Spyware: modern investigative tools. Need of a trade-off between citizens security and citizens' rights

Simone Marforio

January 8, 2021

POLITECNICO
MILANO 1863

Contents

Abstract

This paper explores the necessity by law enforcement to use malware during investigation in order to fight crimes in the interest of the citizens. It aims to point out aspects that can lead to power abuses and invasion of citizens' privacy. It analyze the issue related to the utilizations of this software and presents the need for regulation of these tools and of the manufacturing companies. It will be shown how some decisions, of dubious morality, taken by manufacturers, have gone beyond the boundaries of citizens' safety, allowing governments and other institutions to abuse their powers.

Introduction

Criminals and terrorists are increasingly exploiting technological progress to conduct their business, consequently even states and law enforcement agencies must evolve their way of investigating. The use of malware to fight crimes is nothing new but for long time utilization of malware as investigative tool has been kept secret and unregulated. This lack of norms lead to numerous scandals that shown the necessity to regulate this technology. This paper aims to point out some problems that can threat citizen's right in the event that spyware is used inappropriately and without proper rules. It focus on the need to regulate the use of malware by states and the importance to properly monitor the firms that are involved in the manufacturing of the software adopted by the law enforcement. The topic intersects with numerous issues addressed by jurists and lawyers, which are all based on ethical behavioral norms.

The first two sections of the document explore why law enforcement agencies need to use these tools, shows some news cases involving the use of this technology, and briefly explain some features of the malware, necessary to understand the subsequent discussions. The third section focus on the issues that lack of regulation can lead to, showing how much powerful are malware and comparing it with older investigation techniques. After that, the attention is shifted towards the importance of controlling supplier companies so that they do not support espionage activities that violate human rights.

Malware

The term malware stand for malicious software, it is a generic term that includes Trojan horses and spyware, and describe any software with subversive purpose [1]. Trojans and spyware, after infecting a machine, aims to collect files, monitor user operations, turn on the webcam and capture pictures, and, at the end, reports the gathered information to a remote server controlled by the attacker. In some cases this software can be designed to remotely execute other programs on the victim machine. In this work I will often use the general term malware to refer to any kind of malicious software that act as Trojans.

Perhaps is already clear from the previous definition that malware is an extremely powerful tool in the digital age, both for illegal activities and for defense purposes. However, before discussing how this software can be used, some other considerations about their nature have to be pointed out, with the aim of better understanding which are the benefits and the risks that this kind of technology brings along with it. First I try to point out which are the properties that characterize a malware. Then I try to sum up which are the required steps to take advantage of these tools.

For our purpose I can summarize malware's characteristics as hidden, boundless, invasive and wasting resources. One of the key points that allows this kind of malicious software to be so powerful is because it works silently, the user ignore its presence, and it is extremely difficult to discover. Another strength is related to the fact that this technology is designed to work in the cyberspace where all the conventional boundaries have been destroyed. In this scenario anyone with a computer, and enough knowledge, can deploy an attack against someone located miles away from him. The invasiveness of a malware is due to the fact that the security countermeasure are bypassed and every file, program, microphone, webcam and so on can be accessed remotely and used without the user consent. Look Trojans as "wasting resource" [2] is necessary to understand some problems that I will explore in the next chapters. Before being able to develop a malware that can take controls of a computer, a vulnerability in a program must be discovered and correctly exploited. A vulnerability is a weakness in a software caused by a not quite correct implementation functionalities. Programmers, software houses, researchers are constantly involved in looking up to this kind of weak point with the purpose of fix it. On the other side also hackers or other groups are interested in this field with the aim to sell vulnerabilities or use it. Having said that, and having pointed out that this is a match between who want to fix weakness in name of security against who

want to take advantage of it, what remain to understand is that when a malware is discovered for the first time, also the exploited vulnerabilities become of public domain and this mean that programmers start to fix them and the weaknesses are no longer available.

As Jonathan Mayer identified in his works, utilization of a malware can be divided in four distinct steps: "delivery, exploitation, execution and reporting" [3]. Even if Mayer make this consideration explicitly regard to government malware, I think that this workflow suits well also to a more general context, where the attacker, the one who benefits of the use of this tool, can be a government, a hacker or anyone else. In the delivery phase the attacker have to find a way to install on the victim machine the malicious software. This can be done in different ways such as using social engineer techniques, inducing the target to click on a suspicious link, can be done manually, breaking into the office of the target, or can be done compromising an infrastructure in order to be able to monitor the entire data flow of the website. The exploitation phase require to tail the malicious software according to the target information, the data want to be collected and the available vulnerabilities. In the third step, the malware executes its behaviour and start collecting information or do whatever it is programmed to do. An important key point for some of the following discussions is that this phase not always has a deadline, certain malware can remain operational for a long period and neither the attacker stop it. And finally, the Trojan have to report the information to server that is under control of the attacker.

Use of malware by law enforcements

Before starting to argue and discuss any possible problem related to the utilization of malware in name of national security, is important to understand why governments have necessity to supply law enforcement with this kind of technology. In a wider context, malware can be classified as cyberweapons, justified by necessity to fight the growing threat of cyber terrorism, perpetrated by terrorist organizations, sometimes sponsored by adversarial states [4]. For this reason is legitimate to ask if the utilization of these technologies is admissible outside a cyberwar context. In my opinion their utilization can be morally justified considering two principle: the law of international conflict, which regulate and legitimate the use of armed force as countermeasure to a possible threat, that can be extended to conflicts in cyberspace, and the principle of self-defence that allow states and non-states entity to use force in order to protect themselves. These aspects are well presented by D. Denning in

"The Ethics of Cyber Conflict"[5], and in conclusion, utilization of spyware by law enforcement is permissible for defensive purpose, but response must be carefully proportioned to the threat, and subjected to strict controls and rules.
Anyway, without further explore the cyberwar scenario, the utilization of malware by law enforcement is easily understood analysing how information is exchanged over Internet. "The government's need to use malware to investigate crime is almost always connected to a target's successful use of encryption" [6], "As encryption and anonymization tools become more prevalent, the government will foreseeably increase its resort to malware"[7]. As we can see from the two previous quotes, Paul Ohm, Jonathan Mayer and many other experts [8] agree that the main reason to use malware is the end-to-end encryption of the communication. As the correct implementation of the encryption algorithm makes useless any interception, with the installation of a malware directly on the device of the target allow to eavesdrop the information in plain text. There are many successful utilization of this technology that are jumped on the front page of newspaper, in example the recent European conjuncted operation that lead to dismantling EncroChat, an encrypted network, and to arrest about hundreds of criminals [9][10]. However this kind of techniques, and their purpose, are also involved in many scandals such persecutions on journalists, activists or citizens [11][12][13].

It's clear that in some context utilization of malware is necessary and is the only solution against criminals that hide their identity or exchange information using encrypted channels.

Moral and legal problems

From now on I want to analyze and discuss some troubles and damage that such an invasive and persistent software can lead to, if not used with strict regulations. First I try to point out the main problems regarding the utilization and the users, comparing this investigative tool with other forms of surveillance. After that I want to highlight a problem regarding the developing and the selling of this software, and some possible scenarios where preciosity of the vulnerabilities could harm an innocent person in court.

The need to tame Trojan horses

Governments have been secretly using malware for many years, but management of these tools cannot be left to chance. Fortunately in recent years, thanks to some

information leaks that reveal this practice to the citizen, States and organization starts to discuss and to regulate this kind of software, for instance in Italy the decree law No. 216/2017[14] and its subsequent update (d.l. No. 28/2020[15]) aims to this. One of the main aspect to consider is when spyware can be used and against whom. In order to avoid misuse is important to define some special case in which law enforcement can require the utilization of malware, and this kind of situation are restricted to the case in which the interception is strictly necessary for the continuation of the investigation and other techniques are ineffective. The Italian decree law No. 28/2020 define the utilization of spyware in cases where the survey relate to some specific crime [16]. Some other problems are harder to regulate because more related to the information technology field. Is important to ask whether a government can use a malware only in investigations that are done over its territory, or it can deploy an attack against someone that live in another country. Other considerations can be done trying to analyze the four steps necessary to perform a wiretap with a malware: delivery, exploitation, execution and reporting. The delivery phase require to find a way to install the spyware in the victim machine, this can be done through social engineering technique or manually, but can happen that these methods fails. One solution is to exploit some other delivery network, install the spyware on thousand of device and, at the end, collect the data of the interested party only. This is what happened for example with the German spyware case[17] or the Italian scandal of Exodus[18]. These situations, where spyware launched 'in the wild', highlight the importance of a solid regulation since is not always possible to discriminate a specific target. Therefore, we can debate if launch a spyware 'in the wild' in name of national security is justifiable, but as Rossano Ferraris wrote "The answer is simple: it is not possible!"[19], if the use of malware is justified against criminals, install it in most of citizens'devices, without evidence of crime, cannot be justified in any way, especially considering the abuses that can be done with this tool. I will explain the issue related to the exploitation phase further on because strictly connected to the concept of vulnerability, now focus on the execution phase. I think that there are three important questions to answer in order to try to regulate the use of malware: how long they can stay active, when they can collect data and, more important, what exactly can do. This remote intrusion software, usually, are not provided with a switch off button, moreover is difficult to discover them. These properties imply that it can remain active for a long, and nobody can uninstall it without reveal the presence of it. This may be a problem in the cases in which the investigator have not enough evidence to accuse the investigated, and the survey are abandoned. The second questions regard the moments in which this tools can perform their work. With the old wiretap techniques, investigators had to

install hidden microphones, physically stalk the suspects or listen their phone calls. Using malware all this thing can be done better, more easily and with less risks. This, of course, damage the privacy of the investigated, someone can assert that is irrelevant because we are trying to unmask a criminal, and I could be agree, but, also the privacy of every other individual that interact with the suspect is threatened. With the old techniques the amount of information collected were proportional to the efforts of the police and limited to the business they were investigating on, while with the use of malware the data that can be collected are not only related to the criminal activity, but to anything happening near the infected device. To make it more clear, if the spyware is collecting images from the camera and accidentally frame a loving betrayal of two strangers we get into a privacy violation. I will expand the third question in detail later on, for now I want to point out that spyware provide a power that the traditional wiretapping techniques did not have: they are not only passive tools, they are active, can also "use" the device. In the reporting phase the collected data have to be transmitted through the internet and stored in a computer. In the d.l. No. 216/2017 is not defined any requirements concerning where store the information and only some generic indication are given about the way this data have to be transferred to destination server[20]. The regulation of these aspects is crucial to guarantee the right of privacy of citizen since they are handling sensitive data. Strict requirements have to be provided defining the communication protocols and also imposing that the information have to be stored in an infrastructure managed by the state, avoiding any possibility of outsourcing to some well known tech company, which provide a cloud storage service, but aims firstly to increase its incoming.

Other forms of surveillance

As I wrote before, is important to allow the use of spyware by law enforcement only when this type of technology is strictly necessary for the continuation of the investigation. In the other cases exist other techniques that provide the same results. I already spent some words comparing spyware and old investigative techniques, now I want to focus on which are the differences between Trojan horses and other two technology used by law enforcement: cell-site simulators and facial recognition. Cell-site simulator, or IMSI catchers, are devices, controlled by police, that emulate legitimate telecommunication infrastructure and trick phones into connecting to these devices rather than a cell-phone tower. These devices are used to better triangulate the location of a phone, intercept the conversation that pass through it and, sometimes, can alter the content of communications. Seems that IMSI catcher are almost invasive like spyware, or worst, because also innocent users are duped by

the fake cell-site. However is hard that the wiretap with this technology last for long time, because is likely that the suspect change its position during the day and is expensive for law enforcement to stalk him. Moreover I want to point out something that I had not explored before, the fact that exploiting a vulnerability, i.e. use a malware, can be morally questionable because broke an unwritten contract of trust between the user and the service provider, that guarantees to the buyer the product is secure. Instead, as Paul Ohm wrote [21], cell-site simulator take advantage of the openness of the cell phone standards and the necessity of backwards compatibility, meaning that no bugs or system misconfigurations are exploited. Regarding the face recognition technology, even if can be more easily abused by law enforcement, due to the fact that image comparison algorithm can be used multiple times, without wasting any resource and with a low deployment of forces, this technology is limited to take in input photos or video of an anonymous people, that can come from social networks or other sources, and provide as output the (likely) identity of the suspect. All three technology can be misused, for this reason all have to be regulated, but, neither the cell-site simulator nor the facial recognition, allow to collect the same amount of information as with a spyware. Malware are not only a wiretapping tools, they are persistent and, more important, can act, having full access to the device.

Malware manufactures and moral issues

I already provided some example of abuse of this technology, all of them perpetrated by liberal states, and it's clear that, if such abuse can happen in liberal states, in dictatorial states, where humans rights violations are commonplace, this type of technology can only increase to the detriment of citizens' freedom. In 2015 Hacking Team was an Italian information technology company in the offensive security field, able to develop powerful intrusion tools which could be used by anyone after a two week course. Their spearhead was the Remote Control System called Galileo, which led to the signing of millionaire contracts with governments and individuals. On July 5, 2015 the firms was hacked and about 400 GB of sensitive data had been published on WikiLeaks, showing a picture of clients and contacts of dubious morality. The previous year the company had already been criticized by The Citizen Lab which published a report[22] that connect Hacking Team with some actions of undemocratic governments. The stolen data not only confirmed the work conducted by The Citizen Lab, but designed a bigger picture. Hacking Team's customers included Italian and American intelligence agencies, but also private companies, arms dealers and governments such as Sudan (embargoed by the UN) and Egypt (full customer list on Wikipedia[23]). In addition, situations of favoritism

emerged with unjustified collaboration between the private company and high officials of the government intelligence services[24]. The same Hacking Team's business can be found in other companies in the same industry, such as the Anglo-German Gamma Group (previously Gamma International), or the Israel based NICE Ltd. From these events emerge that the problems associated with this type of software do not concern only their use, but also their sale. Even if the European Commission in 2014 (EU regulation 1382/2014[25]) introduced intrusions software in the list of dual-use products, a list of goods, technology and software that can be used both for civil and military application, and are subject to more stringent export regulations, it's clearly necessary a more strict regulation of the providers company[26] and, a way to identify the responsibilities of the involved players. The question is whether firms are the right type of entity to develop a such powerful technology. Developing intrusion software can be expensive for national agencies and private company can be a valid resource. What have to be kept in mind is that in a such sensitive field the social nature of the company must be well defined and constantly controlled by the government. As Filippo Pierozzi wrote in his report, Hacking Team had an hybrid nature, the firm had "a strong nationalistic connotation" [27] but it did not hesitate to sell the product to possible enemy of the nation. In this sense Hacking Team was a business only firm, but has gained so much power that it can afford favors from very influential people. For these reasons, another question is who is responsible for the humans rights violation perpetrated with that software. Donaldson and Dunfee[28] argue that firms have "free space" to select their moral value within the boundaries of certain "moral minima". Governments instead, if they call themselves liberals, have to respect their moral values and their citizens. In the Italian scandal emerged that not only Hacking Team company is morally responsible of crimes perpetrated by their software, but some guilt can be attributed to governments and commissions that have not properly supervised. In such sensitive partnership between public and private, that involves diplomatic relations and national security field, the government have to protect its interests and relationships with other states, imposing a complete transparency from the private company. Players that are not agree with the moral standards of a firm have to be free to don't do business with this company, in order to not be held responsible for any future violation of any kind[29]. One last discussion that I want to introduce concerns the possible implications that selling a software "ready-to-use", such as RCS Galileo, may have. This software, thanks to their simplicity and a short training course, allow anyone, without background in computer security field to perpetrate attack against other people. The difference between selling this software versus vulnerabilities only is in the audience size. While the sale of vulnerabilities shrinks the pool of buyers to experts only, "ready-to-use"

software has a larger pool of buyers. Therefore the problems of this technology is not only related to their uncontrolled sale to government and subversive, but also to the fact that this software is sold to individuals or companies to spy on their opponents or employees, without any right or justification in doing this.

Vulnerabilities like diamonds, rare and precious

In this last paragraph I complete the speech concerning the issue of malware deployment by law enforcement, expanding the exploitation phase aspects. As already said, malware (and vulnerabilities) can be seen as a wasting resource and according to Paul Ohm this intrinsic characteristic make government abuse less likely[2], however the same characteristic can lead to other problems. An important element during a trial is the possibility for the defense to be able to fully analyze the work of the prosecution. Of course sometimes this is not possible for reasons of secrecy, but with the use of malware this can become the practice, moreover, hypothetically, thanks to the enormous amount of information that can be recovered with these tools, an entire process could be based only on the evidence gathered with spyware. What can happen is that due to the need not to burn a vulnerability, more information than the necessary are kept secret and some details of the investigation are omitted from the report, causing a lack of usable evidence in defense of the accused. Another issue can be identified thinking about the actions malware can perform once it is installed on a device: not only collect information but also interact with programs and files. This full access to the resources with the impossibility to make the source code of the intrusion software public for review, complicates being able to prove if any abuse, orchestration or falsification of the evidence took place during the investigation phases. Even if law enforcement and government agencies are trusted element of the state that have to act in the interest of citizens (while firms such as Hacking Team are not), these latter aspects pointed out, one more time, how easy is to abuse these tools and how important is to regulate and limit their use.

Conclusions

The adoption of malware by the police is inevitable to fight the criminals that today increasingly exploit encrypted messaging and anonymization services to conduct their business. With spyware law enforcement are able to gather information before that those protection mechanism take place, however such powerful tool can harm citizen's privacy. To best guarantee the safety of citizens and their rights, governments have to adopt a strict regulation in this regard. Define the boundaries of use of this

technology and constantly monitoring users is not enough to ensure that there is no abuse of power by the owners of these software. Governments and communities must monitor the manufacturers and suppliers of these tools and prevent them from being sold to arms dealers or states that would abuse them. Regulate is possible and compliance with moral norms can prevent human rights violations, moreover, informing and making citizens and experts in the sector aware of this issue, allows to take the right decisions in advance for the collective good.

References

[1] Anne Kerr Andrew Butterfield Gerard Ekembe Ngondi. *A Dictionary of Computer Science (7 ed.)* Malware : An inclusive term for any software with a subversive purpose. Malware includes Trojan horses, viruses, worms, adware (def. 2), and spyware. Oxford University Press, 2016, p. 758. ISBN: 9780199688975.

[2] Paul Ohm. "The Investigative Dynamics of the Use of Malware by Law Enforcement". In: 26 Wm. & Mary Bill Rts. J. 303 (2017), 2017, pp. 313–314. URL: https://scholarship.law.wm.edu/wmborj/vol26/iss2/4.

[3] Jonathan Mayer. "Government Hacking". In: *127 Yale L.J. (2017)* (2017), pp. 583–589. URL: https://digitalcommons.law.yale.edu/ylj/vol127/iss3/2.

[4] Marwan Albahar. "Cyber Attacks and Terrorism: A Twenty-First Century Conundrum". In: *Science and Engineering Ethics* 25 (Aug. 2019). DOI: 10.1007/s11948-016-9864-0.

[5] Dorothy E. Denning. "The Ethics of Cyber Conflict". In: *The Handbook of Information and Computer Ethics* (2008). DOI: 10.1002/9780470281819.ch17.

[6] Paul Ohm. "The Investigative Dynamics of the Use of Malware by Law Enforcement". In: 26 Wm. & Mary Bill Rts. J. 303 (2017), 2017, p. 317. URL: https://scholarship.law.wm.edu/wmborj/vol26/iss2/4.

[7] Jonathan Mayer. "Government Hacking". In: *127 Yale L.J. (2017)* (2017), p. 570. URL: https://digitalcommons.law.yale.edu/ylj/vol127/iss3/2.

[8] Barbara Indovina. "I captatori informatici: una riforma troppo contenuta per uno strumento investigativo così pervasivo". In: *MediaLaws* (2018). URL: http://www.medialaws.eu/rivista/i-captatori-informatici-una-riforma-troppo-contenuta-per-uno-strumento-investigativo-cosi-pervasivo/.

[9] Ylva Johansson. Aug. 2020. URL: https://ec.europa.eu/commission/commissioners/2019-2024/johansson/blog/encrochat-shows-europol-irreplaceable-fighting-cross-border-crime_en.

[10] Carola Frediani. July 2020. URL: https://www.valigiablu.it/encrochat-maxiretata-criminalita/.

[11] John Scott-Railton and Ronald J. Deibert. Mar. 2019. URL: https://www.theglobeandmail.com/opinion/article-governments-are-deploying-spyware-on-killers-drug-lords-and/.

[12] Stephanie Kirchgaessner and Sam Jones. July 2020. URL: https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware/.

[13] *Global surveillance disclosures*. URL: https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present).

[14] *Decreto Legislativo 29 dicembre 2017, n. 216*. URL: https://www.gazzettaufficiale.it/eli/id/2018/01/11/18G00002/sg.

[15] *Decreto-Legge 30 aprile 2020, n. 28*. URL: https://www.gazzettaufficiale.it/eli/id/2020/04/30/20G00046/sg.

[16] *La riforma della disciplina delle intercettazioni*. May 2020. URL: https://temi.camera.it/leg18/temi/la-riforma-della-disciplina-delle-intercettazioni.html.

[17] Adam Taylor. *Here's What You Need To Know About Germany's Government Spyware Scandal*. URL: https://www.businessinsider.com/germany-spyware-r2d2-2011-10?IR=T.

[18] Alessador Longo. *Più di mille italiani intercettati sul cellulare, per errore, da un hacker di Stato*. URL: https://www.repubblica.it/tecnologia/sicurezza/2019/03/30/news/molte_centinaia_di_italiani_intercettati_su_cellulare_per_errore_da_hacker_di_stato-222865990/.

[19] Rossano Ferraris. *Spyware governativi: realtà o leggenda?* 2011. URL: http://www.aipsi.org/images/stories/pubblicazioni/contr/spyware%20governativi.pdf.

[20] Barbara Indovina. "I captatori informatici: una riforma troppo contenuta per uno strumento investigativo così pervasivo". In: *MediaLaws* (2018), p. 11. URL: http://www.medialaws.eu/rivista/i-captatori-informatici-una-riforma-troppo-contenuta-per-uno-strumento-investigativo-cosi-pervasivo/.

[21] Paul Ohm. “The Investigative Dynamics of the Use of Malware by Law Enforcement”. In: 26 Wm. & Mary Bill Rts. J. 303 (2017), 2017, p. 325. URL: https://scholarship.law.wm.edu/wmborj/vol26/iss2/4.

[22] Morgan Marquis-Boire Bill Marczak Claudio Guarnieri and John Scott-Railton. “Mapping Hacking Team’s “Untraceable” Spyware”. In: (2014). URL: https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

[23] *Hacking Team*. URL: https://en.wikipedia.org/wiki/Hacking_Team.

[24] Russo Massimo Frediani Carola Ruffilli Bruno and Zanotti Raphael. *Attacco ai pirati. L’affondamento di Hacking Time: tutti i segreti del datagate italiano*. La Stampa, 2015.

[25] *Commission Delegated Regulation (EU) No 1382/2014*. 2014. URL: https://eur-lex.europa.eu/eli/reg_del/2014/1382/oj/eng.

[26] CILD. Coalizione Italiana Libertà e Diritti Civili. “TROJAN & CO. Tecnologie di sorveglianza e controllo delle esportazioni”. In: (). URL: https://cild.eu/wp-content/uploads/2017/06/TrojanCo-IT.pdf.

[27] Filippo Pierozzi. “Il caso ‘Hacking Team’: quis custodiet ipsos custodes? Problematiche e sfide per una più efficiente partnership tra settore privato e agenzie d’intelligence nella cybersecurity”. In: (2015), p. 5. URL: https://www.dsps.unifi.it/upload/sub/filippo-pierozzi-hacking-team-paper.pdf.

[28] "Thomas Donaldson and Thomas W Dunfee". “"Ties that bind in business ethics: Social contracts and why they matter"”. In: *"Journal of Banking & Finance"* "26"."9" ("2002"), "1853–1865". ISSN: "0378-4266". DOI: "https://doi.org/10.1016/S0378-4266(02)00195-4". URL: http://www.sciencedirect.com/science/article/pii/S0378426602001954.

[29] Jeffrey Moriarty. “Business Ethics”. In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Fall 2017. Metaphysics Research Lab, Stanford University, 2017. URL: https://plato.stanford.edu/archives/fall2017/entries/ethics-business/.