Predictive Model for Exploit Kit based Attacks

Slim Trabelsi[1], Skander Ben Mahmoud[1] and Anis Zouaoui[2]
[1]*SAP Security Research, Mougins, France*
[2]*ESPRIT, Tunis, Tunisia*

Keywords: Cybersecurity, Predictive, Exploit, Attack, Hacking, Vulnerabilities, Social Media.

Abstract: Exploit kits are becoming frequently used to generate attacks against systems and software components. These exploit kits are really popular among the non-expert community (script kiddies) and are publicly available on Social Medias. In this paper we demonstrate how this popularity of such exploit kits on social media can impact the severity of the attacks generated from these tools. We propose we propose a new predictive model to estimate in advance the possible attacks that could be generated from trendy kits.

1 INTRODUCTION

A software vulnerability, is a failure in the software source code or process design that can permit to a malicious user (attacker) to exploit it in order to modify the "normal" behaviour of the program. The portion of code or a structured process that is generated to take advantage of such vulnerabilities is called exploit. Traditionally exploits are used by security experts and hackers that have enough knowledge, to understand this code, to compile it and execute it against targeted systems. Since 2006 (Chen, 2015) appeared the exploit kit that is an easy to use a toolkit that automates the exploitation of known or unknown software vulnerabilities. Usually, the exploit kit does not require a specific development or security expertise to run it. For this reason, exploit kits are appreciated by script kiddies and cybercriminals to setup browser-based attacks against some of the most popular systems. The usage and the diversity of these tools completely changed the recent years by becoming widely distributed and easily available on the internet. In the CISCO's 2015 Midyear Security Report (CISCO, 2015) exploit-kits based attacks are identified as the most increasing threat affecting companies. They evaluated the impact of a single exploit kit called ANGLER (Zaharia, 2015) to 30$M Annually revenue impacting 90K users every days. In 2015 according to all the security reports ANGLER was identified as one of the most devastating exploit kit ever seen in the cybersecurity history. In order to evaluate the impact the attacks orchestrated using these exploit kits, security professionals in big companies like Symantec, Trend Micro, CISCO, McAfee, F-Secure etc. has to monitor all the logs, and data collected from their anti-virus, anti-malware, firewalls, IDS systems in order to quantify the infected machines and servers then generate reports describing the phenomena. In order to do that, they need to spend a lot of resources in order to analyze a huge amount of data (data that they own and that is not accessible to anybody). In this paper we try to reconstruct these observations and these tendencies by exploiting other data sources publicly available like in Social Medias (especially Twitter). We propose a study in which we compare the figures related to exploits, published in different security reports from 2014 to 2015, with the presence and the popularity of these kits on Social Media. Through this study we first want to answer to the question: Does the popularity of an exploit published on Social Medias has an impact on the severity of the attacks resulting from these exploits? Our hypothesis concerns the simplicity of consumption offered by Social Media platforms to dangerous toolkits that can damage systems. In the past, a malicious or curious attacker had to subscribe to some hidden and closed hackers forums in order to access to such exploit kits, but now these tools are publicly available and widely shared.

If we can answer to this question positively, this could open to us new perspectives related to the predictability of the damage that could cause the popularity of an exploit. Because we can monitor in real-time the presence and the popularity of these kits in Social Medias, we can also trigger alerts with

Trabelsi, S., Mahmoud, S. and Zouaoui, A.
Predictive Model for Exploit Kit based Attacks.
DOI: 10.5220/0005999904770482
In *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 4: SECRYPT*, pages 477-482
ISBN: 978-989-758-196-0

regards to the potential threats targeting specific systems. We don't have to wait every end of quarter, semester or year in order to evaluate the impact of a threat, we can guess it in real time.

This paper is organized as follows: In Section 2 we start with a state of the art related to the first analysis of Social Media for cybersecurity purposes. In Section 3 we present the tool used to perform our study. In Section 4 we compare our results those published in diverse cybersecurity reports. In section 5 we start describing the first insights of the predictive model. And finally in Section 6 we conclude our study and we discuss about our future plans with regards this topic.

2 STATE OF THE ART

The concept of software vulnerability monitoring through Social Media analysis already spotted new phenomena's related to the way how security information (vulnerabilities, zero-days, exploit codes, bugs etc.) are shared and exploited by attackers. In (Trabelsi, 2015) authors conducted a study to evaluate the quality and the relevance of security information related on Twitter. They discovered that 75% of the CVEs[1] related to the Linux-kernel software component in 2014 were already disclosed on twitter before and more globally 41% of the CVEs published by the NIST NVD were already present on Social media before. The same authors were using a real time vulnerability monitoring system that crawls and analyse Twitter streams (Trabelsi2, 2015) .In (Edkrantz, 2015) authors made a study that correlates the existence of exploit code on twitter with real-word attacks. In this work, authors proposed an early alerting tool that signals the emergence of a new exploit that could present a potential threat to existent systems.

The first tentative to predict potential vulnerability exploits was proposed by (Sabottke, 2015) with the idea to use machine learning algorithms learning to make automatic predictions for unseen vulnerabilities based on previous exploit patterns published on NVDs. For this study only NVDs and Exploit DBs were used, and there was no correlation with Social Medias.

In our study we will try to correlate the impact of attacks generated from exploit kits with their popularity on Social Medias, in order to predict in advance which exploit kit will be used and which software components will be affected and what would be the expected severity of the attacks. In comparison with the related work we compare our results with official public reports published by recognized security professionals.

[1] CVE: Common Vulnerabilities and Exposures, allows the structured description of software vulnerabilities

3 VULNERABILITY AUTOPSY: A CYBERSECURITY REVIEW ON SOCIAL MEDIA

3.1 Autopsy Tool

As introduced in the previous section, more and more security researchers are now using Social Media to monitor security issues. The advantage of using Social Medias is the diversity and the aggregation of sources; instead of monitoring several websites, blogs, forums, bug trackers, Social Media platforms like Twitter, due to its diversity, offers an aggregator of links and sources coming from all origins. Social Medias offers also a good dataset archive that can be exploited in order to study phenomena related to cybersecurity and threats. For this reason we developed a tool called SMASH-Autopsy (in extension to SMASH-Live (Trabelsi3, 2015) that searches back in Social Media archive and performs automated analytics and statistics on past security events related to software vendors, programs and components. This tool searches for all the publications related to any security information referring to a software component. The collected information is clustered by content then categorized by topic (vulnerability, zero-day, exploit, patch, bug, data flaw, etc.) for every topic we have sub-categories related to the different type of topics. For example for the Vulnerability topic, the sub-categories would be SQL Injection, XSS, DDoS, etc. Once the information is clustered and classified, we start a quantitative analysis in order to generate statistics on the number of issues, the frequency, the number of patches and solutions and the impact of the issues.

Figure 1: Vulnerability Autopsy Process.

In the current version of the SMASH-Autopsy tool, we mainly rely on a Twitter Search API, but we are currently integrating other sources like Facebook

and Google News. The clustering algorithm that we use is defined here (Trabelsi4, 2015) and is based on vector distance grouping process.

3.2 Popularity and Presence on Social Media

Measuring presence and influence on Social Media is a quite fertile topic that generated a lot of studies and research work with an important diversity of measurement models like (Bakshy, 2011), (Rosenman,2012). A multitude of parameters were taken into account, like net-work size or sentiment feedbacks of the shared data, but three parameters are always present: Number of messages dealing with the topic, number of shares and citations. In our study we will limit our simple popularity computation model to these three parameters. We make a simple addition to these parameters and we compute a general score that will represent the presence of a particular information on the selected Social Medias. This model is quite simplistic and can easily been discussed, but we choose it as a starting point with the objective to improve it in the future.

3.3 Review on the Presence of Exploit Kits in Social Medias in 2015 /2014

According to several security reports (Chen, 2015), (CISCO, 2015), (McAffee, 2015) published between 2015 and 2016 Exploit kit based attacks appeared to be the most growing cybersecurity threats between 2014 and 2015. For this reason we decided to take a closer toll to this phenomena by observing the evolution of the presence of information related to exploit kits on social media and specially Twitter. To do that we used our SMAHS-Autopsy tool as entry keyword "exploit kit" for the period between Q1 2014 to Q3 2015. We obtained more than 9000 results. These results were processed, filtered and clustered then finally categorized according to the tool name and the targeted software component. For every exploit kit we computed its popularity using the model presented in the previous section.

The list of most popular exploit kits published on twitter between 2014 and 2015 is the following: Angler, Magnitude, Nuclear, Rig, Sweet Orange, Neutrino, Sundown, Hanjuan, Fiesta. This list corresponds the list of exploit kits observed by trend Micro between Q1 and Q3 2015.

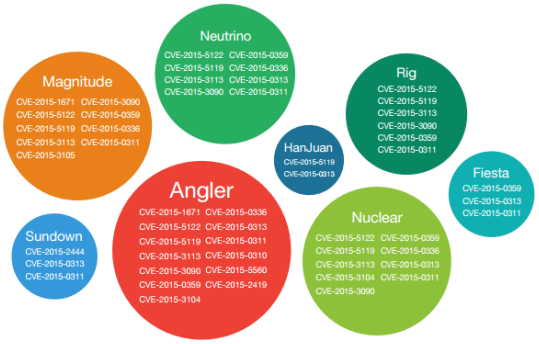


Figure 2: Vulnerability exploits integrated into kits (1Q-3Q 2015) (TrendLabs, 2015).

The exception is Sweet Orange that is a kit popular in 2014 that disappeared in 2015.

This result is quite encouraging in the sense that the presence of exploit kits on twitter is similar to its presence on security reports. We used this result as a starting point to a correlation study with our observations and the facts reported by security professionals.

4 EXPLOIT KIT CASE STUDY

Between 2014 and 2015 according to all the security reports, the ANGLER exploit kit was the most active one. This observation was also observed on Social Media where ANGLER was the most popular keyword related to exploits shared on Twitter during the same period.

4.1 Exploit Kit Distribution

In 2015 Trend Micro (TrendLabs, 2015) recorded a certain number of malicious URLs generated by different exploit kits. They evaluated the ratio of each URL pattern in order to quantify the usage of every kit. We compared this quantification with the popularity of every kit for the same period.

We clearly notice a similarity on the distribution classification although if in terms of proportion we cannot compare the quantity knowing for example that a corrupted URL can appear several times for the same web page.

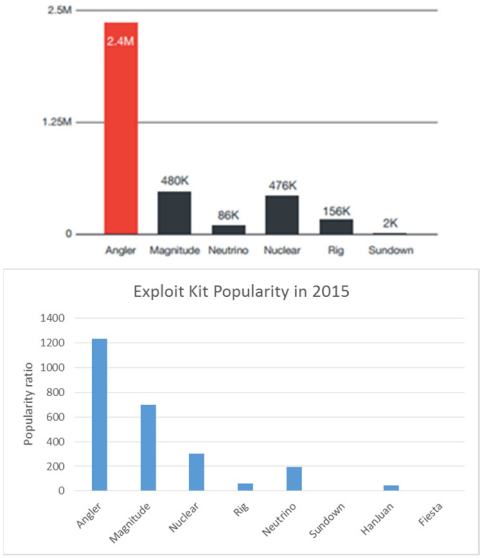
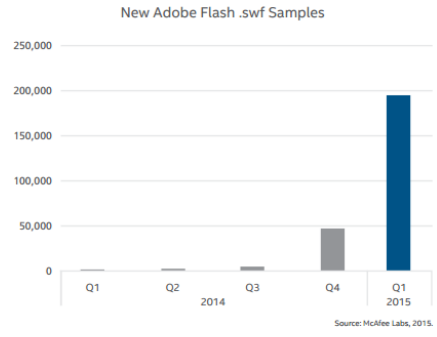


Figure 3: Exploit kit attack distribution (TrendLabs, 2015) Vs Exploit kit popularity distribution.

4.2 Impact on Adobe Flash Content using Exploit Kits

Between 2014 and 2015 the number of attacks sibling Flash websites drastically grown up due the diversity of exploit kits targeting this technology and due to the unusual number of severe vulnerabilities related to Adobe Flash player. If we try to quantify all the recorded attacks against flash and we compare it to the popularity of the different exploits targeting flash on Twitter we can also observe a similitude in the growth and brutal growth of the attacks (see figure 4). We clearly notice a correlation between the severity of the attacks generated from these exploits published by McAfee [12] and the popularity of the flash exploits on Twitter.



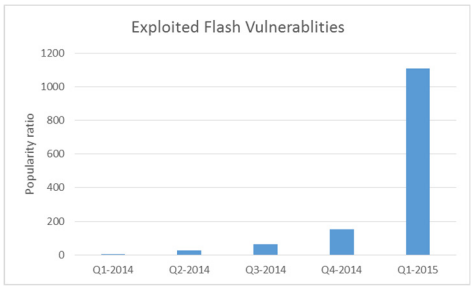


Figure 4: Evolution of the attacks targeting flash (McAffee, 2015) Vs popularity of Flash exploits on Twitter.

4.3 Distribution of the Exploit Kits in July 2015

F-Secure proposed a fine grained observation of the exploit kits in July for a few days (F-Secure, 2015). Although if we cannot have such granularity (by day) we tried to evaluate the popularity of these exploit kits during the entire month of July and compare the tendencies. The comparison is shown in figure 5.

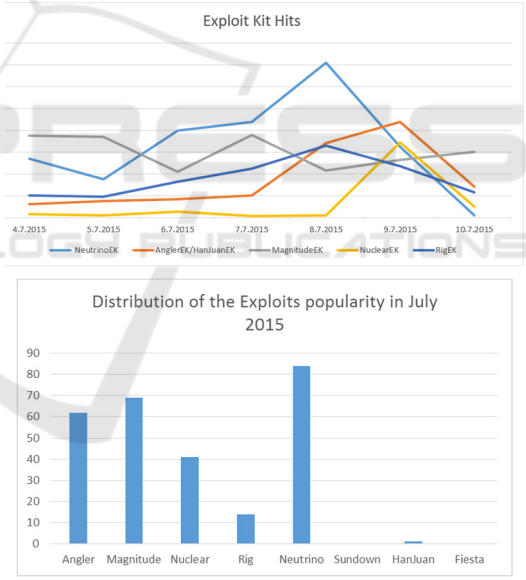


Figure 5: Exploit kits hits July 2015 (F-Secure, 2015) Vs Exploit kits popularity on Twitter July 2015.

We observe that the number of registered hits during this weak in July corresponds in terms of order distribution to the popularity of every distinct exploit kit sited on Twitter. This confirms us that we can have a granularity of at least one month in order to cover the most popular/used exploit kits.

5 PREDICTING POTENTIAL THREATS

The observations reported during this study highlighted many correlation between real attacks generated by exploits kits and their popularity on Social Medias. This consolidates somehow our hypothesis related to the impact on the presence of exploit kits in public Social Media that could influence the cybersecurity landscape. For this reason we propose in this paper to rely on Social Media real time analysis as input to a prediction model concept. This model would rely on the popularity of certain topics related to vulnerabilities, exploits and bug details. We propose to work on time series to determine whether a variation of popularity related to these topics can provide some hints on the new threats that can target vulnerable or non-patched systems. We are currently working on this model in order to try to validate it through a long term study that will compare real facts reported by security professionals with the predictions generated by this model. We also noticed that the cyber-threat landscape is permanently evolving and morphing, and Social Media can accompany this evolution as hacking community is more and more present in these kind of media. We propose to apply machine learning algorithms to adapt the analysis to these new tendencies and not only rely on a static predictive model dedicated to only one kind of threat.

This model can be used for companies to optimize the prioritization their patching schedule and try to apply very urgent patches before a huge wave of attacks targeting these specific systems.

6 CONCLUSION AND FUTURE WORK

In this position paper we demonstrate the influence of Social Media Networks on the cybersecurity landscape. We proposed a study that analyses the presence and the popularity of information related to exploit kits on Twitter in order to correlate these measurements with real data related to the impact of the attacks generated by these kits. This data is provided by security professional reports (from 2014 to 2015). The results obtained are very encouraging especially with regards to the strong correlation between the popularity of an exploit with the importance of the related attack. This led us to comfort our hypothesis: the more an exploit is popular on social media, the more the probability of having attacks generated from it is high. For this reason we started developing a predictive model based on security information collected from Social Medias. Social Medias tell us what is the favourite exploit kit and we can guess what could be the future attacks. In this paper we describe the concept of threat pre-diction without detailing the predictive model since we need to conduct a long term study in order to validate the predictions generated by this tool, and this requires time. It is not yet clear to us the estimation of the time delay between the first apparition of an exploit on Twitter and the first recorded attack. We need security professional proprietary data to obtain this information.

Beside the pure time series based predictive model we are also working on a ma-chine learning based algorithm that tends to adapt the monitoring on the type of security information that is highly changing over the time. We are also experimenting different existing popularity computation algorithms for Social Media is order to verify the existence of a better algorithm that could correspond better to the information distribution of the real attacks.

REFERENCES

Chen, J. C., Li, B., 2015. *Evolution of Exploit Kits: Exploring Past Trends and Current Improvements*. Trend Micro White paper report 2015.

CISCO, 2015. *Midyear Security Report* http://www.cisco.com/assets/global/UK/events/switchup_challenge/pdf/cisco-msr-2015.pdf.

Zaharia, A., 2015. *The Ultimate Guide to Angler Exploit Kit for Non-Technical People*. Heimdal Security https://heimdalsecurity.com/blog/ultimate-guide-angler-exploit-kit-non-technical-people/

Trabelsi S., Plate H., Abida A., Ben Aoun M., Zouaoui A., Missaoui C., Gharbi S. and Ayari A., 2015. *Mining social networks for software vulnerabilities monitoring*. In 7th Internation-al Conference on New Technologies, Mobility and Security (NTMS), 2015 (pp. 1-7). IEEE.

Sabottke C., Suciu. O. and Dumitraş, T,. 2015. *Vulnerability disclosure in the age of social media: Exploiting Twitter for predicting real-world exploits*. USENIX Security Symposium (USENIX Security), Washington DC.

Edkrantz, M., Said, A., 2015. *Predicting Cyber Vulnerability Exploits with Machine Learning*. IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud) (pp513 – 514).

Trabelsi, S., 2015. *SMASH Goes Live: Software Vulnerability Live Monitoring on HANA*. SAP Community Network https://scn.sap.com/community/hana-in-memory/use-cases/blog/2015/06/04/smash-goes-live-software-vulnerability-live-monitoring-on-hana.

Trabelsi, S., 2015: *SMASH Demo: Monitoring Software Vulnerabilities through Social Media Analysis*. SAP Community Network . http://scn.sap.com/community/security/blog/2015/11/05/smash-demo-monitoring-software-vulnerabilitites-through-social-media-analysis.

Trabelsi S., Plate H., Abida A., Ben Aoun M., Zouaoui A., Missaoui C., Gharbi S. and Ayari A., 2015. *Monitoring Software Vulnerabilities through Social Networks Analysis*. In Pro-ceedings of the 12th International Conference on Security and Cryptography, pages 236-242.

Bakshy, E., Hofman, J. M., Mason, W. A., & Watts, D. J., 2011. *Everyone's an influencer: quan-tifying influence on twitter*. In Proceedings of the fourth ACM international conference on Web search and data mining (pp. 65-74). ACM.

Rosenman, E. T.. 2012. *Retweets—but not just retweets: Quantifying and predicting influence on twitter* (Doctoral dissertation, Bachelor's thesis, applied mathematics. Harvard College, Cambridge).

McAfee, 2015. *Labs Threat Report May* http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf.

TrendLabsSM 3Q 2015 *Security Roundup* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-hazards-ahead.pdf.

F-Secure Labs, 2015. *Hacking Team 0-day Flash Wave with Exploit Kits* https://www.f-secure.com/weblog/archives/00002819.html.