International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Delivery Methods of Spyware and its Counter Measures : A Review

Rajiv Makwana[*1], Ravi Sheth[2]

[*1]M.Tech, Department of IT & Telecommunication, Raksha Shakti University, Ahmedabad, Gujarat, India
[2]Asst. Professor, Department of IT & Telecommunication, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

Malware became the major issue for the industry and everyday new samples come ups with different method and technology. Each day the anti-virus industries collects the new malware and the job of security expert becomes more challenging. This paper will briefly introduce malware types and emphasis on the spyware which is not so harmful but performing crucial part as loader for other malwares for getting into system to perform malicious and dangerous activities.

Keywords : Spyware, Trojan horse, Ransomware, Ad-ware, Virus, Rootkit, Worm, Crypter, Active X

I. INTRODUCTION

Malware is a computer program which is created to infect computer and cause damage in many ways. Malware creation is became very popular because by creating new types of malwares money making is became easy through organize internet crime. Computers and devices can get infected by malware in tons of way as they have multiple forms. Malware can damage or it can disable whole system or gives full or limited control of system to the creator. It's not easy to differentiate the useful software and the malicious software but it's necessary for user to identify them. Malware has many types we will see brief introduction of them. [1]

II. TYPES OF MALWARE

1) **Rootkit:** The name rootkit derived from the Unix terminology for the admin account called "root" and "kits," which is the software use to apply tools. The tool helps the hacker to hide the malware in a way that the anti-virus can't differentiate the important file and the file which has harmful code. Rootkit itself is not harm-full but they hides harm-full executables. [2]
2) **Trojan horse:** Trojan is malware which is camouflage itself as useful software. Trojan is used by hackers and attackers to get into the remote system. Generally the users become victims by some sort of social engineering into loading and executing Trojans on their machines. Once the trojan is get on victims system keeping eyes on victim's machine and stealing of your data is became way more easy for attacker. The trojan can used as backdoor to access machines in future.[3]
3) **Ransomware:** It's a malicious code used to block access of computer system and demand ransom to release the controls. WannaCry, Petya, Cerber, Locky and CryptoLocker are the ransomware which have made high impact. [4]
4) **Ad-ware:** Advertising malware or adware is used by hacker to present unwanted advertisement using intrusive and at times dangerous methods for making some cash from business. It can generate infinite pop-ups, consume your data, can spy on activities, slowing down your device.[5]
5) **Virus:** Virus are aimed to spread them self from system to system and it can generate clones. The virus cannot regenerate or spread without file or document. The virus will inject itself into other programs like files or documents which has

functions like macro using which they can execute the code. [6]

6) **Worm:** It's a stand-alone code that can duplicate itself without and spread on network. Once it get into your system through network or as downloaded file, it can replicate itself and propagate into other systems and servers connected on the network which has applied weak defensive technique. As each copy of worm is capable of replicate itself worm can spread faster than any other malicious code.[7]
7) **Crypter:** Crypter is a first layer of defence for the malicious core. They camouflage them self as harmless program to protect them self from pattern or behaviour base detection tools and then decrypt the malicious code.[8] They use icons and meta-data of famous products to make the malware as legitimate software. The attackers use it to mask the malicious code they want to send.

III. WHAT IS SPYWARE?

From above all purpose-built malware spyware is dangerous because of its hard to detect. Spyware is dangerous because it won't harm you directly rather doing that it will keep watch on your activities like silent spy and send your personal data to attacker which used to plan long term attack on specific victim. It gather information from victims behaviour of surfing, browsing history, or personal data (like financial details), and share those information to attacker through internet while keeping victim in dark.[9] Spyware can use your webcam, microphone to collect the audio and video data. In this paper we will focus on spyware.

3.1 DELIVERY METHODS

1) Social Engineering banner ads

There are website which use banner ads which use advertising pictures but most of the banner are misleading. Few of them use images which look like windows message box showing critical content and ask user to click. User redirected to other site soon they click on image it start installation of malicious software or redirect to further web pages.

2) Drive by downloads

In drive by download the users get request to install the program unknown to them and it's performed by automatic web page refresh and Active X control installers.

3) Automatic refresh

When web page performed the redirection of browser to using the EXE which can prompt the dialog box it refresh the web page automatically. To perform redirection like this simple HTML or JavaScript is enough. The IE prompts warning to user indicating application contains malicious code and this trick may use on each program the user wants to download, therefore the user learned to ignore those messages and 'Run' the program.

4) Active X

ActiveX controller provides dynamic content in static HTML page. The message prompt to install ActiveX controller to view the dynamic content. Instead of giving dynamic content it's used to mislead user to install spyware program. Delivery through ActiveX is reliable than other as it gives text control of install prompt to vendor allowing them to write anything in message box to mislead user.

5) Bundled and chained install

In this technique malicious programs are wrapped with third-party software. There are some software which notify user that following software are going to install. Some of software write details of bundled programs in license agreement. Once bundled program installed in victim's machine it download additional malicious programs without informing user this method is known as chained installs.

6) Peer to peer installation

In this method spyware are seeded on P2P networks file with appealing name may contain the spyware and it also bundled with pirated media like TV shows, games, movies.

7) Exploits

The exploits of web browser is used to spread the spyware like IE browser has vulnerability it allows content to be download and execute automatically while user stays unaware of it.

3.2 HOW TO PROTECT

1) Use spyware scanner

Applications are available which provides active protection, detection and removal of malicious programs and free for personal use. Few of them will

detect internet cookie and inform user which websites they refer back to.

2) Use pop-up blocker

Browsers of current date can disable all sites from generating pop-up windows. User can active this functionality for life time or configured in such a way that it generate alert whenever sites wants t serve pop-up windows. It can tell you origin of pop-up and reliability of its source.

3) Disable Active-X

Disabling ActiveX from web browser will definitely protect you from spyware which can take advantage of these technology to spread themselves. It is true that it also disable genuine use of Active-X.

4) Think before installing new software

Do not install any extension or plug-in you are unaware of unless it is necessary for you. Installing plug-in after getting some background information is the best practice to protect your machine. Once you find out it's safe to install then go for it.

5) Use "X" to close the pop-up window

Get familiar with you system message box how they look-alike this will help you to differentiate the original and fake message box. Use 'X' placed in right corner to close the message box. It would be more secure if you use keyboards short cut keys to close the message box.

3.3 EXAMPLE OF SPYWARE

A. Pony

Pony steal all type of data from the system infected by it. These machines became the part of botnet and the acquired data were sent to hacker which can be further used to access the victim's machines with the higher privileges and he/she can view the data by logging into an administration panel.

Pony is a credential harvesting portion of malware with other trojan capabilities. The purpose of pony is data collection but it also used as malware loader to infect systems with additional malware in multi-stage infections chains.

Involvements

1) **Feb 2014:** Involvement found in $200K in different digital currencies and over 700000 login IDs and passwords are stolen.
2) **Dec 2015:** A group of cybercriminal used pony with angler exploit kit and CryptoWall ransomware.
3) **Jun 2016:** Involvement found in delivering the RAA ransomware variant. [10]

B. CoolWebSearch:

It includes variety of browser hijackers. Code of version is different but they all used for redirecting user to CoolWebSearch and websites associated with its operators. [11]

One from many disreputable hijackers known to date which has variety of versions, and they all use different methods.

Properties

1) CWS will add others software linked to the server to generate extra money.
2) It may change settings of security software.
3) Add itself in start-up for auto start.
4) It will change browser setting like changing the home page of browser to CoolWebSearch.com
5) It may use internet without informing user.
6) CWS used to show ad on user screen through pop-ups.

C. Zbot (ZeusV3)

The ZeusV3 is designed to gather victim's banking credential and capture e-banking session while remaining invisible to virus detection tools. It use SSL protocol to remain undented while communicating to its creator.

It steal amount from the accounts with balances of higher than $1000 and hide unauthorised withdrawals by redirecting the victim to fake web page.[12]

D. Look2Me

Rather than calling a virus Look2me is more like platform for downloading other virus and trojans adware/spyware components. On every start-up the program contacts a server and it downloads many malwares and its components which can automatically install them self and causes more damage than the actual application. Eventually the victim's computer becomes unstable. [13]

Detecting it is hard as there's no process to locate or identify plus it has some rootkits properties. It can run itself in safe mode. The IT companies called them PUPs Potentially Unwanted Programmes".

Look2Me use for making money from business advertisement by redirecting the traffic to victim's computer but using this program hackers may find the way to install potentially harmful programs in victim's machine which makes these kind of program dangerous. Downloading software from sites which provides their own setup and .exe files to download specific software setup is become reason for getting your system infected.

IV. CONCLUSION

In this paper, we have seen malware and its type. Brief introduction of spyware, few infamous spyware samples, methods they apply to spread themselves and remedies to protect our system from them. However, sypware is not so harmful but necessary precaution is required as it make your system open for other dangerous malwares and breach your privacy.

V. WEB REFERENCES

[1]. https://usa.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it
[2]. http://www.pctools.com/security-news/what-is-a-rootkit-virus/
[3]. https://usa.kaspersky.com/resource-center/threats/trojans
[4]. https://www.avast.com/c-ransomware
[5]. https://www.avg.com/en/signal/what-is-adware
[6]. https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html
[7]. https://www.kaspersky.co.in/resource-center/threats/viruses-worms
[8]. https://blog.malwarebytes.com/threat-analysis/2015/12/malware-crypters-the-deceptive-first-layer/
[9]. https://www.kaspersky.co.in/resource-center/threats/spyware
[10]. https://www.cyber.nj.gov/threat-profiles/trojan-variants/pony
[11]. http://www.spywareguide.com/spydet_599_coolwebsearch.html
[12]. http://www.computerweekly.com/news/1280093514/Zeus-v3-Trojan-draining-more-than-675000-from-UK-bank
[13]. https://look2me-remover.en.softonic.com/
[14]. https://www.symantec.com/avcenter/reference/techniques.of.adware.and.spyware.pdf
[15]. http://how-does-things-work.blogspot.in/2010/01/working-of-spyware.html