INTERNATIONAL JOURNAL OF ADVANCED STUDIES
IN COMPUTER SCIENCE AND ENGINEERING
IJASCSE VOLUME 6 ISSUE 9, 2017
09/30/2017

# Testing the security products against next generation malware

*Manusankar C*
Head, Department of Computer Science, SSV College
Research Scholar, Mahatma Gandhi University

*Dr. Vargheese Paul*
Professor Department of IT, SOE CUSAT
Research Supervisor, Mahatma Gandhi University

***Abstract*—The recent attacks in the cyber world is really a night mare for the users as well as the security product companies. Even-though these companies claim that the systems in which the infections affected were not having the up-to date security products, we cannot agree with them completely as we had tested several products with new infections and the detection rate was not up to the mark. This paper presents the results and findings of Sec-Test Auto in the next generation malware scenario. This work is a real time testing with WannaCry and Petaya malwares and other malwares with a Virtual testbed( SecTest Auto) created by the author for testing various Security products.***

***Keywords-SecTest Auto; Ransomware; Malware; WannaCry; Petaya; Virtual Testbed;***

## I. INTRODUCTION

The world started to know more about the ransomware after the WannaCry attack of May 2017. Even if ransomware attack was first recorded in 1989, the "AIDS Trojan" created by Joseph Popp, we would like to consider this WannaCry and other ransomware attacks as a next generation malware as the impact which these ransomwares created among the computer users across the globe was very high. So in this work, we are going to consider all the significant malware attacks during 2017, till July. Our application SecTestAuto analyzed the effect of all the new available malware on various security products. Based on these analysis we would like to propose some measures to limit the attacks in the near future.

### *A. Ransomware*

Ransomware can be any set of malicious programs which can convert the data into unusable format and then ask for a "ransom" or money, which nowadays takes the form of bitcoins, so as to make the data usable again. The recently used ransomwares are WannaCry, CryptoLocker and Petya. All three ransomwares made use of vulnerabilities inside MS Windows Operating System. The common malwares which can be considerd under the ransomware category are [3]

- WannaCry
- CryptoLocker
- Petya
- Apocalypse
- Bab Block
- Bart
- Crypt888
- S2FLocker
- TeslaCrypt
- PetrWrap

*1)* How it commonly works

As mentioned earlier, commonly the ransomwares make use of the operating system vulnerabilities to enter the system. Upon entering the system, it will search for the user files and documents and will start encrypting them. After this process, all these ransomwares will commonly opt for a system restart. Upon restart, it will take over the usual desktop application and will instead display a warning message mentioning files are encrypted and asking for ransom. The methods will slightly varies for different ransomwares.

*2)* WannaCry

Unlike the common ransomware spreads, the WannaCry incorporates the worm elements together with the common method of email infection. These worm elements are responsible for the widespread of this attack. The worm element will also help WannaCry to infect the network of the affected computer. As we have heard in the news that it was to be considered as a zero day threat as the vulnerability showcased by the shadow brokers were being used.

*3)* Petya

Uses the same eternal blue vulnerability of the Microsoft OSs. This has an additional feature of automatic reboot after the infection and also uses more than one method to spread infection which makes it more dangerous.

The Antivirus software makes use of several methods for detecting infections, they includes

- Signature Based detection
- Heuristics based detection
- Sand Box or Behavioral based detection

Signature Based techniques[1], traditionally used by AV scanners, can be used for detecting primary file components

such as the executable components of a threat. However, this technique is not necessarily the most suitable for detecting secondary file components,particularly data files, log files, etc. that are subject to frequent, unpredictable changes. In addition it is not always necessary to detect every component directly via content scanning, since once the scan has determined that a particular threat is installed there are more efficient meth- ods, such as the context scanning technique discussed below, for detecting the remainder of the threat.

Contextual scanning techniques[1], more commonly relied upon by dedi- cated anti-spyware solutions, provide a method for detecting threats based on the known presence of a particular set of entries on the system being scanned. This method uses rules such as combinations of names Context scanning is not the most effective or practical technique when used on its own. For example,this scanning technique is not very effective at the gateway where no installed con- text rules can be applied. There is also the complication of making a positive identification of a particular threat, where common file names or registry en- tries are being added or modified, leading to non-specific reports such as,'this file and these registry entries are suspicious'.There is also a greater risk of false positive reports,particularly when relying on individual component attributes such as the names of files or registry entries.

## II. SECTEST AUTO TESTING

The most efficient way to test the effectiveness of any security product is by bringing in the real threat to the system. This same method was used in the work. We made use of our test environment SecTestAuto to deploy the actual ransomware in to the system. The ransomware source, available online by the fellow researchers were used for this work.

Several test case scenarios were used including different types of windows operating systems - both before and after the security update. Surprisingly, no infections were affected after the system update. So we reinstalled the OSs and used the antivirus products released in 2017 without the update.

### *A. Procedure used*

The procedure used in the testbed [1]

1. Manually install the AV program of user's choice
2. Temporarily deactivate the AV to use developed test-bed.
3. Infect the system with known and unknown (no-key) malware (auto)
4. Use our custom scan to check if the malware was detected
5. Restart the OS in the Virtual Machine
6. On demand scanning is done

Apart from testing the regular AV products, we also introduced the ransomware specific security products to our environment which showed and increased level of detection but these products were not functioning satisfactorily with the ransomwares outside their scope analysis ie with newer versions released at the time of research.

As mentioned above during the time of our research, several new ransomwares were released. These malware were also used to test our systems. Due to this, apart from our usual automatic method of product testing, we were forced to add a manual approach as we have to place new infections into the system. The manual approach helped us a lot in creating a very good test case for new infections so that the effectiveness of the security products can be clearly studied.

## III. ANALYSIS AND RESULT

The actual ransomwares were selected in such a way that the antivirus software has to do the content scanning, context scanning, and behaviour scanning. A variety of ransomware samples were used as each uses different methods to infect the systems. Some old type of ransomwares were also analysed and used for testing in the initial stages and while proceeding further it seems to be redundant and most of the AV softwares detected them.

The main problem when dealing with ransomwares was that when the protection was compromised or testion framework was also not abe to fetch the results, in those special cases we had to manually check the performance and had to restore the system back.

When the system was uptodate almost all the ramsomwares were not able to compromise the security provided by the most antivirus vendors but new infections still possed some threats.

## IV. CONCLUSION & FURURE SCOPE

Our work revealed that all the big players in the AV industry are very well equipped after the WannaCry attack, but in some rare test cases they failed. The products which were not updated showed an increased flaw in avoiding them and in some cases even detecting the infection. All the ransomware specific products were successful in preventing those specific ransomwares.

Currently for this work we only considerd the windows specific ransomwares, in future we would like to consider ronsomwares in other platforms as well. So while concluding this work and considering the history of ransomwares, we would like to say that security products should also evolve a mechanism to find the vulnarabilities ot its platform so as to avoid the future threats.

## ACKNOWLEDGMENT

The authors would like to thank the Director School of Computer Sciences and here team for all the support through out this research. The authors would also like to thank the Administrators of SSV College and CUSAT for all their help and support throughout this research. This work was completed only because of the grace and blessings of God Almighty and with the support of our families.

## REFERENCES

[1] *C Manusankar Dr. Vargheese Paul "SecTestAuto-An Improved Virtual TestBed for Testing AntiVirus and other Security Products" International conference of cyber security (ICCS) 2016 from Aug 13 to Aug 14, 2016*

[2] "ICSGMalwareWorkingGroup."http://standards.ieee.org/develop/ indconn/icsg/.

[3] "AVG Ransomware Decryption" https://www.avg.com/en-in/ransomware-decryption-tools

[4] Manusankar C, Dr. Vargheese Paul, "Improved Virtual Test Bed and Testing Strategies for Antivirus and other Security Products" in International Journal of Inter Diciplinary Research in Computer Science Volume 1 Issue 1

[5] Haffejee, J.,Irwin, B., "Testing antivirus engines to determine their effectiveness as a security layer" at International Conference on Information Security for South Africa (ISSA), 2014

[6] R. Harrison, "The antivirus defense-in- depth guide." http://www.bitdefender.com/files/KnowledgeBase/file/Antivirus Defense-in-Depth Guide.pdf.

[7] K. R. Straub, "Information security managing risk with defense depth."http://www.sans.org/readingroom/whitepapers/infosec/information-security- managing-risk- defense- in-depth- 1224 .

[8] "The history of Ransomware" https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

[9] Alexander Volynkin& Victor Skormin, "Large-scale Reconfigurable Virtual Testbed for Information Security Experiments" at 3rd International Conference on Testbeds and Research Infrastructures for the Development of Networks and