Proposed Approach for Targeted Attacks Detection

Ibrahim Ghafir and Vaclav Prenosil

Abstract For years governments, organizations and companies have made great efforts to keep hackers, malware, cyber attacks at bay with different degrees of success. On the other hand, cyber criminals and miscreants produced more advanced techniques to compromise Internet infrastructure. Targeted attack or advanced persistent threat (APT) attack is a new challenge and aims to accomplish a specific goal, most often espionage. APTs are presently the biggest threat to governments and organizations. This paper states research questions and propose a novel approach to intrusion detection system processes network traffic and able to detect potential APT attack. This detection of APT attack is based on the correlation between the events which we get as outputs of our detection methods. Each detection method aims to detect one technique used in one of APT attack steps.

Keywords Cyber attacks · Targeted attacks · Advanced persistent threat · Malware · Intrusion detection system

1 Introduction

Nowadays the cost of cyber attacks, malicious activities on Internet infrastructures, is estimated to somewhere between 100 billion and 1 trillion US dollars annually around the world [1]. Targeted attack or advanced persistent threat (APT) attack is a new challenge and aims to accomplish a specific goal, most often espionage. APTs are presently the biggest threat to governments and organizations [2]. These APTs create a problem for existent detection methods because the current techniques are based on known signatures of attacks and APTs often use new security holes for

I. Ghafir (✉) · V. Prenosil
Faculty of Informatics, Masaryk University, 60200 Brno, Czech Republic
e-mail: ibrahim_ghafir@hotmail.com

V. Prenosil
e-mail: prenosil@fi.muni.cz

H.A. Sulaiman et al. (eds.), *Advanced Computer and Communication Engineering Technology*, Lecture Notes in Electrical Engineering 362,
DOI 10.1007/978-3-319-24584-3_7

attacks. The financial losses due to a successful APT attack can be very high as it is confirmed through many previous research findings on APTs [3–5]. The expected economic effect of attacks is the major influence on investments in security measures [6].

In this paper we state our research questions and present our proposed approach for APT detection. In this research we are aiming to contribute to intrusion detection systems, particularly to APT attack detection. The goal of this work is to research a novel approach of intrusion detection processes network traffic and able to detect APT attack. The detection of APT attack is based on the correlation between the events which we get as outputs of our detection methods. We believe that the opportunity for using this approach in APTs detection is big and, to the best of our knowledge, still unexplored.

The remainder of this paper is organized as follows. State of the art is described in Sect. 2. We state our research questions in Sect. 3. Section 4 presents our proposed approach for APT attack detection and Sect. 5 concludes the paper.

2 State of the Art

In January 2011, Google published the first report about APT. Known as Operation Aurora [3]; the attack has begun in the second half of 2009. It was considerably large-scale and is mentioned to have targeted 34 companies, including Dow Chemical, Morgan Stanley, Northrop Grumman, Symantec, Northrop Grumman and Yahoo, as well as Google itself. Later on, other research findings on APT attack are reported in [4, 5, 7].

Some researches have been done on analyzing already identified of APTs. In [8], the authors showed how to detect the N most likely infected hosts of the attack; their approach is based on the knowledge of previous APT attacks. By improving the performance in terms of false positives and detection rate, they developed a search engine for APT investigators to quickly reveal the possible infected hosts based on the features of a known APT infected host. They made use of N-gram based mechanisms.

During the year 2011, many targeted attacks were identified by Symantec. This large corpus of APTs was analyzed in-depth by the authors in [9]. Based on advanced TRIAGE data analytics, they were able to attribute many of advanced persistent threats to attack campaigns quite likely accomplished by the same individuals. They analyzed the dynamics and features of those attacks and presented new ideas into the modus operandi of attackers engaged in those campaigns.

By using an undirected graph in [10], the authors showed that APTs against the same target could be correlated. In addition, it is possible to identify clusters and create a map of APT activity that may uncover the activities of single group of malware writers.

With regards to detect potential targeted attack, in [11] they proposed a novel system to detect possible APT attack based on the information gathered on the

host's side. The system depends on clustering techniques to classify groups of hosts that have a similar behavior with respect to the suspicious resources they request (e.g., C&C servers, drive-by downloads or exploit kits). The system was called SPuNge and implemented in a working prototype. SPuNge correlates the sites and industry data in which those hosts run (e.g., government or gas and oil) to detect interesting attack activities.

An abridged version of initial Duqu analysis was presented in [12]. A European corporation was targeted by a new malware, Duqu, and valuable information was stolen. The authors described the Duqu detector toolkit, a set of heuristic tools that they developed to detect Duqu and its variants.

Given the related works presented above, most of the above works focus on analyzing already identified campaigns, while the scope of our work is to present a new approach that detect possible APT attacks, none of the related works address explicitly the problem of detecting potential APT attacks by means of monitoring network traffic and correlation between detection methods of possible techniques used in APT attack life cycle.

3 Research Questions

To achieve the goal of this work we should answer the following research questions:

Research question 1: What are the detection methods can be used for detecting possible techniques used through APT attack life cycle? To answer this question we have proposed 8 detection methods presented in Sect. 4. We will try to implement these methods in the first phase of our research. These proposed methods are not fixed; we can remove or suggest a new method based on the research progress.

Research question 2: How can we make the detection system resulting from our approach extensible and flexible? The attackers always try to find new techniques to perform APT attack, therefore each detection method should be independent from the other methods, so at any time we can add new method (for detecting new technique used in APT attack life cycle) to the system and correlate it with the other methods in the correlation framework. To achieve the flexibility, in the correlation framework it should be easy to remove or add a new rule for raising an alert on APT attack detection.

Research question 3: Is this approach able to handle the network traffic in the real-time? The detection system should support the real-time detection because if an attack, or an attempted attack, is detected quickly, then it can be much easier to trace back the attacker, minimize the damage and prevent further break-ins. To answer this question, in our approach and in the first phase, the detection methods should not depend on storing data and then analyzing it for detection. They should be able to process the network traffic in the real-time and submit their events to the next phase for correlation.

Research question 4: Is this approach effective? The effectiveness of the approach, which is its ability to detect APT attacks, should be high. This should be combined with a high accuracy resulting into a low number of false warnings. We expect that the chance at a false positive is lower when there is a direct link to other steps or correlation between the events. In order to achieve efficiency for our approach we should identify suitable rules for correlation between the events and this will depend on the evaluation of each detection method and will be done in the last phase of our research.

4 Proposed Approach

In this research we are aiming to contribute to intrusion detection systems, particularly to APT attack detection. The goal of this work is to research a novel approach of intrusion detection processes network traffic and able to detect APT attack. The detection of APT attack is based on the correlation between the events which we get as outputs of our detection methods. We believe that the opportunity for using this approach in APTs detection is big and, to the best of our knowledge, still unexplored.

We will implement our proposed approach on top of Bro intrusion detection system [13, 14]. Bro is a passive, open-source network traffic analyzer. It is primarily a security monitor that inspects all traffic on a link in depth for signs of suspicious activity. The most immediate benefit that we gain from deploying Bro is an extensive set of *log files* that record a network's activity in high-level terms. These logs include not only a comprehensive record of every connection seen on the wire, but also application-layer transcripts such as, e.g., all HTTP sessions with their requested URIs, key headers, MIME types, and server responses; DNS requests with replies; and much more.

Our proposed approach, as it is shown in Fig. 1, consists of two main phases:

In the first phase, we process the network traffic to detect possible techniques used in APT attack life cycle. To this end we have our detection methods; each

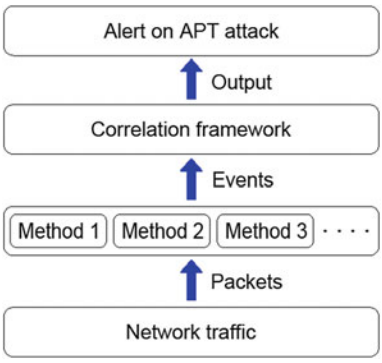

Fig. 1 Architecture of our proposed approach

detection method aims to detect one technique used in one of APT attack steps. Each detection method is independent from the other methods and should be evaluated before it is adopted. The outputs of these detection methods should be submitted to the second phase where correlated to raise an alert on APT attack.

In the second phase, we have the correlation framework, this framework takes the events (the outputs of our detection methods) as an input and correlates them according to rules specified by the user (we can specify those rules based on the evaluation of each method) to raise an alert on APT attack detection. The correlation method is based on voting between the detection methods to raise an alert on APT attack and the detection can be based on one, two or three events. We believe that this correlation will reduce the false positive rate of our detection system.

A key question in our research is: What are the detection methods can be used for detecting possible techniques used through APT attack life cycle. To answer this question taking into consideration the life cycle of APT attack, which is shown in Fig. 2 [15], we have 8 detection methods should be implemented in the first phase of our research:

1. Intelligence gathering: This initial phase aims to get information about the target, like its organizational structure, IT environment and even about people who are working for that target. For this purpose, the attacker can use public sources (LinkedIn, Facebook, etc.) and prepare a customized attack.
2. Initial compromise (Point of entry): Performed by use of social engineering and spear phishing, over email, using zero-day exploits. Another popular infection method was planting malware on a website that the victim employees will be likely to visit. The most common technique used for this step is spear phishing emails, which may contain link to malicious website, malicious attachment or link to malicious file.

Fig. 2 Typical steps of APT attack

Method 1, from previous findings on APTs, we have a list of exploited domain names (FQDNS) used in APT attack [5], we can analyze the traffic of possible protocols used in sending and retrieving emails and if there is a link to one of exploited FQDNS, we can detect spear phishing attack.
Method 2, detection of any connection to a malicious domains based on a blacklist of malicious domains [16–21].
In case of malicious attachment, executable files supposed to end in.exe are made to appear as simple document files (pdf, doc, ppt, excel).
Method 3, detecting if the content of the file is exe while the extension is not exe.
Method 4, for each new file, we can calculate MD5, SHA1 and SHA256 hash, and compare with a blacklist of file hashes (from previous findings on APTs) [5], if a match is found, we detect an attack.

3. Command and control (C&C) communication: After an organization's perimeter has been breached, continuous communication between the infected host and the C&C server should be preserved to instruct and guide the compromised machine. These communications are usually protected by Secure Sockets Layer (SSL) encryption, making it difficult to identify if the traffic directed to sites is malicious.
   Method 5, we have a blacklist of SSL certificates (from previous reports) [22, 23], so we can monitor SSL certificates and match with the blacklist, if a match is found, we detect an attack.
   Method 6, we have a blacklist of C&C servers [24–27], any connection to one of those servers is an attack.
   Another technique can be used in this step is domain flux technique [28]; an exploited host may try to connect to a large number of domain names which are expected to be C&C servers. The goal of this technique is to make it difficult or even impossible to shut down all of these domain names. This technique leads to many of DNS query failures because not all of these domains are registered.
   Method 7, domain flux detection based on DNS query failure.
4. Lateral movement: Once getting an access to the target's network, the attacker laterally moves throughout the target's network searching for new hosts to infect. Some techniques used: Brute force and pass the hash attacks.
5. Asset/Data discovery: This step aims to identify and isolate the noteworthy assets within the target's network for future data exfiltration.
   Since the traffic of the steps 4 and 5 are inside the compromised network, we cannot see it.
6. Data exfiltration: Data of interest is transmitted into external servers which are controlled by the attacker. There are some techniques used for data exfiltration like built-in file transfer, via FTP or HTTP and via the Tor anonymity network.
   Method 8, Tor connection detection based on Tor server list [29].

The blacklists of blacklist-based detection methods should be automatically updated each day and the detection by all methods should be in the real time.

5 Conclusion

In this paper we proposed a novel approach for detecting potential APT attack and presented the research questions which we should answer to achieve this goal. The detection of APT attack is based on the correlation between the detection methods of possible techniques used in APT attack life cycle. We believe that the opportunity for using this approach in APTs detection is big and, to the best of our knowledge, still unexplored.

Acknowledgments This work has been supported by the project "CYBER-2" funded by the Ministry of Defence of the Czech Republic under contract No. 1201 4 7110.

References

1. Kshetri, N.: The global cybercrime industry: economic, institutional and strategic perspectives. Springer, Berlin (2010)
2. Wood, P., Nisbet, M., Egan, G., Johnston, N., Haley, K., Krishnappa, B., Tran, T. K., Asrar, I., Cox, O., Hittel, S., et al.: Symantec Internet Security Threat Report Trends for 2011, vol. XVII (2012)
3. Tankard, C.: Advanced persistent threats and how to monitor and deter them. Netw. Secur. **2011**(8), 16–19 (2011)
4. Kaspersky Lab ZAO. Red October diplomatic cyber attacks investigation. http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation. Accessed 10-11-2014
5. Mandiant Intelligence Center. Apt1: Exposing one of china's cyber espionage units. Technical report, Mandiant, Tech. Rep (2013)
6. Rakes, T. R., Deane, J. K., Rees, L. P.: It security planning under uncertainty for high-impact events. Omega **40**(1), 79–88 (2012)
7. Ronald, D., Rafal R.: Tracking ghostnet: Investigating a cyber espionage network. Inf. Warf. Monitor, p. 6 (2009)
8. Liu, S.T., Chen, Y. M., Lin, S. J.: A novel search engine to uncover potential victims for apt investigations. In: Network and Parallel Computing, pp. 405–416. Springer, Berlin (2013)
9. Thonnard, O., Bilge, L., O'Gorman, G., Kiernan, S., Lee, M.: Industrial espionage and targeted attacks: Understanding the characteristics of an escalating threat. In Research in Attacks, Intrusions, and Defenses, pp. 64–85. Springer, Berlin (2012)
10. Lee, M, Lewis, D.: Clustering disparate attacks: mapping the activities of the advanced persistent threat. In: Proceedings of the 21st Virus Bulletin International Conference, pp. 122–127 (October 2011)
11. Marco Balduzzi, Vincenzo Ciangaglini, and Robert McArdle. Targeted attacks detection with spunge (2013)
12. Bencsath, B., Pek, G., Buttyan, L., Felegyhazi, M.: Duqu: Analysis, detection, and lessons learned. In ACM European Workshop on System Security (EuroSec), vol. 2012 (2012)
13. Paxson, Vern: Bro: a system for detecting network intruders in real-time. Comput. Netw. **31**(23), 2435–2463 (1999)
14. Bro Project. The bro network security monitor. http://bro.org/. Accessed 10-11-2014
15. Trend Micro white paper. The custom defense against targeted attacks. http://www.trendmicro.fr/media/wp/custom-defense-against-targeted-attacks-whitepaper-en.pdf. Accessed: 10-11-2014

16. Blade defender. http://www.blade-defender.org/eval-lab/blade.csv. Accessed 10-11-2014
17. Malware domain list. http://www.malwaredomainlist.com/hostslist/hosts.txt. Accessed 10-11-2014
18. Malware domains. http://www.malware-domains.com/files/. Accessed 10-11-2014
19. Abuse.ch. Palevo domain blocklist. https://palevotracker.abuse.ch/blocklists.php?download=domainblocklist. Accessed 10-11-2014
20. Abuse.ch. Spyeye domain blocklist. https://spyeyetracker.abuse.ch/blocklist.php?download=domainblocklist. Accessed 10-11-2014
21. Abuse.ch. Zeus domain blocklist. https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist. Accessed 10-11-2014
22. Abuse.ch. SSL blacklist a new weapon to fight malware and botnet. http://securityaffairs.co/wordpress/26672/cyber-crime/ssl-blacklist-new-weapon-fight-malware-botnet.html. Accessed 10-11-2014
23. Mandiant. Mandiant apt1 report appendix f update: SSL certificate hashes. https://www.mandiant.com/blog/md5-sha1/. Accessed 10-11-2014
24. Malware domain list. http://www.malwaredomainlist.com/hostslist/ip.txt. Accessed 10-11-2014
25. Abuse.ch. Palevo C&C ip blocklist. https://palevotracker.abuse.ch/blocklists.php?download=ipblocklist. Accessed 10-11-2014
26. Abuse.ch. Spyeye ip blocklist. https://spyeyetracker.abuse.ch/blocklist.php?download=ipblocklist. Accessed 10-11-2014
27. Abuse.ch. Zeus ip blocklist. https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist. Accessed: 10-11-2014
28. Yadav, S., Reddy, A.K.K., Narasimha Reddy, A.L., Ranjan, S.: Detecting algorithmically generated domain flux attacks with DNS traffic analysis. IEEE/ACM Trans. Netw. **20**(5), 1663–1677 (2012)
29. Tor Network Status. CSV list of all current tor server ip addresses. http://torstatus.blutmagie.de/. Accessed 10-11-2014