Advanced Engineering Days

aed.mersin.edu.tr

A simple mechanism for controlling and reducing malwares at network level, preventing possible cyber incidents

Vilma Tomco [*1], **Miranda Harizaj** [2], **Argena Prendi** [3]

[1]*University of Tirana Faculty of Economy, Albania. vilma.tomco@unitir.edu.al*
[2]*Polytechnic university of Tirana, Albania. Miranda.harizaj@upt.edu.al*
[3]*National Authority for Electronic Certification and Cybersecurity, Tirana, Albania, Argena.prendi@cesk.gov.al*

Cite this study: Tomco, V., Harizaj, M. & Prendi, A. (2022). A simple mechanism for controlling and reducing malwares at network level, preventing possible cyber incidents. 5th Advanced Engineering Days, 57-59

Keywords
Malware
Traffic monitoring
Cybersecurity

Abstract

Cybersecurity is become the most important issue in the new geopolitical situation, and the consideration about cyberwar as the fifth domain of the war is confirming everyday this definition. The increased rate of public services digitalization, the increased usage of internet access and online services in one side has made easier the life of citizens and businesses but in the other side has become the paradise for cyber criminals, hackers, hacktivism and also for cyberattacks towards countries and regions. Considering that prevention and detection is the most important part of defense capabilities, all national cybersecurity are investing on building cybersecurity capacity (including technical infrastructure and human resources skills as well as on the awareness). Depending on the financial possibilities that also needs quick intervention and a huge budget, there are several mechanisms in order to support cyber experts to deter and prevent in advance the most possible incidents or attacks. We are trying through monitoring and analyzing the internet traffic information collected to identify and report in advance the possible issues with intention to lower the future incidents.

Introduction

As the work has moved mostly to online environment, also the incidents that previously happened in physical world were transfer towards virtual world. So, the efforts to protect infrastructures and systems in order to detect and prevent possible incidents is become a necessity mostly for the countries that have limited technical capacities. Cybercriminals have intensified their attacks not only towards critical information infrastructures but also towards individuals. The methods of receiving control of their digital equipment's generally are the same: phishing, spoofing, ransomware etc. Through installments of malwares, they gain access to victim information and intent towards main systems or application in order to change information, theft it for selling or asking money or destroy it for creating trouble. Financial sector and other important CII have established their protection systems (intruder's detection systems etc.) and together with implementation of cybersecurity standards at their premises aims to guarantee the protection of system and information. Lots of other companies and individuals are not able to implement such measures and often are target of hackers and becomes a risk for other users on the internet or different networks. Our mechanism aims collection of information from ISP network, analyzing the malwares that are installed at end-users, inform them through communication with ISP in order to reduce the number of infected PC, reducing the possibilities for creating other incidents or attacks.

Result

As we have stressed in our previous research, [1] it is needed a longer period for monitoring, analyzing and notifying the proper ISP to clean up malware-infected end-user computers. This process requires specific tools and we choose information delivered from shadowserver.org. In order to see the results of our work, a better and continuous communication with all internet service providers where needed. In this regard, we use a sharing information platform (MISP) for communication to share information and receive the results. Monitoring of the network has begun on May 2021 with only 2 ISP and we saw a considerable reduce of malwares after sending report with notification to them. It is increased the number of ISP and institution in monitoring process and we try to change the behavior notification.

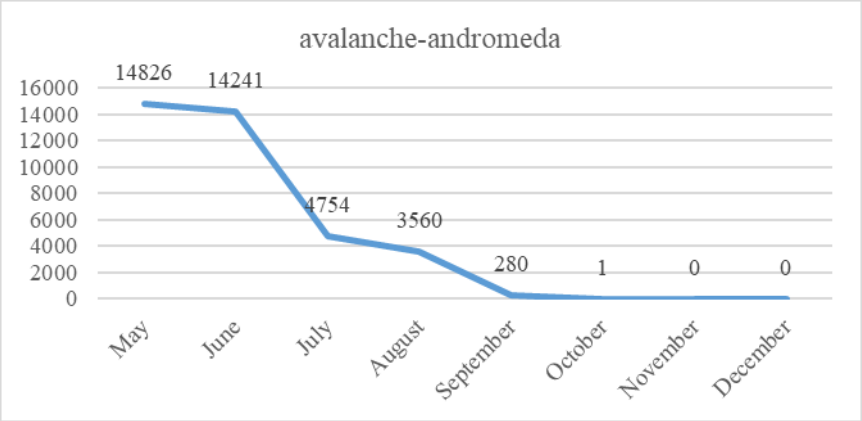

Figure 1. Avalanche – Andromeda Malware reduction – 1 ISP

We monitored all infected IP and existed malware circulated through ISP network. Among lots of other malwares, Avalanche - Andromeda was the virus that has infected the majority of IP's. After one year of regular monitoring/notification process, it results a huge decrease of this malware as well as other malwares. In order to support all expert with quick action in cleaning malwares from their network a recommendation material [2] has been prepared and distributed to all ISP and CII. It is a very important fact that when it was stopping the process of notification, a slight and occasional or significant increase of infected IP was noticed. The second fact, it was noticed that the same IP's results again infected.

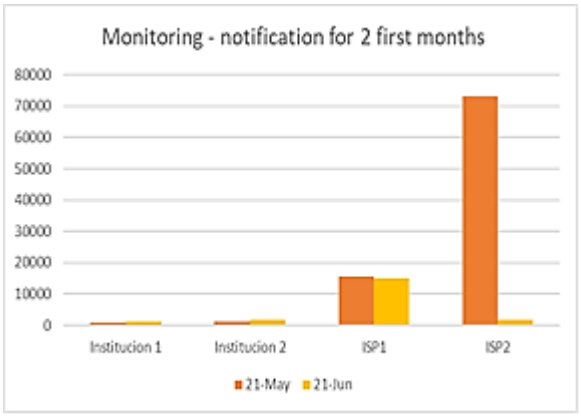

Figure 2. Number of IPs, May-June 2021, for 2 Insitution and 2 ISP (3 without notification**)**

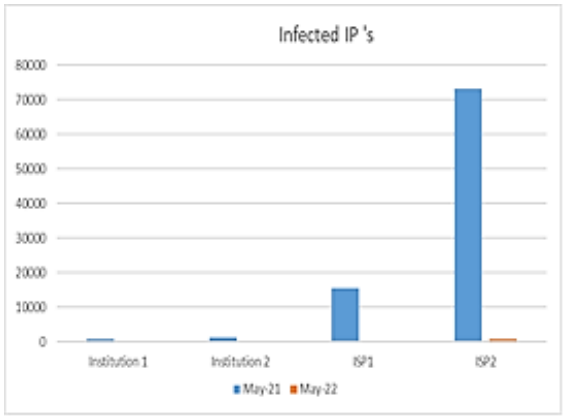

Figure 3. Number of Ip's reduction , May 2021 – May 2022

Discussion and Conclusion

As the result of all this process of continuing monitoring for one year of the internet traffic for infected IP together with malware types, it was notice:

- A reduction when notifications were sent to ISP's and follow up the process of actions were taken from them
- When notification was stopped, a directly increase of the figure of malwares and infected IP's were noticed.

What we can suggest in actual situation, without any injection on establishing cybersecurity tools (SOC's or other system) which requires considerable budget to them, a well define and continues process *monitoring-notification-responding-analyzation* will reduce the cases.

It is a very important fact that when it was stopping the process of notification, was noticed a slight and occasional or significant increase of infected IP. The second fact, in some cases, the same IP's results again infected. It needs more analyzes and monitoring of client behaviors for understanding and preventing happening this fact again.

References

1. Tomço, V., Hyra, A., & Prendi, A. (2021). Monitoring and Notification on Prevention andReduction of Threats and Malwares at Network Level. 1st International Conference in Informationa Technologies and Educational Engineering (ICITEE 21)
2. Wikipedia. (n.d.). *https://en.wikipedia.org/wiki/Fifth_Dimension_Operations*. Retrieved from https://en.wikipedia.org/wiki/Fifth_Dimension_Operation