Threat Intelligence

Improving SIEM cybercriminality awareness using information from IP blacklists

João Alves[a], Ana Respício[b]
a.LASIGE; b. CMAFIO
Faculdade de Ciências, Universidade de Lisboa
Lisbon, Portugal
joaop.talves@outlook.com, alrespicio@fc.ul.pt

Ivo Rosa, Pedro Rodrigues
DSI – Segurança Informação
EDP – Energias de Portugal, S.A.
Lisbon, Portugal
{Ivo.Rosa;PedroDias.Rodrigues}@edp.pt

***Abstract* — Cybercrime activity has been growing over the years and there is no evidence that this tendency will stop in the near future, hence it raises the obligation of the organization's cybersecurity team to strengthen the cybersecurity, to avoid irreversible damages. The use of public blacklists is one strategy to monitor the organization's network to detect suspicious communications, however, the use of public blacklist generates a high percentage of false positives alerts. This paper describes a solution that gathers external information about malicious IP, reported by public blacklists, and organization's internal information regarding security incidents, to calculate reputation scores for external IP and public IP blacklists. The reputation score is used by the SIEM rules to select the type of alert for each IP address to monitor. The objective is to decrease the rate of false positives alerts that are usually generated when using public blacklists. The trustworthiness score will aid the SOC team to select the public blacklists that can be more suitable for the organization cyber context. The presented solution is aimed at enhancing the SIEM's coverage on cybercrime activity over the organization's network. Preliminary results of an application on a worldwide company are presented.**

Keywords—threat intelligence; security metrics; public blacklists; open-source intelligence, security information and event management, cybercrime

I. INTRODUCTION

The cybercrime activity has been drastically raising over the past few years. The number of ransomware attacks increased 300% in 2016, in relation to the previous year [9]. As for bot activity, Symantec observed an increase of 6.7 million hosts in 2016 [8].

Due to this increase, any Security Operations Center (SOC) team must reinforce the cybersecurity efforts to ensure a secure network in the organization and the safety of the assets that communicate over it. One method to detect illegal activity in the network is the continuous monitoring of the network, however, this requires knowledge about the current cyber-threats and vigilance of the organization's communications.

Threat Intelligence (TI) [2] is the process of extracting information about cyberthreats from diverse sources, internal and external to the organization. The Internet cyber security information sources can provide reliable indicators about cyberthreats and constitute external sources, as for instance, public blacklists. These are lists created by communities or organization entities, which reports IP addresses that are suspicious of illegal activity. Some of these lists also provide additional information about the IP addresses, such as the number of confirmed attacks, the type of cybercrime or the last time they were reported. Although the use of public blacklists reinforces the cybersecurity by monitoring the organization network communication, these blacklists provide a significant percentage of false positives [5-7]. The security events collected by the organization provide knowledge about its security status, therefore, constitute an internal source supporting the identification of vulnerabilities that can be exploited.

The platform Security Information and Event Management (SIEM) aggregates all the information about cybersecurity events from various and different type of sources, normalizes it, enriches it and sends it to a centralized management console. The effectiveness of the cybersecurity incident response team on the cybercrime activities depends on the capability of the SIEM to produce detailed and contextualized alarms for real threats.

The solution here presented aims at providing information to the SIEM system, from internal and external sources, thus improving the alarmistic of the SIEM and contributing to the effectiveness of the SOC team when responding to security incidents. We envisage enhancing the security of the organization and improving the combat against the cybercrime. To achieve that, we will integrate the TI process into the SIEM system and do a trustworthiness reevaluation of the external information considering the analysis of security incidents from the SOC team. The TI integration, the continuous reevaluation of the reputation of IP addresses threats, and the evaluation of the trustworthiness of several public blacklists will aid the SOC team to have a finer detection on the cybercrimes that can occur within the organization's network.

II. SOLUTION OVERVIEW: TRUSTWORTHY BLACKLISTS

Our solution has four independent modules, combined into a framework to collect IP addresses that are suspicious of cybercrime from a set of public blacklists, assesses those IP addresses as well as the public blacklists and, monitors the organization's network, alerting the SOC team when there is communication with one of the suspicious IP addresses.

The first module, the *collector*, has the purpose of collecting suspicious IP addresses from a set of blacklists. The program uses the concept of open-source intelligence (OSINT) [4] to search through a set of previously defined public blacklists and gather the reported IP addresses. After the collection, normalization and standardization of the IP addresses, all the collected information is saved and passed on to the next module.

The *assessment* module consists with a set of equations to evaluate the reputation of criminal threat of the suspicious IP addresses and the trustworthiness of the blacklists. The reputation value of an IP address depends on four components. Each component evaluates the IP address with external and internal information, regarding 1) the number of public blacklists that reported the IP address, 2) the presence of the IP address of the last three months, 3) the trustworthiness of the public blacklists that reported the IP address as suspicious of illegal activity, and 4) the precision of the IP address, regarding if is associated with true or false positive cases of the organization. The precision value is the number of true positive cases, divided by the total number of cases that the IP address is associated to. The trustworthiness value of a blacklist is composed by two components: precision and history. The precision is computed as the one of the IP addresses. The history sums the trustworthiness value of the blacklists over the last three months, with a weight associated for each month.

The next module, *Trustworthy Assessment Blacklists Interface (TABI)*, is a web interface management console, allowing the SOC team to manage the blacklists, add and associate incident cases with IP addresses. Finally, the web interface console also illustrates security metrics regarding the performance of each blacklist over time.

The last module, *SIEM rules*, contains a set of rules that selects the suspicious IP addresses to be monitored in a SIEM system considering their reputation scores. The IP addresses with a higher reputation will only require one communication between the organization and the suspicious IP address to trigger an alert, while the IP addresses with a low reputation will require a bigger number of communications to activate an alert. The aim is that these rules will reduce the false positive alerts.

III. Conclusion and Future Work

In our investigation, we did not find any work that used the inside information of the organization to assess the public blacklists, and tuning the blacklists content to select the most relevant for the status of threats in the organization. The two works that are closer to our work are the IntelMQ [3] and AlienVault OTX [1]. IntelMQ only gathers information from public blacklists, with some requirements and complexities. The AlienVault OTX has a community that contains blacklists, however does not assess the information regarding the organization context. AlienVault also provides a public list that only assess the possible level of threat of the IP address using the information provided by the community.

We conducted a study experience at a worldwide company (EDP), in a period of five months using 121 public blacklists. Over that time, the solution started to prioritize the IP addresses that were being reported by the blacklists that had a better trustworthiness score – calculated by the *assessment* module. The score aids the SOC team to have knowledge about the public blacklists that were providing more suitable information about possible threats for the organization.

By maintaining the IP addresses that were continuously reported by the blacklists and that were associated with positive cases (precision), the solution improved the number of true positive cases and led to an increase of 2,57% in precision, when comparing with a list used by the SOC, which includes public and private/paid blacklists.

The *persistence* and the *precision* components are the main factors of the solution's good results, due to its consideration of the internal information of the incidents operations by the SOC team to classify, maintain or discard an IP address. Our solution can support the SOC team to focus on the real cybercrimes that are targeting the organization, by reducing false positives.

The next step of our work is the categorization of IP addresses by types of threats (e.g. ransomware, phishing, trojans), which are associated with different cybercrimes, and use it for the IP assessment. The use of this new component will prioritize the IP addresses related with threats that the organization considers more dangerous. The solution will also correlate the threats with the security incidents cases to alert the SOC team about the cybercrimes targeting the organization. This way, the SOC team can have a better view of threats and allocate their efforts to protect the organization's network against these cybercrimes.

Acknowledgements

This work was partially funded by the DiSIEM project, financed by European Commission in the H2020 program, G.A. No 700692, and by FCT through project UID/MAT/04561/2013. The authors are grateful for the collaboration of Gonçalo Martins.

References

[1] AlienVault (2016). AlienVault Open Threat Exchange (OTX) TM User Guide. AlienVault.

[2] Bromiley, M. (2016). Threat Intelligence: What It Is, and How to Use It Effectively. SANS Institute Reading Room site.

[3] Enisa (2017). Incident handling automation. Retrieved June 27, 2017, from https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation.

[4] Johnson, L. K. (2007). Handbook of intelligence studies. Routledge.

[5] Kührer M., Rossow C., Holz T. (2014) Paint It Black: Evaluating the Effectiveness of Malware Blacklists. In: Stavrou A., Bos H., Portokalidis G. (eds) Research in Attacks, Intrusions and Defenses. RAID 2014. Lecture Notes in Computer Science, vol 8688. Springer, Cham

[6] Rossow, C., Czerwinski, T., Dietrich, C. J., & Pohlmann, N. (2010). Detecting Gray in Black and White. MIT Spam Conference

[7] Sinha, S., Bailey, M., & Jahanian, F. (2008). Shades of Grey: On the effectiveness of reputation based black-lists. Proceedings of the International Conference on Malicious and Unwanted Software(Malware), 57{64.

[8] Symantec. (2017). *Internet Security Threat Report (ISTR) Government*, vol. 22. Retrieved September 17, 2017, from https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf.

[9] U.S. Government. (2016). How to Protecting Your Networks from Ransomware, 2–8. Retrieved September 17, 2017, from https://www.justice.gov/criminal-ccips/file/872771/download