The dangerous world of Spyware Literature Review

https://doi.org/10.53732/ideas/v1i1.630

Roberth G. Lima Carvajal, Marco Inlago-Cuascota

Faculty of Engineering in Applied Sciences, Software Engineering,
North Technical University,
Ibarra, Ecuador

ABSTRACT

Abstract. Computer security is an issue that has been gaining strength in the last decade, this because the possibility that the government or companies outside the law monitor citizens is worrying. Spyware, a software that does nothing more than violate the privacy of people who are unfortunately infected with one or more and this is done in a hidden and quite silent way. For this reason, it is extremely important to know, recognize and even determine how to fight against these tiny cyber threats. This small software filters, searches and steals information abruptly, which could cause economic catastrophes in a family, or in a company, selling information or taking advantage of all the stolen content to wreak havoc. Although some spyware developers sell their product to control employees, this does not detract from the fact that their program handles the same operation as if it were to do evil. The following work introduces the world of Spyware. According to the investigations that have been carried out, we have obtained as a result its uses, its types, operation and even some ways of how to prevent it and if it is the case, also how to eliminate it. Individuals and companies have a responsibility to act on every spyware problem, and it is their duty to improve the security of each device to avoid more similar problems in the future.

Keywords: Computer Security, Data Security, Data Privacy, Malware, Privacy, Security, Spyware

Introducción

Currently the concern about cyber privacy is gradually becoming a fairly extensive topic on which a lot of people are taking into account and seeking preventive measures, which often are totally contradictory to the problem which they want to avoid, such as installing software pages that do not have certificates, or are not safe, and all with the desire to protect themselves from malicious software are infected by the general ignorance that exists in the population.

The worrying thing is that most people don't find out about this program because of research or merit, but because of some general magazine, or a post on Facebook where they saw that a certain celebrity or character suffered from a Spyware virus, and now readers want to avoid this [1].

The purpose of the following investigative work is to find what are the most important aspects of spyware, such as: What is it? Its functionality, its types, ways to prevent it and how to eliminate it and summarize it in a way that readers understand faster into the dangerous world of spyware. In addition, it is important that people fully understand how dangerous spyware can be.

Theoretical Foundation

It should be clarified that a Spyware in simple terms is a software in the first instance illegal, since its function completely breaks with the non-violation of user privacy, of course in certain ways the software if you can ask the user's consent to enter your machine, but as mentioned, on certain occasions, and at certain times, as it would be on computers, or laptops in a company, where the manager or boss wants to be attentive 24/7 hours a day watching and monitoring what activities has made the worker in the company computer while he is using it [2].

It should be noted that this program focuses on stealing information, and in most cases not for legal or "kind" activities so to speak, and after having stolen the information it shares it

through the internet, causing the leakage caused to be quite dangerous. [3]

What is spyware?

It is a software, usually installed on a user's computer without his consent or without the user's knowledge, the function of which is to secretly collect information from the computer on which he is working, and then transmit that information, also covertly, to another person. [2] It is also known as a "secret data collection software", which is used to collect information from a user's computer without the user's consent or knowledge.

Spyware can infiltrate a computer either as a virus or as a Trojan, hidden inside another program; it can also hide in corrupted hardware, such as a USB drive [3].

As Spyware leaks information whether it is normal or confidential, it is a danger for companies, as their data, statistics could be being seen by people who do not intend anything good with the use of that information [4].

To better understand the concept of Spyware is worth mentioning its main function, which is to record and track activity on computers and mobile devices, as currently this virus can also affect the mobile environment as Android or IOS, and that worries users, as they thought they were free of this by the simple fact of using devices with operating systems mentioned above [1].

But its main function does not stop there, it also has secondary functions, which are closely related to the theft of information, as a good Spyware virus can detect all your activity on a computer, and this without the user realizing it. Among other functions are also:

- Taking screenshots
- Recording the screen without the person's consent
- Track user's online activities
- Monitor everything written, downloaded, and uploaded
- Activate the camera and microphone without the user's consent

And those are just a few of the illegal uses that spyware can be put to. One use that may be more alarming to many is to track online activities and record/monitor everything written, downloaded, and uploaded to the network, as this means that easily if a person makes a purchase online using their credit or debit card, the spyware may already have copied exactly all the data from the card, which would cause a theft of money without the user even realizing it [5].

On the other hand, this depends a lot on the people who have been infected, because if a child is infected by this malicious software, for obvious reasons there will not be much to filter this, so the program would be extremely useless; it is worth mentioning that despite this spyware can also spread through the network, infecting all devices that are connected to the same WIFI network, and there if putting at risk the privacy of an entire family, all for the carelessness of an infant. [6].

But of course, as in life everything good has its bad side and vice versa, in this case it could be said that the Spyware can have a legal use, in quite specific occasions. As, for example, in the work of a company, previously mentioned a case where it was explained a little about how you could use this software and treat it as a help to the bosses of a particular company, but how?

Since this could be done because in a company it is not necessary that workers are wandering on social networks like Facebook, Instagram, etc., therefore, certain developers of this software promote their program as an easy solution for these cases, where in each machine running these software's and monitor all activities that the worker performs on it, and thus avoid activities that are not allowed in the company.

A somewhat extreme functionality, usually used by governments and which the FBI has stated they use, is to use Spyware to track various situations in which they cannot wait to act, be it cases such as bomb threats, evidence of guilt, harassment, intimidation, and even the leaking of information from governments themselves. [7]

How does spyware work?

Fig. 1. A graphic that represents in an artistic way what the user does not see when suffering vulnerabilities behind the computer screen.

A Spyware has a quite punctual operation, this because by a simple mistake like introducing unknown hardware to our computer this could be attacked by this software, starting first by granting permissions without the user realizes, this to know all the movements that a person has within your computer site, then once inside the computer, the spyware begins to collect and extract as much information as possible (Numbers, etc.), cards, videos, photos, images, histories, messages, screenshots and others). As mentioned before, this has a very specific operation, which is the filtering and theft of all the information that can, but we must also consider the side effects that this can have. Since Spyware works as a scanner that always performs its action, this could slow down the infected computer, so as a side effect of being infected with Spyware can be a considerable decrease in the performance of the user's computer. [8]

Types of spyware

Currently there are different types of spyware, this time we will present some of the most common spyware of which have been recorded. They are ordered according to the impact they have had on the user [9].

Cookies and web bugs

Cookies are small pieces of data that are stored on web servers. Because many websites use the same advertising provider, they can have the ability to study the behavior of users on many web pages. On the other hand, web bugs are described as unseen images found on web pages and are used to locate a connection between a specific website and an end user. They are related to cookies in that they often contract with website owners to install these bugs, but because of the way they are used, they are considered purely passive forms of spyware [9].

Adware

Software in charge of displaying advertising that adapts to the activity that the user is doing, in most cases these adware programs only show commercial content, some that are modified are dedicated to informing third parties about the aggregate or anonymous user behavior [10].

Tracks

This is a generic name given to information recorded by an operating system or application about actions a user has performed. Some of these tracks include lists of recently visited websites, searches, forms, lists of files and programs installed on the user's system.

Browser hijackers

This spyware program is responsible for modifying the home page, search functions and some other browser settings. These hijackers that usually affect Windows operating systems, use some mechanisms to achieve their goal which is: install an extension in the browser also known as "browser helper object", to subsequently modify the registry entries of the operating system, also can manipulate or replace browser preference files [9].

Spybots

They are prototypes of spyware, they are dedicated to monitor the behavior of a user, records the activities performed and delivers them to third parties. The information these spybots collect can be the following fields typed in web forms, list of email addresses that are collected for SPAM, and lists of URLs that the user has visited. Spybots can be installed as a browser helper object [9].

Malware

It is a set of instructions that are executed on a computer and make the system do things that the attacker wants it to do. There are a wide variety of malicious software including viruses, worms, and Trojan horses [11].

Rats (remote administration Trojans)

It is a case of malicious program that is presented as an attachment in emails which attack taking advantage of the weaknesses of Microsoft or some operating system to be installed, after that have another objective which is to activate utilities installers that monitor and control the user's computer for purposes that can become very mild as those of redirecting a website to another or very threatening as the production and transmission of spam email mass email [12].

Spyware Symptoms

A user who manages his computer can detect that something is wrong, as the speed and power of the computer decreases a lot. Programs and executions are becoming slower and slower, and crashes and freezes are more frequent because of memory overload. Other symptoms that may occur are difficulties in connecting to the Internet or changing the home page to a commercial site. As we know viruses and worms cause very serious damage to computers, spyware uses resources and lowers the performance of computers where it is also confused by viruses [13].

This type of software, as well as viruses are analyzed by people and companies to detect them and create processes for their elimination. If someone suspects that a computer is infected with spyware, they report it to a computer technician or contact an antivirus provider, however it is difficult for a user to know who to report spyware to [14].

How to prevent Spyware

One of the main culprits of spyware transmission is free software downloads that are done over the Internet. Therefore, if you choose to download applications over the internet you should be aware that the license agreement included with the software will indicate that the company providing the software has the right to monitor your use of the application to collect information for certain purposes [12]. Therefore, there are a few ways to protect yourself:

- Avoid downloading free software that you are not familiar with.
- Do not download software, if you are not willing to examine the license before executing the download.
- Maintain a high degree of awareness of the state in which your computer operates.
- Integrate a spyware monitoring and tracking program into your computer, just as you do to prevent viruses.

Results and discussion

After the research we did, we came to understand that spyware is a software which is responsible for recording the activities of a user to give them to third parties, so they can affect the user. This type of software can be in each of our computers collecting information, that is why we must take appropriate measures that were mentioned above to prevent spyware.

Many times, we have thought that the activity we do on our computer, or the activities carried out by companies are private. Now we understand that all the time we can be monitored by any of these software's either by cyber criminals or who knows by the same governments of each country to control us.

Conclusions

With the advancement of technology, spyware will continue to increase and improve exponentially to damage many computer systems controlled by malicious agents. As mentioned in the document, spyware is one of the most dangerous malwares which has the ability to record the activity of any infected device in addition to reducing the performance of computers, which is a very negative aspect for users and companies, since this would imply an expense in what is maintenance and repair of equipment and in very extreme cases very large losses of money due to the theft of information. It is important that people read the terms and conditions of the software they are going to use in detail and avoid the use of illegal or cracked software as much as possible.

In this work we carry out an investigation on spyware, where we mention the operation, the types, the consequences of its infection and some basic ways of its prevention, in order that the readers can understand in an easier and faster way what It is spyware so that they can protect their devices and companies to avoid very serious problems that could affect the future of the person or company.

References

G. Maclachlan, «Scandal, Spyware and Trust», Infosecurity, vol. 8, n.o 5, p. 45, sep. 2011, doi: 10.1016/S1754-4548(11)70071-7.

S. Hinde, «Spyware: the spy in the computer», Comput. Fraud Secur., vol. 2004, n.o 12, pp. 15-16, dic. 2004, doi: 10.1016/S1361-3723(05)70185-8.

S. S. M. Chow, L. C. K. Hui, S. M. Yiu, K. P. Chow, y R. W. C. Lui, «A generic antispyware solution by access control list at kernel level», J. Syst. Softw., vol. 75, n.o 1-2, pp. 227-234, feb. 2005, doi: 10.1016/j.jss.2004.05.027.

I. Grigg, «"The Internet is not secure enough for online " banking», p. 2.

S. Mathieson y E. Dallaway, «Kiwis decided identity cards will not fly», p. 1.

D. Forte, «Spyware: more than a costly annoyance», Netw. Secur., vol. 2005, n.o 12, pp. 8-10, dic. 2005, doi: 10.1016/S1353-4858(05)70312-3.

P. Hunter, «FBI spyware admission opens can of worms», Comput. Fraud Secur., vol. 2007, n.o 8, pp. 14-15, ago. 2007, doi: 10.1016/S1361-3723(07)70104-5.

T. F. Stafford y A. Urbaczewski, «Spyware: The Ghost in the Machine», Commun. Assoc. Inf. Syst., vol. 14, 2004, doi: 10.17705/1CAIS.01415.

B. C. y A. J. Martin Boldt, «BoldtCarlssonJacobsson.fm _ Enhanced Reader.pdf». BTH, Ronneby, SUECIA, p. 16, 2004.

A. R. GARCIA MONGE, «Seguridad Informáticay el Malware», pp. 1-11, 2017.

Stefan Saroiu, Steven D. Gribble y, y Henry M. Levy, «Documento técnico NSDI '04», Medición y análisis de software espía en un entorno universitari, mar. 22, 2004. https://www.usenix.org/legacy/events/nsdi0/tech/full_papers/saroiu/saroiu_html/ (accedido nov. 06, 2021).

A. Gorlin, «The ghost in the machine», Surrealism Archit., n.o May 2014, pp. 103-119, 2004, doi: 10.4324/9780203339541.

T. Shelton, «Information technology», Sci. Soccer Second Ed., vol. 20, n.o 5, pp. 276283, 2003, doi: 10.4324/9780203417553.

R. Sellers, «SPYWARE –An Evolution in Process», vol. 4, n.o Security 401, pp. 1-30, 2002.