Volume 4, Issue 5, May-2017, pp. 176-179 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Malware as a Component in Cybercrime: A Survey

Rodney Anthony Raj[1], Chayapathi A R [2]

[1]*Student, Information science and engineering, Acharya institute of technolgy,_ Doctor Sarvepalli Radhakrishnan Rd, Bengaluru, Karnataka 560107, India.*

[2]*Assistant Professor, Acharya institute of technolgy,_ Doctor Sarvepalli Radhakrishnan Rd, Bengaluru, Karnataka 560107, India.*

Rodney.mtcf.15@acharya.ac.in[1], chayapathiar@acharya.ac.in[2].

Abstract:-In today's world we face lot of trouble by cybercrimes where every individual by some mean is a victim towards cybercrime knowingly or unknowingly. One of the main components in the cybercrime is malware and it really comes handy to wage an attack. This paper is a survey on what kind of malwares are used and how effectively they use malware to exploit the world through cybercrime.

Keywords: Malware, Ransomware, Virus, Cybercrime, Rootkits, Attacker, and Hacker.

---

1. Introduction

A malware is a software/program/code which enters system without user authorization and takes unsolicited actions. The term is frequently used instead of virus, even yet the two are not the same. Malware is actually a summarized, adjoined term used to refer viruses, worms, Trojans, spyware, adware, rootkits, botnets etc. In today's computing world malwares are a big threat and are endlessly growing with high complexity [2]. With this growing nature of malwares where it's being the number one threat for all users over the World Wide Web. Nowadays we have so many malwares created where many sites contain potential malwares and we become victim to those malwares and many of us even without our knowledge would be part of many attacks as our machines are turned into botnets to attack webservers, data centers, or breaching information.

Cybercrime is a generic term for using this (malware) for attacking and not only malware there are many other aspects involved but, we are focusing on the malware as main component which leads to devastating actions [1]. Systems are so affected with malwares, which are so intelligently built where it's not even detected by Antivirus software. So, to achieve all this attacker does exploit our network or they try to pull layman by sending some unwanted links which seems to be very lucrative. For example, messages saying you have won one lakh and followed by a link which potentially holds the malware. We've to fight against these adware and educate people with some basic security tips which would help them gaining some knowledge [3].

So, malware is basically a super weapon in the hands of cybercriminals where they do use it to the highest potential they can and this all starts with our basic stupidity [2].

2. Types of malware

Malwares were evolved certainly as mentioned below, where they were of stealth and no stealth. Where stealth attacking malwares are the one which causes more trouble. The below mentioned are some basic malwares which can be used to its full potential.

Viruses, these are the basic malwares where a piece of code written to spoil the work of a system and spoil the system.

Worms, are impartial malicious software that can activate autonomously and don't catch itself to proliferate.

Rootkits, are the concealing techniques for malware, basically designed to conceal the malevolent intent of the program from the antivirus deduction programs

Botnets, a network of isolated computers infected with malicious software and meticulous as a group without the proprietor's awareness. Authors are responsible for obtaining any security clearances [7 8 9].

3. Malware in Cybercrimes

In this section, let's take a look at how the use of malware in cybercrime is increased with the stats available and the tests run by many antivirus companies and the labs which conduct these tests to know the present usage of malwares in real life.

Kaspersky lab detected 3,626,458 malicious installation packages in their Q2 2016 quarterly test, where the Kaspersky run these test every quarter to keep track of malware being generated. Where they claim it to be 1.7 times more than the previous quarter test [12].

AVTEST, an independent IT-security institute which works on malware and malicious contents claim these below stats for the past 10 years and the growth of malware are shown in the grap [13].

The graph shows us how the malware have their impact on cybercrimes as one of the main and weaponized component for attackers. To showcase this we can consider a real incident where the hackers or attackers weaponized everyday devices such as webcams and DVR's to create a botnet and to rage an attack on multiple popular sites by performing a DDOS attack [11].

To support this we have a blog with the stats of growing malware and the troubles faced by companies and the growth in malware shown in (figure 1).

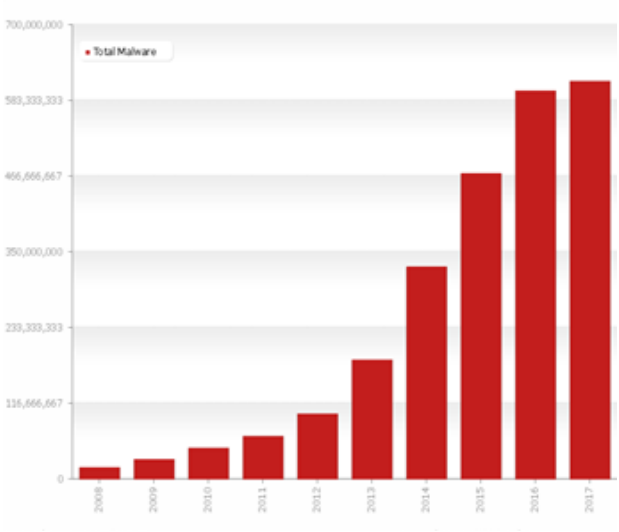

Figure 1: Stats showing the growth of malware every year.

In Q3 of the year 2016 alone there were more than 18 million malware's were identified by a single company alone that's almost a 200,000 malware's a day 6. Many of the industry faced almost a 4000 ransomware threats and still haven't taken any action against preventing these threats. Many users claim even though they know the link is malicious and still they click on it. There are many industries where they were under attack and even then they're not ready to implement or improve their security features [5].

So, we do see such a rise in modern world technology where we are bitten by malware and say that 90% devices in world are infected by malware at least once. Ransomware and cyber espionage are continuing to steal the user data and especially with transactions made through devices. This will increase as the growth in malware increase [9].

To make our understandings more clear let me give out an example where my example covers 4 types of people. A layman, techie, manager, and security analyst. Considering all of them coming across a malware and the way they react and before coming across a malware how do they even know it's a malware should be our question? But, not many are aware and even when aware they don't seem to be stop clicking or opening the link or site. Let's add another person to the above list and call him a hacker and he's somehow try and interrogate with all of the above.

Firstly, hacker sends a mail to the layman saying he has won a cash price of some random amount and tells him to follow instructions provide in the below link and a happy layman who wants to earn some amount through lucky dip clicks on the link and the hacker meanwhile the layman trying to read instruction deploys a rootkit

and takes over the control of the machine and this rootkit gives the hacker all access to the machine and deployment is done in such a way even if the system is resstarted the rootkit runs as a background process and comes up when booted. So now the hacker has a complete control over the machine.

Secondly, the techie falls into a trap which was created by a hacker. Where the hacker has created a blog which gives solution for coding and issues faced by machines. Where the blog is so useful the techie gets all his answers and falls into a trap by blindly believing the blog so much where any posted content and media is downloaded and installed. The installed media will be the rootkit for the hacker to get a permanent access to that machine in using it for a future attack.

Thirdly, the manager or management this is where the real attacks break in as now writing this I've acquired a little knowledge working in a company the management level people never bats an eye for these kind of issues for them security is at the last and they never react until and unless there's a problem. These people just install stuffs without reviewing and they'd even demand an environment where their workstation shouldn't stop adding software or any other stuffs. This is where the problem lies.

Finally, security analyst where in real time is not just an IT person. In real an analyst has to analyze things before hand by reviewing the possibilities of a malware or virus or say anything which affects the network or system. This will be the main observance and concern of an analyst. This is where he/she could be handful in working against odds.

The above example shows how much we require a security analyst for each and every company but which isn't the current situation. There are companies still think why do they need to pay extra for another employee and make their IT to deal with security. This leads to the havoc of the networks by these killer malwares. This is a made up story to make our understanding better [4 10].

4. Protection or Prevention

Here I hit out the question whether we should prevent or protect our network from malware? It is a quite complicated question because, we can either protect or prevent we can prevent by adding security features and protect by appointing a security analyst. Now that security is the buzz word running there's more attackers on the verge. Prevention and protection are both coexistent and should be handled with utmost care. The prevention should be our goto because we can't miss the data's and loss of data is purely inevitable. We can prevent by using proxies and we must evenly concentrate on protection by having antivirus or malware scanners. We can even run network vulnerability scanner and follow strict patch management and where we shouldn't be the cause for vulnerability where it can be exploited by payloads using tools or scripts. Being aware is also a protection.

5. Conclusion

In this paper, I conclude malware are the biggest threat in security and cybercrimes. So, we have to be more concentrated towards malware and act accordingly before the attacker strikes. The companies should acknowledge this by taking more serious steps in alerting people and by taking right initiatives. It's always better to build a shield before an attack and now there are many cyber security professionals who can help the company in coping against the cyber assault. The company should start with awareness program on cyber security and should deploy policies where the outside network never interacts with the inside, put on the latest firewall with access policies and better to cover up the company website with a cloud proxy as many attacks initiate from website which leads to the company internal network. It's even better if the website a general purpose site to be hosted on an isolated network and not putting many detailed information of people who are part of the company which can ultimately lead to social engineering. So, as we take a lot of care towards security the safer we are.

6. References

1. 2016: Current State of Cybercrime, RSA whitepaper.
2. Basic survey on Malware Analysis, Tools, and Techniques. Dolly Uppall, Vishaka Mehra, and Vinod Verma.
3. A survey of cybercrime. Zhicheng Yang.
4. Detecting and Classifying Morphed Malwares: A Survey, Sanjam Singla.
5. Evolution, Detection and Analysis of Malware for Smart Devices Guillermo Suarez-Tangil, Juan E. Tapiador, Pedro Peris-Lopez, and Arturo Ribagorda.
6. A Survey on Techniques in Detection and Analyzing Malware Executables, Kirti Mathur.
7. Malware Analysis and Classification: A Survey

Ekta Gandotra, Divya Bansal, Sanjeev Sofat.

8. Malware and cyber crime. House of Commons, Science and Technology Committee.

9. Malware and Malware Detection Techniques: A Survey. Jyoti Landage.

10. A Survey on Malware Attacks on Smartphones Kireet, Dr.Meda, and Sreenivasa Rao

11. https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault

12. https://securelist.com/analysis/quarterly-malware-reports/75640/it-threat-evolution-in-q2-2016-statistics/

13. https://www.av-test.org/en/statistics/malware/

14. https://blog.barkly.com/cyber-security-statistics-2017.

