuel C. McQuade III, ed, Encyclopedia of Cybercrime (2008, Greenwood Publishing).*

7 *Neil Barrett, Digital Crime: Policing the Cybernation (1997, Kogan Page).*

8 *Daniel Bilar, 'Known knowns, known unknowns and unknown unknowns: anti-virus issues, malicious software and internet attacks for non-technical audiences', Digital Evidence and Electronic Signature Law Review, 6 (2009), 123-131, at 124.*

9 *Holger Hesterberg, Das neue "Computergrundrecht" und die "Bundestrojaner", Anwalt.de, 17.10.2011, available at http://www.anwalt.de/rechtstipps/das-neue-computergrundrecht-und-die-bundestrojaner_021554.html.*

Constitutional Court decisions 1 BvR 370/07 and 1 BvR 595/07 on 27 February 2007.[10]

Bots

A bot is a program that infects a computer system and enables a third party to control the infected computer or computer system. An attacker can exploit a security flaw of a computer connected to the internet, and install on it a large number of small programs (called Demons). Infected computers are called zombies, and can be controlled remotely.[11] One of the features of a bot is that the software does not directly interfere with the system on which it is running – the user is not usually aware that his system is infected.[12] Only when the operator activates the bots, can the functions of the system be compromised. When the attack ends, or the third party deactivates the bots, the infected system runs smoothly again. The efficiency of bots depend on the level of protection in the computer system. For instance, firewalls are a typical form of defense against bots and other malicious code.

The Trojan horse defence in general

The first known instance of the Trojan horse defence in England and Wales was the case of Charles Schofield. Schofield was cleared of charges of possessing abusive images of children.[13] Julian Green was charged with possession of abusive images of children, and also argued the Trojan horse defence. After examining his computer, the forensic team found many malicious codes (including Trojan horses). Green argued that these codes were responsible for the images. The digital evidence specialists for the prosecution were not able to refute his claims.[14]

The first example of the Trojan horse defence that was successful and received a great deal of publicity occurred in October 2003 in England and Wales. The members of the jury acquitted Aaron Caffrey. Caffrey was accused of a Distributed Denial of Service (DDoS) attack on the port of Houston. The attack had caused enormous damage, because port network connections were not available, and therefore not able to provide information to ships masters, mooring companies and support companies responsible for the support of ships sailing and leaving the port.[15]

The attack was executed through Caffrey's computer system. A forensics team found the programs used for the attack, but no traces of a Trojan horse. The defence argued that Caffrey was a member of a hacker group, but that he did not execute the attack. Instead, members of his team must have breached his system and executed a DDoS attack on the port through his computer. The defence also argued that it must have been a special type of a Trojan horse, which erased all traces after it was used, so that it could not be detected in his system.[16] Professor Neil Barrett explained to the court that it was impossible for anyone to have edited the recorded log files on Caffrey's computer,[17] and that if a Trojan horse really was the source of the attack, than at least some traces should have been found. This explanation failed to convince the jury. Kotadia[18] wondered if the decision would have been the same if the members of the jury had consisted of technology experts, or at least computer-conscious people.

An important difference between the Schofield and Green cases and the Caffrey case, is that the forensic team in the first two cases found traces of Trojans and other malware in the computer system which could have been responsible for the claims made by the defendants. However, in the Caffrey case, there were no traces of any malware.

An analysis of the Trojan horse defence

Consider the analogy with murder. Invariably, a forensics team will probably find traces of DNA of the defendant and other people, any of whom could have committed the murder. If there is no other compelling evidence against the accused, their innocence must be presumed as long as the possibility that another unknown person was responsible for the act. If there is no trace of any other presence, besides that of the defendant, then a defence

10 *German Constitutional Court (Das Bundesverfassungsgericht) decisions 1 BvR 370/07 1 and 1 BvR 595/07, available at: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.*

11 *Jonathan Clough, Principles of cybercrime.*

12 *Samuel C. McQuade III, ed, Encyclopedia of Cybercrime.*

13 *John Leyden, 'Trojan defence clears man on child porn charges', The Register, 24 April 2003, available at http://www.theregister.co.uk/2003/04/24/trojan_defence_clears_man/.*

14 *'Man cleared over porn "may sue"', BBC News, 31 July 2003, available at http://news.bbc.co.uk/1/hi/england/devon/3114815.stm.*

15 *Jelena Mirković and Peter L. Reiher, 'A Taxonomy of DDoS Attack and DDoS Defense Mechanisms', ACM SIGCOMM Computer Communication Review, Volume 34, Number 2, 2004, pp. 39-53, available on-line at http://www.eecis.udel.edu/~sunshine/publications/ccr.pdf.*

16 *Susan W. Brenner and Brian Carrier, with Jef Henninger, 'The trojan horse defense in cybercrime cases'; see also an on-line note by Susan Brenner, 'Trojan Horse Defence CYB3RCRIM3, Observations on technology, law and lawlessness', 17 June 2006, available at http://cyb3rcrim3.blogspot.com/2006/06/trojan-horse-defense.html.*

17 *This is not correct. Root kits can do this.*

18 *Munir Kotadia, 'The case of the Trojan Wookie', ZDNet UK, 21 October 2003, available at http://www.zdnet.co.uk/news/it-strategy/2003/10/21/the-case-of-the-trojan-wookiee-39117240/; for further references, see Stephen Mason, gen. ed., Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010), 10.199-10.200.*

that some other person must have committed the crime and then wiped all traces of DNA after the murder will often not be successful. It follows that the prosecution will have to provide other evidence, such as whether the accused was able to inflict death, and whether he had a motive.

Similarly in cyber crime cases, digital evidence alone will often not suffice. A multidisciplinary approach will usually be required. In addition to digital evidence, the prosecution will have to provide other forms of evidence (physical evidence, evidence of motive, witnesses). Traditional forms of evidence will also act to increase the weight of any digital evidence.[19] It is important to be careful not to blindly believe all the digital evidence, since the possibility of forged digital evidence is always possible.[20]

Daniel Bilar explains how antivirus programs work, and points out that a lot of malicious codes are not recognized by antivirus software that is not updated regularly. Between 26 and 31 per cent of malicious software is not detected on antivirus programs that are not up-dated for a week (this percentage is only valid for better antivirus programs – poor quality antivirus programs can miss up to 80 per cent of malicious codes). It is clear that it is reasonably probable, and not only a hypothetical exception, that a computer can be infected with a Trojan horse. It is important to be aware that although people might have a basic understanding of technology (for instance, the majority will not necessarily open strange files received by e-mail), very few are aware of the fact that they can download various forms of malicious code (such as Trojan horses) simply by launching an URL site, opening a PDF document or browsing internet pages. Up-dated antivirus software, firewalls, and caution on the internet help reduce the risk, but cannot completely eliminate it.[21]

When we speak of 'defence' it is appropriate that we briefly explain what this means in criminal proceedings. The definition of an offence is based on an objective part (the act), and the subjective part (the mental element). When a person is charged with committing a statutory crime (the act) and being required to be responsible for the act (the mental element), he may respond by giving an explanation (a defence) with which he can negate accusations of the prosecution and prove his innocence: the 'defence operates as an excuse. The culpability of the accused is negated and he is excused from the normal consequences of conviction and sentencing which would flow from commission of the prohibited act with the requisite mens rea.'[22]

Modern English and American criminal law doctrine distinguishes between 'justification' and an 'excuse', as noted by Professor Ormerod: 'An act is justified when society positively approves of it. It is merely excused when society disapproves of it but thinks it is not right to punish the defendant.'[23] The problem of this distinction is that 'there is no agreement on the precise model that the classifications should take.'[24] In this regard, the Trojan horse defence not only negates the mental element, but also the act – the defendant's case is not only he did not commit the act, he and did not even know about the crime being committed, as noted by Allen: 'A plea of justification operates to cancel the unlawfulness of the accused's conduct; there being no unlawful act, there is thus no crime of which to convict him.'[25]

The Slovenian criminal law differs from common law. A defence in Slovenian criminal law may be defined as any act of the defendant which intends to prove his innocence or disprove the allegations against him by the prosecution. 'Defensive tactics' is a broader term that includes both the strategy of the defendant, as with the procedural acts that follow this strategy (defence with insanity; procedural acts: a proposal for an expert opinion – such as a psychiatrist; presenting evidence on the use of certain substances that could lead to insanity).

It is obvious that a Trojan horse defence will often be misused in offences connected with computer systems. Any forensic examination of a computer system that finds a Trojan horse or other malicious code will present an opportunity for the defence to plea a potential Trojan horse defence, and with it the doubting of all the digital evidence. The latter often only proves that a crime was committed – but not with certainty by whom. However, it does not follow that because Trojan horse software or other forms of malicious software are found on a computer, that such evidence is relevant to the case. It

19 *For a more detailed anaylsis and discussion on this precise points, see Stephen Mason and Professor Burkhard Schafer, Chapter 2, The characteristics of digital evidence, in Stephen Mason, gen. ed., Electronic Evidence.*

20 *Sergey Bratus, Ashlyn Lembree and Anna Shubiana, ' Software on the Witness Stand: What Should It Take for Us to Trust It?' Lecture Notes in Computer Science, Volume 6101 (Springer, 2010), pp 396-416, paper available on-line at http://www.cs.dartmouth.edu/~sergey/; see the examples of the forgery of digital evidence in Stephen Mason, gen. ed., Electronic Evidence.*

21 *Daniel Bilar, ' Known knowns, known unknowns and unknown unknowns: anti-virus issues, malicious software and internet attacks for non-technical audiences' .*

22 *Michael Allen, Textbook on Criminal Law, (11th edn, Oxford University Press), p 169.*

23 *David Ormerod, Smith and Hogan Criminal Law, (13th edn, 2011, Oxford University Press), p 248.*

24 *David Ormerod, Smith and Hogan Criminal Law, p. 248.2*

25 *Michael Allen, Textbook on Criminal Law, p 169.*

might be that the malicious software is responsible for the computer undertaking certain activities that the owner or user is not aware, but it is possible that some or all of the items of malicious software found might not have any effect on the nature of the offence, because the software found does not undertake the activities that the defence claim, as in the case of the US case of *State of Connecticut v Julie Amero*.[26]

An extensive Australian study on cyber crime reported[27] that the number of detected attacks by Trojans is stagnating or even increasing. In 2006, of those organizations questioned, 21 per cent detected infection with Trojans, while 45 per cent detected infection with worms or worm infection (reports were prepared for each year between 2003 and 2006, which allows for comparisons to be made). On page 22, the authors remind us that:

> Testing of malware developed for the purposes of stealing personal information and account credentials has revealed that, on average, 60% are not detectable by anti-virus software at the time they are discovered in the wild. Therefore, client computers with the most "up to date" anti-virus software signatures are likely to be vulnerable to such attacks about 60% of the time. The relatively high level of trojan infections reported in this survey is, therefore, likely to be a function of this weakness. Attackers work to increase the effectiveness of their attacks by modifying trojan malware to create new variants that are unlikely to be detected by most "up to date" anti-virus software upon release.

The investigation and the Trojan horse defence

Before discussing the matter from a prosecutor's point of view, it is right to acknowledge that a Trojan horse defence can be a completely legitimate and justified defence of an innocent defendant, as Rasch noted in 2004:

> 'It is relatively easy to manufacture and plant electronic evidence consistent with guilt. In fact, with a few skills and tools, not only could you plant such evidence, but you could do so in such a way as to be virtually undetected, and so that it would be virtually impossible to determine that your target was not guilty.'[28]

When law enforcement agencies are informed about a computer-related crime, of necessity they trace the crime to a specific computer system or systems. After seizing it, digital evidence specialists perform a systematic examination of the computer system. In addition, they should explore the possibility of a Trojan horse, bot or other malware that can be responsible for the offence. In Slovenia, according to Kragelj,[29] a forensic examiner will ideally use a number of antivirus programs to recognize possible infections.[30] However, if a digital evidence specialist only relies only on a single program for the purposes of a forensic analysis of the hard drive, (and this program does not recognize the Trojan horse in the system), and testifies that no Trojan horse or other malicious software was found, it is possible that the jury will deliver a guilty verdict to an innocent man, depending on the quality of the defence lawyer. In Slovenia, some investigators usually use only one antivirus program in a system check for malicious codes,[31] which could present a serious problem regarding reasonable doubt that the program found all the possible malicious codes. It is always necessary to bear in mind the statement made by Šavnik, a Slovenian court digital evidence specialist, that 'Nothing in cyberspace is ever 100 per cent certain. There is always room for doubt.'[32]

There are a number of issues that any investigation into a crime involving digital data that should be considered to ensure fairness to the accused:

1. Educating digital evidence specialists, and requiring them as a matter of best practice to use several investigative programs and their integration.[33] Thus Leuhr points that:

> 'lawyers should always inquire about the depth

26 For an exhaustive analysis of this case, see Stephen Mason, gen. ed., International Electronic Evidence, xxxvi-lxxv.

27 AusCert, Computer Crime and Security Survey (2006), available at http://www.auscert.org.au/render.html?it=2001.

28 Mark Rasch, ' The Giant Wooden Horse Did It!' comments on Securityfocus.com, 19 January 2004, at http://www.securityfocus.com/columnists/208.

29 Interview with Primož Kragelj, a Forensics IT specialist in Slovenia, on 28 March 2012.

30 It is not proposed to set out the practical methodology used to seize, examine and retain digital data, because such issues are covered extensively in the technical forensic and legal literature, some examples include: Eoghan Casey, Digital Evidence and Computer Crime (3rd edn, Academic Press, 2011) and Stephen Mason, ed, Electronic Evidence, amongst others (both texts provide a large number of further references).

31 Interview with Primož Kragelj, a Forensics IT specialist in Slovenia, on 28 March 2012.

32 Janko Šavnik, Role of a Forensic Examiner for Computer Forensics, Digital Evidence Conference, (Law Faculty and Faculty of Criminal Justice and Security of University of Maribor, 2012).

> and breadth of a potential expert's background. Lawyers should avoid the one-trick examiner who has only imaged and analyzed one type of computer using a single forensic tool. Rather, an attorney should look for a forensic examiner who has analyzed a number of different machines or systems, in a number of different settings, in a wide variety of legal cases.'[34]

The investigation of digital traces and evidence is certainly a modern challenge for digital evidence specialists, who must constantly upgrade their knowledge. Of necessity, a forensic examiner must adapt to the rapid development of information technology; use up-to-date technical equipment and information (which may be a major problem in poor countries, or if their country does not provide them with the appropriate hardware and software), and not to rely only on a single investigation program and outdated approach to studying computer systems.

2. Digital evidence is not the only evidence that must be considered when examining cyber crime offences (especially if consideration is given to the possibility of forged digital evidence).[35]

Law enforcement agencies often rely on 'classical' evidence, such as motive, physical evidence (in the form of media or paper records) and testimony of potential witnesses. Corroborative evidence is helpful, such as photographs (as physical evidence) of children taken in front of a kindergarten or elementary school by the accused may serve as indirect evidence of his intentions. Through such evidence, the judge and the jury might reasonably conclude that the abusive images of children on the computer were really obtained and possessed by the accused, and that they were not planted there by some malicious code. A similar proof might be a testimony of a person who was asked by the defendant where he can get child pornography, as well as a testimony of a digital evidence specialist who was questioned by the defendant about how he might be able to conceal his identity and hide certain files in his computer – a later forensic examination might show that files were hidden in the computer in the way that was described to the defendant.

Evidence in non-digital form will be an important addition to digital evidence. Traditional evidence in combination with digital evidence will help the court to decide about the guilt of the accused. In a famous case of the botnet Mariposa,[36] the alleged mastermind and creator of the bot, Dejan Janžekovič, was found in Maribor in Slovenia in 2011 (the case was also under the investigation by the FBI). The Trojan horse defence was introduced at a very early stage of the investigation. The criminal investigators, who obtained evidence that the suspect had sold copies of the bot kit for few hundred dollars for each copy, refuted it. Such 'classical' evidence helps to negate any sort of electronic or digital oriented defences.

3. The testimonies of medical and psychological experts on the mental state of the accused are also relevant. Such evidence might indicate that the suspect is unlikely to be the perpetrator (for example, an examination of the computer shows that abusive images of children are hidden with a very complex encryption method, but it is clear that the suspect is a computer illiterate and could not have hidden the files in such a manner).

4. Consideration might be given to the fact that the accused can plant Trojan horses on his computer system in order to later use this as a defence tactic. In such an example, the prosecution may need to point out the defendant's computer knowledge and skill. If he is deemed to be a computer expert, the prosecution can argue that it is very probable that he planted such a malicious code and that he had the skills to do it. Furthermore, the prosecution can argue that it is extremely unlikely that the defendant (who is a computer expert) would infect his computer with an extremely primitive Trojan horse hidden in a suspicious file, which was received with an unknown e-mail. If the accused is computer illiterate, then such arguments might be favourable to the defence.

33 In the case of State of Arizona v Bandy, the defence case was that malicious software was responsible for the action of uploading abusive images of children to the internet. At the request of the defence, the investigators looked at the hard disk three times. Each time, they found more incriminating material. For an analysis of this case, see Stephen Mason, gen. ed., International Electronic Evidence, lxxv-lxxxiii

34 Paul H. Leuhr, ' Real Evidence, Virtual Crimes' Criminal Justice, Volume 20, number 3 (Fall 2005), 14-23, at 18.

35 Sergey Bratus, Lembree Ashlyn and Anna Shubiana, ' Software on the Witness Stand: What Should It Take for Us to Trust It?', available at http://www.cs.dartmouth.edu/~sergey/trusting-e-evidence.pdf.

36 ' John Layden, ' How FBI, Police busted massive botnet' The Register, 3 March 2010, The Mariposa botnet was principally geared towards stealing online login credentials for banks, email services and the like from compromised Windows PCs. The malware infected an estimated 12.7 million computers in more than 190 countries' ; John Leyden, ' Maripose botnet suspects quizzed in Slovenia' The Register, 22 July 2010; FBI, Slovenian and Spanish Police Arrest Mariposa Botnet Creator, Operators (FBI National Press Office, 28 July 2010), available at http://www.fbi.gov/news/pressrel/press-releases/fbi-slovenian-and-spanish-police-arrest-mariposa-botnet-creator-operators.

If the accused wanted to erase any trace of a Trojan horse or other malicious code, it would be necessary to use a specific program, a ' wiping tool' , which could erase the traces of a malicious code on a system

However, one of the problems is how to assess the level of the computer expertise of the accused, because such specific knowledge is often not taught in universities and other schools, rather it is often self-taught and obtained through the social connections of the accused. The prosecutor will have to use indirect evidence, indications and signs, because there is no direct technical option of proving one's computer knowledge without the cooperation of the accused. The computer system of the accused will have to be examined for possible leads, such as the kind of programs he uses; whether he uses programming language; examine his internet history, and look for any statements on internet forums and chat rooms (if attainable).

In the opinion of Kovačič,[37] the mere possession of 'hacking programs' is not enough to assess the computer knowledge and skills of the accused. There are legal hacking tools that are used for penetration testing (such as Backtrack programs, for instance), and on the other hand, intrusion can also be made through a regular web browser (such as SQL injection). A good indication would be if the accused developed some kind of a hacking tool or a virus, or if traces of such tools are found. As already pointed out, law enforcement agents should always combine digital evidence with traditional evidence. The police should therefore question the 'social connections' of the accused (his friends, on-line colleagues, persons he is communicating with on a 'hacker' oriented forum) and by doing so, gain some insight on his computer knowledge.

In the Caffrey case, the defence pleaded that a technologically advanced Trojan horse erased all traces from the defendant's computer after it carried out the activities. While computer expert Neil Barrett testified that this is practically impossible, it is highly questionable whether the same could be argued in 2012.

Brenner, Carrier and Henninger write, on page 19, that 'police have found traces of Trojan horses in many cases we have seen so far.' If the accused wanted to erase any trace of a Trojan horse or other malicious code, it would be necessary to use a specific program, a 'wiping tool', which could erase the traces of a malicious code on a system. However, traces of wiping tools remain on the system. The cleaning program cannot clean itself. Thus, it is practically impossible that there would be no digital traces of malware or at least the use of wiping tools on a computer system.[38] However, the new format of hard drives called Solid-State Drives (SSD) with a TRIM[39] function enabled, can erase all the files that were deleted from the drive completely in three minutes. The advanced recovery programs that digital evidence specialists use cannot recover such files. Special write blockers used by digital evidence specialists cannot prevent complete erasure of the files.[40] The new formats of SSD hard drives (with enabled TRIM function) can present a real problem when a Trojan horse defence is used and when the defence argues that the Trojan horse was deleted by a third person. Since SSD hard drives automatically erase all deleted files, forensic examiners will not be able to disprove the claims of the defence.

Leuhr also recommends a comprehensive forensic examination of the registry and startup files system, where the examiner can find traces of malware that is activated at each startup of the system.[41] Brenner and colleagues advise a thorough examination of the network connections of the computer system.[42] If a computer system was not connected to the network, then this would conceivably exclude the possibility of a malicious code

37 *Interview with Matej Kovačič PhD, an IT specialist with the Commission for the prevention of corruption, in Slovenia on 24 May 2012.*

38 *Susan W. Brenner and Brian Carrier, with Jef Henninger, ' The trojan horse defense in cybercrime cases' , pp 26 and 27.*

39 *A TRIM command enables an operating system to communicate with a solid state drive to inform it which blocks off data can be deleted or wiped.*

40 *Matej. Kovačič, Hash algorithms and integrity ensurance of digital evidence, Digital Evidence Conference, (Law Faculty and Faculty of Criminal Justice and Security of University of Maribor, 2012).*

41 *Paul H. Leuhr, ' Real Evidence, Virtual Crimes' , 15.*

42 *Susan W. Brenner and Brian Carrier, with Jef Henninger, ' The trojan horse defense in cybercrime cases' , p 47.*

or some other offender committing the crime through the computer system of the defendant.

If the investigator finds malicious software on the system, he must examine its performance and how it might affect the system. The investigator must also determine when these codes were installed on the system and if they ever really ran on it. If the investigator does not find any malicious software on the system, he must consider the possibility that these were wiped with wiping tools – he must therefore look for traces of these programs (this will be problematic on SSD hard drives with enabled TRIM function).

The investigator will also have difficulties in examining the computer system for malicious software in a case on an encrypted hard disk, where the computer is protected by a BIOS password, and the accused refuses to cooperate. There are basically two types of 'BIOS protection'. One is that the BIOS password on the motherboard only prevents the computer from booting up. This protection is relatively easy to circumvent by disconnecting the battery from the motherboard and then to try and change the password with the factory set master password, or the hard drive can be connected to another computer. The second possibility is that the accused has prevented access to the hard drive with a special password in the system BIOS (this is possible with a special ATA command block or low-level hard disk encryption). The investigator can try to circumvent this protection by entering the factory-set master password, if this option exists. Lists of factory default passwords are found on the internet or with the manufacturer, however not all the manufacturers have included such passwords in their hardware.[43]

Kovačič points out that BIOS protection is rarely used in practice, since it is relatively easy to circumvent. Instead, software encryption of the hard drive (with a program such as TrueCrypt) is often used. This protection can be broken by cryptanalysis (a theoretical possibility that is almost never used in practice), or by installing special equipment into the computer, such as a hardware interceptor (key logger) to record the password as it is typed into the computer, or the software version of these interceptors. The computer system has to be returned to the owner and then seized again when he has inputted the password. The final option is that the computer is seized in the moment the accused is using it (at that time the hard drive is not encrypted). However, all these solutions are quite impractical and can be sabotaged. For instance, the suspect can scan the computer and remove the key logger software, or he can use software that locks down the hard drive remotely via Bluetooth, when the computer is moved or when the network connection is interrupted.[44]

The interrogation of the suspect is also of great importance in all crimes where digital evidence is present, and when there is a potential Trojan horse defence in play. Since cyber crime perpetrators often have no experience with law enforcement, a confession will be often easier to get, as indicated by Brenner and colleagues: 'These suspects often confess readily and may even confess before being interrogated. This is especially true of child pornography collectors, most of whom have no prior contact with law enforcement. Their inexperience with the criminal justice system, coupled with the embarrassing nature of the crime, often prompts them to confess.'[45]

Undercover investigative measures are not to be underestimated. Article 150 of the Slovenian Criminal Procedural Act[46] contains the following covert investigative measure: 'Surveillance of electronic communications with eavesdropping and recording, and control and preservation of evidence in all forms of communication'.[47] Combined with covert measures of surveillance, this can be a powerful help in the hands of the prosecution. However, the Slovenian Criminal Procedural Act stipulates that surveillance can only be undertaken when it is reasonable to expect that the police will not be able to detect, prevent, or prove the criminal offence with any other measure, or if this would present disproportionate difficulties.[48] Law enforcement agencies do not use undercover investigative measures only to rebut a possible defence tactic. Undercover investigative measures are used for the purpose of identifying the possible perpetrator of a criminal offence or to provide evidence for the prosecution – and not for the purpose of countering a possible defence that a defendant might or

43 Interview with Matej Kovačič PhD, an IT specialist with the Commission for the prevention of corruption, in Slovenia on 24 May 2012.

44 For relevant case law on encryption in England & Wales and the United States of America, see Stephen Mason, Electronic Evidence.

45 Susan W. Brenner and Brian Carrier, with Jef Henninger, ' The trojan horse defense in cybercrime cases' , p 27.

46 Slovenian Criminal Procedural Act (ZKP-UPB4) Ur. l. RS n. 32/2007, amended by ZKP-I, ur. l. RS n. 68/2008, ZKP-J, ur. l. RS n. 77/2009 and ZKP-K, ur. l. RS n. 91/2011.

47 In the Slovenian language ' Nadzor elektronskih komunikacij s prisluškovanjem in snemanjem ter kontrola in zavarovanje dokazov o vseh oblikah komuniciranja, ki se prenašajo v elektronskem komunikacijskem omrežju.'

48 Ana Burgar and Klara Miletič, ' Slovenia' in Stephen Mason, gen. ed., International Electronic Evidence, 827-829.

might not use in trial. Given the fact that the defendant will use the Trojan horse defence only when faced with accusations, it must be concluded that in Slovenia, undercover investigative measures will not be used only with the aim of countering a Trojan horse defence (but could of course be used simply to gather evidence about the crime and the possible perpetrator).

Concluding comments

The dilemmas presented in this article clearly show the complexity of malicious codes and the potential for a Trojan horse defence. However, digital evidence specialists are restricted by the government and institutions in which they work, both in the education they are provided and with the technical resources (hardware, software) which are available to them. Technological expertise can be a significant problem especially in poor countries. In Slovenia, the technical and software equipment is adequate. However, lack of funding presents a problem.[49]

The Trojan horse defence can be used in two roles: to exonerate an innocent defendant or suspect, and as a last resort of a real perpetrator, against whom all the evidence points to his guilt. In such cases, the Trojan horse defence becomes a tactic whose purpose is to provide for confusion and uncertainty in the minds of the jury and the judge. Which version of the defence is used will often be difficult to detect. The burden of proof is, of course, on the prosecution, and in reality it is on the examination of the digital evidence.

When dealing with a Trojan horse defence the following course of action should be undertaken in the investigation. Digital evidence specialists should perform a systematic examination of the computer system for malicious software, using more than one investigation tool (new SSD hard drives and software encryption of the hard drive could pose a problem). It is preferable than more investigators examine the system and compare the results. A multidisciplinary approach should always be considered. It is important that the prosecution connects digital evidence with corroborative evidence, such as witnesses, evidence of motive, physical evidence such as photographs, undercover investigative measures and interrogation of the accused. By combining classical evidence with digital evidence, the prosecution will reduce the probability of the presence of a malicious code.

Miha Šepec is a graduate of Ljubljana Law University, presently a criminal law assistant at the Faculty of Criminal Justice and Security, University of Maribor and European Law Faculty, University of Nova Gorica, and a PhD (Development, trends and problems of cybercrime offences) candidate at the Law Faculty, University of Maribor.

miha.sepec@fvv.uni-mb.si

49 Interview with Primož Kragelj, a Forensics IT specialist in Slovenia on 28 March 2012.

