Please Police Me

Craig Johnston
Asia Pacific Regional Channel Manager
ESET LLC

David Harley CISSP FBCS CITP
Director of Malware Intelligence
ESET LLC

This paper was presented at the 12th Association of anti Virus Asia Researchers International Conference (AVAR 2009) in Kyoto, and was published in the Conference Proceedings.

Abstract

Sed quis custodiet ipsos custodies [1]? (Who will guard the guards themselves?)

While the anti-malware industry has always tended to avoid poachers turned gamekeepers, the rest of the security industry has fewer scruples. But what about gamekeepers turned poacher? Time and time again, civil liberties groups are obliged to intervene as best they can when governments and law enforcement agencies attempt to expand their ability to eavesdrop electronically using "hacking" techniques and keylogging malware more often associated with the other side of the cops and robbers divide.

An issue with particular resonance in the anti-malware community is the idea of a "good" Trojan like the FBI's Magic Lantern, which not only poses ethical issues for the anti-malware industry - would vendors be prepared (or forced) to make an exception for detection? - but also inspires misgivings in the community as a whole, from privacy campaigners to the wider security community to everyday business and home users.

In this paper, we'll consider not only the ethical and political issues around "policeware" and other surveillance tools and techniques, but practicalities such as the mechanisms for distributing and installing such tools, and the maintenance and enforcement of secrecy and compliance.

Introduction

We all know and understand the intent and use of malicious software – “malware”. It’s software that is designed to do something malicious. Yes, that’s a very broad description, but the description needs to be broad to cover the many and varied ways in which software may be used for malicious purposes. It could be to steal a person’s personal information in order to steal their identity to defraud them. It could be to steal corporate secrets from businesses. It could be used to destroy data or to render systems and networks useless. We know that there are many intentions and motivations when it comes to malware, from sociopathic criminal damage, to breaking security measures so as to gain peer respect and bolster self-image, to a shameless desire to make criminal profits at the expense of others [2].

The anti-malware industry has always tended to avoid poachers turned gamekeepers, as Mike Ellison, formerly known as the virus writer Stormbringer, discovered at a Virus Bulletin conference in 1987 [3]. However, the rest of the security industry has fewer scruples: even malware writers have often found a security niche elsewhere in the IT industry on the strength of their presumed skills [4], while being convicted of hacking-related offences has often proved a viable way to establish a lucrative career in consultancy and/or the media, especially if your name happens to be Kevin [5].

But what about gamekeepers turned poacher? What if the “good guys” want to use the same methods to get access to your personal or corporate data for “legitimate” purposes such as forestalling criminal actions? How could they do it? Should they be allowed to do it? Are they allowed to do it now? If they aren’t, are they doing it anyway?

Time and time again, civil liberties groups are obliged to intervene (or at least protest) [6] as best they can when governments [7] and law enforcement agencies [8] attempt to expand their ability to eavesdrop electronically using “hacking” techniques and keylogging software more often associated with the other side of the cops and robbers divide (we assume that government agencies don’t consider the word “malware” appropriate when applied to software used for law enforcement and national security purposes…)

Government & law enforcement agencies want to be able to eavesdrop on suspect’s Internet communications and examine the contents of a suspect’s hard drive remotely, in order to enhance their own core efficiency in fighting crime and defending national security. The idea of a "good" Trojan like the FBI’s does, however, pose serious ethical issues for a security vendor, certainly one grounded in the traditionally straitlaced anti-malware industry, and even more so if there is the faintest suggestion of a replicative function.

Clipper to Green Dam

But this is not a new issue. Government & law enforcement agencies have had a desire to spy on suspect’s computers for quite some time now (and before that, there were the contentious Clipper and Capstone chips, for voice and data encryption [9]. Carnivore was a system used by the FBI around the turn of the century [10]. It was a packet sniffing device that would be installed at an ISP’s location where it could selectively monitor the Internet traffic on a suspect’s computer. The use of this system was initially allowed through a court order, though section 216 of the USA PATRIOT Act legitimized its use by the agency for limited surveillance without having to establish probable cause in order to obtain a wiretap warrant. However, it appears that by 2005 the agency had long ceased to make use of it, preferring to resort to unnamed commercial software.

Probably the best known example of a law-enforcement initiative to allow monitoring of computers in criminal investigation is the FBI’s “Magic Lantern” [11] (in the US, at any rate). The existence of this software was first reported in November 2001. Although the FBI confirmed the existence of such a program quite early on, they denied that it had ever been deployed. Apparently the purpose of the “Magic Lantern” was to install a keylogger via an email attachment. This keylogger would then be used to record & divulge encryption keys used by a suspect to encrypt his or her hard disk contents and/or email messages. Some major anti-virus companies were accused [11] of working with the FBI to allow this software safe passage through their products, but it’s by no means clear that any major vendor did actually waive detection. F-Secure, for one, specifically stated that they would not waive detection for Magic Lantern [12], while insisting that they would also retain detection of known crimeware, even where it was associated with violent criminals such as the Mafia, or with terrorist organizations.

CIPAV – the Computer and Internet Protocol Verifier – appears to be a tool used by the FBI to track and gather location data on suspects. This operates much like spyware, gathering information on the suspect’s computer and online activities then sends them back to a central point, without the knowledge or consent of the suspect. This software was used in July 2007 in a case against a teen who had made bomb threats against his high school [13].

In 2006 Microsoft held discussions with the British government about the possibility of them putting a backdoor into their operating systems so that government authorities could gain access to the content of users’ hard drives. Microsoft later said in a statement that “Microsoft has not & will not put ‘backdoors’ into Windows”. [14]

In 2007 US Drug Enforcement Agency agents broke into the home of an alleged mobster and installed a keylogger on the suspect’s computer in order to gather evidence against his suspected Ecstasy manufacturing activities. This was deemed to be necessary as the contents of the suspect’s hard drive had been encrypted using PGP. It was done after the agents had obtained court orders allowing them to take such action [15].

More recently, earlier this year the Chinese government mandated that, beginning July 1 2009, every PC sold in China must include a censorship program called Green Dam. This software is designed to monitor Internet connections and text typed on the computer. It blocks undesirable or politically sensitive content and optionally reports it to authorities. Green Dam was developed by a company called Jin Hui and is available as a free download. But not long before the first of July, in a quite unexpected move, the Chinese authorities have indefinitely postponed their order that all PCs sold in the country must come with software, called Green Dam Youth Escort, which blocks certain websites. However, the use of the software remains mandatory in “public” computers [16] and questions remain unanswered about some of the purposes and even the provenance of some of the code.

Bird on a Wiretap

Some legislation in some places allows the tapping of Internet lines, similar to phone tapping. But if the suspect hasn’t downloaded or uploaded the material in question, then eavesdropping on the line won’t help law enforcement agencies.

So what options do law enforcement agencies have open to them? One option is for them to create some code that will act as a keylogger or at least open a backdoor for further downloading of code to gain access to the information on the computer. The delivery mechanism, however, would be hit and miss: in particular, it’s unlikely that replicative policeware would meet the warrant criteria for a (quasi)wiretap or phone tap, because of the difficulty of restricting its spread to named and targeted suspects.

But this approach has a number of other problems. Anti-virus (AV) companies focus their efforts to identify/block/clean/delete/quarantine code that they identify as a Trojan, backdoor, keylogger or anything that appears to be acting maliciously. The agency would need to supply every anti-virus vendor with a sample of the code and get them to agree to NOT trigger if it is detected, effectively whitelisting the code. Chances are, most if not all of the AV vendors would probably not agree to that. Reputable security companies usually prefer to cooperate with law enforcement agencies rather than thwarting them – after all, we’re very much in the business of remediating criminal activities. But having to give the code to EVERY AV vendor would spread the secret very far & wide, making it virtually impossible to keep the secret. And, if the secret DID get out and the bad guys got their hands on the code that all AV vendors had agreed not to detect, then they could and almost certainly would use it for malicious purposes with total immunity. That would be a huge problem.

Then we have the legislative issues. Are the good guys allowed to spy on the contents of your computer? Are they allowed to eavesdrop on the traffic passing to and from your computer? It seems that the powers and capabilities of cybercrime and homeland security agencies vary from one agency to the other, from one state to another, from nation to nation.

In Australia for example, there is different legislation regarding cybercrime in each state. Cybercrime police in the Victorian police force believe that their legislation would allow them to take such actions. Whereas the cybercrime police in Western Australia believe that they would not be able to plant malware (spyware?, policeware?, surveillanceware?) on a suspect's computer due to the limited powers they have when it comes to cyber investigations.

Whether they are allowed to or not, the question must be asked - SHOULD they be allowed to or not? Civil liberties groups have long fought with government & law enforcement agencies about whether it is appropriate for them to have access to such information, and what safeguards need to be in place to ensure this power to obtain information on an individual or company is not misused. Clearly, this differs according to cultural factors: whereas the rights of the individual are often deemed to be paramount in many Western nations, other cultures feel very differently, and even in the West, support for libertarian groups can shift alarmingly in times of terrorist-induced paranoia.

David Sobel, the General Counsel for the Electronic Privacy Information Centre, said of Magic Lantern [17]: "We don't know what this is capable of and whether it is being properly used. There may be no way to stop this from being installed on a computer." While it's unlikely that any law-enforcement issue will be magically unstoppable, we all know that the only likely way to stop this would be through the use of anti-virus software, firewalls and other IT security measures.

But how different is eavesdropping on your Internet cable to tapping your phone line? Phone tapping is considered acceptable in most places, usually after the need for the tapping is verified & approved by someone in authority, such as a judge. Many will say that there is no conceptual difference, and that if you have nothing to hide, you have nothing to fear, but libertarians are likely to take a different view.

According to a source who used to work for a national security agency, it seems some of the good guys are writing malware for their own purposes anyway. This individual wouldn't actually state openly that this practice was going on, but he certainly alluded to that fact. It seems what they are doing is creating their own malware, but making sure it looked like it had been written by the bad guys, just in case it is discovered on the system. He also suggested that if an anti-virus product at some point detected the code on a suspect's computer it was a major setback to their investigation & surveillance.

Conclusion

So, let's look at the main questions here.

Should government & law enforcement agencies be allowed to plant spyware on a suspect's computer? It depends on your point of view. Privacy & civil liberty groups believe it is an invasion of our privacy. The government & law enforcement agencies claim it may be a vital weapon in their arsenal to use against criminals and terrorists using high tech methods, though some governments are probably not above using national paranoia to push a draconian agenda.

Are government & law enforcement agencies allowed to plant spyware on a suspect's computer now? In some cases, this has been done with the approval of those in authority. But at the moment the planting of spyware on a suspect's computer is not allowed in many countries unless under special circumstances relating to criminal investigation or national security. The reality is that legislation varies greatly around the whole when it comes to this matter. There is very little consistency at the moment, and there is unlikely to be in the absence of a world-wide, homogenizing culture. Indeed, there's little consistency even within individual countries: while much legislation proposed in the West has been focused on increasing the government's capacity for surveillance of the general population as well as of criminals (both cyber criminals and perpetrators of more traditional categories of crime), other legislation has been focused on enhancing the individual's rights to privacy and confidentiality of data – for example, In accordance with the European Directive on Data Protection [18].

Are government & law enforcement agencies planting spyware on a suspect's computer now? The short answer to this question is "almost certainly". Well, I would go so far as to say "certainly". But in most western countries you will be hard pressed to find someone to admit the extent to which the practice goes on, and they do not, in general, seem to be asking antivirus companies to waive detection. But if we were to start agreeing to such requests, would we have to honour requests from *all* countries who asked? (We're assuming here that where local legislation *required* cooperation, vendors would generally be required to comply, though thinking through some of the implications of that assumption could occupy a paper all on its own.

References

[1] Juvenal, Satire VI, line 347

[2] "Crème de la Cybercrime" in "AVIEN Malware Defense Guide for the Enterprise", ed. Harley, Syngress 2007

[3] Kurt Wismer, "Research isn't always victimless", http://anti-virus-rants.blogspot.com/2009/08/research-isnt-always-victimless.html; Mike Ellison, "Defecting from the underground – are ex-virus writers of use to the anti-virus industry?" in Virus Bulletin 7th International Conference Proceedings, Virus Bulletin, 2007

[4] David Harley, "Taking the Mikeyy", http://www.eset.com/threat-center/blog/2009/04/20/taking-the-mikeyy

[5] http://en.wikipedia.org/wiki/Kevin_Poulsen; http://en.wikipedia.org/wiki/Kevin_Mitnick

[6] David Harley, "Magic Lantern in the UK?", http://www.eset.com/threat-center/blog/2009/01/08/magic-lantern-show-in-the-uk

[7] Gadi Evron, "German Intelligence Caught Red-Handed In Computer Spying, Analysis", http://www.darkreading.com/blog/archives/2009/03/german_intellig.html

[8] Nigel Morris, "Civil liberties groups raise alarm over extension of surveillance without warrant", http://www.independent.co.uk/news/uk/home-news/new-powers-for-police-to-hack-your-pc-1225802.html

[9] http://epic.org/crypto/clipper/

[10] Kevin Poulsen, “FBI retires its Carnivore“, http://www.securityfocus.com/news/10307

[11] http://en.wikipedia.org/wiki/Magic_Lantern_(software)

[12] F-Secure: F-Secure Corporation's policy on detecting spying programs developed by various governments: http://www.f-secure.com/virus-info/bdtp.shtml

[13] Kevin Poulsen, FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats: http://www.wired.com/politics/law/news/2007/07/fbi_spyware?currentPage=2

[14] Darknet, "UK Wants Backdoor in Next Version of Microsoft Windows"; http://www.darknet.org.uk/2006/02/uk-wants-backdoor-in-next-version-of-microsoft-windows/; http://news.bbc.co.uk/2/hi/uk_news/politics/4713018.stm

[15] Declan McCullagh, "Feds use keylogger to thwart PGP, Hushmail", http://news.cnet.com/8301-10784_3-9741357-7.html

[16] Matthew Green, “China drops Green Dam web filtering system”, http://www.guardian.co.uk/technology/2009/aug/13/china-drops-web-censorship

[17] David Corn, “The FBI's Black Magic?” http://www.big-brother.net/thefbisblackmagic.htm

[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://www.cdt.org/privacy/eudirective/EU_Directive_.html