Red Queen's Race: APT win-win game

Vit Bukac[1], Vaclav Lorenc[2] and Vashek Matyas[3]

[1] Faculty of Informatics, Masaryk University, Brno, Czech Republic
bukac@mail.muni.cz,
[2] Institute of Computer Science, Masaryk University, Brno, Czech Republic
valor@mail.muni.cz,
[3] Faculty of Informatics, Masaryk University, Brno, Czech Republic
matyas@fi.muni.cz

Abstract. Advanced persistent threats (APTs) are are not only a very prominent buzzword, but often come with a costly impact. A popular approach how to deal with APTs is the kill chain concept. We propose an extension to the kill chain, where the attacker is allowed to continue his attack even after being discovered by defenders. Meanwhile, observing defenders collect valuable intelligence which is to be used to counter future attacks. Benefits and negatives of postponed remediation are presented and related issues are discussed.

Keywords: advanced persistant threats, APT, kill chain, honeypot

1 Background

In the entire human history, economic or military contestants have used subtle techniques to achieve information dominance. They have used anything from bribery to gun threats to modification of satellite communications. Widespread and dependence on computer networks then provided abundant new attack vectors. Advanced persistent threat (APT) is a term coined for an advanced long term stealthy intrusion into a computer system, with the aim to steal an intellectual property of the owner [Man10]. APTs are quickly becoming a nightmare for security officers. APT groups are usually well-funded and possess extensive knowledge. They employ effective intrusion methods such as zero-day attacks or stealth techniques and often have vast infrastructure of compromised servers for support. Their attacks come in campaigns and are often aimed at only a single target globally, being tailored specifically to target with reliance on prior reconnaissance. Traditional security measures such as antivirus software, signature based IDSs and systems hardening are largely inefficient against APTs.

To combat the rapidly growing threat of APTs, security experts from Lockheed Martin recommended adopting the concept of *kill chain* [HCJA11]. The idea behind the kill chain is to create a knowledge base of indicators from all observed phases of an APT in order to continuously improve defenses. The struggle between APT actors and defenders leads to a game where APT actors are adapting their techniques to penetrate encountered defense measures and defenders

are developing new signatures and indicators to have the upper hand in campaigns in the future. The kill chain concept is quickly becoming the weapon of choice against APTs, being fostered by renown companies such as RSA [RSA12], Dell SecureWorks [Sec13], Hewlett-Packard [HP13] or NSS Labs [FA12]. Relevant academic research focuses primarily on efficient data aggregation and analysis [BY13,ILCP13].

Cyber kill chain concept is not limited to APTs. Harris, Konikoff and Petersen investigated the application of kill chain on distributed denial of service (DDoS) attacks. While performing DDoS attacks can always be considered an intended Action on Objective, authors also look for DDoS-related events at other phases [HKP13].

2 Kill chain

APTs can be split into several consecutive phases (Fig. 1). Failure to overcome the defense measures at any phase results in the interruption of entire process. Oppositely, intrusion detection during a certain phase implies that all previous phases executed successfully. Phases are as follows [HCJA11]:

1. Reconnaissance. The attacker learns about the target organization and its members from mailing lists search, social networks crawling and web page crawling.
2. Weaponization. Remote access Trojan is coupled with an exploit to create a deliverable payload. Payload is tested and modified as long as it can be detected by security systems that are known to be used by the organization.
3. Delivery. Payload is delivered to the target, usually in the form of an email, a clickable link or on an USB media.
4. Exploitation. Payload is applied to a vulnerable system, executing malicious code.
5. Installation. Tools of attacker's choice are deployed in the system. Persistence is achieved.
6. Command and Control (C2). Infected host informs the APT actor that the compromise was successful. APT actor may begin pursuing his goals.
7. Actions on Objectives. APT actor moves laterally in the environment, using legitimate methods after he gained access to user accounts. He exports intellectual property from the organization in obfuscated or encrypted containers. He cleans most observable traces from the systems that he no longer needs.

A piece of information that objectively describes an intrusion is called an indicator. APT actor's actions during each phase of the kill chain leave a trail of indicators that can be later examined and used to adjust appropriate countermeasures. Indicators are subsequently used to build an attacker model tailored to each separate APT actor. In turn, the attacker model enables allocation of resources towards most relevant security measures.

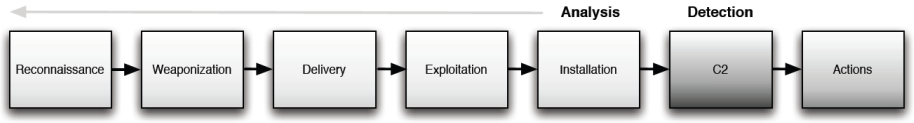

Fig. 1. Kill chain [HCJA11].

Indicator usage example: System is infected by a malware that was encapsulated in a PDF attachment of a spear phishing email. The infection was discovered during a failed attempt to export data to an IP address which is known to belong to APT group. After a forensic analysis of the system, numerous improvements are implemented. A list of all users who received and opened this mail is created and basic security training is scheduled for them. Company antivirus vendor is supplied with binaries of the malware that was installed, along with the description of persistence method and list of file paths where temporary files were stored. Unpatched vulnerability in the PDF viewer is revealed and fixed. A phishing mail subject is added to the watch list in order to track other intrusion attempts of the same campaign. IP addresses of secondary C2 servers that were used to successfully export data to APT actors are blocked.

3 Proposed approach

When an intrusion is detected, both standard intrusion response procedures and kill chain methodic dictate to isolate the affected systems, collect sources of forensics evidence (e.g., HDD images, log files) for later examination and then perform remediation procedures. To our knowledge, no serious thought has been given to the possibility of studying APT actor behavior on a real compromised system.

We propose *to postpone the remediation and focus on collecting as much indicators* on the already compromised system as possible, in order to maximize the knowledge gain from the APT actor. By allowing the attacker to continue his activity under a close passive surveillance or even during an active tampering with his activity, defenders will reveal more from attacker's knowledge and arsenal, leading to an increasingly descriptive set of indicators. We argue that following a win-win scenario in the short term will result in a win-fail scenario for the defender in the mid/long term.

We want to open a discussion whether and under what conditions it is beneficial for system's owner to postpone system remediation and instead focus on monitoring, effectively changing the compromised system to a live honeypot.

APTs are usually detected and identified during the callback phase or the lateral movement phase. After a careful consideration of the triplet (gain; potential associated risks; costs), decision is to be made whether to stop the attack immediately or let it continue under the increased surveillance. Risks taken into account should be: law and policies, intrusion context, data present on the

compromised host, costs of prolonged surveillance and the impact of necessary changes. Regardless of the final decision, sources of forensic evidence for later analysis are always collected. Forensic analysis is performed in parallel to the live system monitoring. Interim monitoring results facilitate the forensic analysis and vice versa.

We propose two stages to the live honeypot – the passive monitoring and the active tampering. During the passive monitoring, defenders focus on learning as much information as possible about the attack without interfering with APT actor's activity. APT actor is misled to believe that his presence in the system has not yet been discovered. We recommend ending this phase after a fixed time deadline or after the attack revealed what type of data (e.g., financial, product documentation, legal documents) was the actual target. Passive monitoring includes but is not limited to:

- Network activity logging both on host and in network (Wireshark, router stats, NIDS logs, proxy logs).
- ACL/filesystem logging (accessed folders, folder listings, created and deleted files).
- Impossible deletion. Any file that is required to be deleted is hidden from the operating system instead.
- Memory dumps of entire host or of selected processes.
- Activation of a collection of low-interaction honeypots to respond to basic network activity.
- System log streaming to a central storage in order to prevent undetectable log file modifications.

During the active tampering defenders create artificial challenges for the attacker to overcome. The goal of defenders is to force the attacker to reveal more from his arsenal (e.g., so far unknown RAT tool, knowledge about internal systems, procedures followed under extreme conditions). Active tampering includes but is not limited to:

- File deletion (e.g., of attacker's temporary files or process binaries). Simulation of activity of external antivirus software. Attacker is forced to use another tool.
- System quarantine, policy hardening. Applying standard tools and policies to block the host from network. Switching the host into a high security mode. Attacker is forced to reveal if he has means to circumvent the limitation.
- Reboot. Attacker is lead to use tools and procedures that are non-volatile. Some attacker actions may not be observable before reboot.
- Network disruption (e.g., rate limiting, gradual IP blocking, TCP maximum segment size limitation). Attacker has to use backup protocols and reveal another part of his control infrastructure.
- Planting baits (e.g., non-essential data, user accounts with various password strengths, encrypted storage with seemingly high value content).

Postponing remediation and close monitoring is a costly action. In order to maintain a reasonable cost/gain ratio, postponed remediation is justifiable only during provably targeted attacks. APTs may be identified from targeted phishing, characteristic behavior (legitimate account misuse, etc.), preliminary analysis that found similarities with previous APT campaigns or from external trusted source (e.g., law enforcement agencies).

4 Properties of postponed remediation

4.1 Benefits

B1 – More attack traces acquired. Identification of used tools, procedures followed, methodics, order of steps, employed stealth techniques, employed cryptography/obfuscation, etc.

- Post-cleanup. If the attacker reaches a cleanup phase, comparison of the system state prior to cleanup and post cleanup may reveal unremoved artifacts, which may be later used to detect other systems compromised in the past. To recognize post-cleanup artifact without prior leads is considered extremely difficult.
- High-level time overview of attacker activity. Time characteristics of different phases of attack, temporal order, frequency of attacker interaction in time, duration of campaigns, duration of each phase of the intrusion, etc.

B2 – Discovery of attacker's goals. What data the attacker is after, whether he wants to maintain presence or leave the system in order to minimize traces, what knowledge the attacker possesses from previous campaigns and he plans to use it, etc. Point B2 is a natural outcome of B1.

B3 – Active tampering. Boosts the efficiency of previous benefits, can produce indicators that are not obtainable by any other means. May provide an insight into the scope of intrusion.

4.2 Negatives

N1 – Policies & Law. Institutional regulations or law may require immediate remediation of an affected system. Privacy issues are raised for users who are working with the compromised host. Proceeding with a postponed remediation on systems with customer's or supplier's data requires agreement of all involved parties.

N2 – Attack spread. Attacker may successfully compromise more systems if he is not contained immediately, especially if he was detected soon after the installation phase.

N3 – Increased costs. Costs of security specialist's time (constant observation and neccesity to prepare emergency procedures), system user's time and engagement of additional resources are higher than in the case of immediate remediation. No guarantees that there will be more information collected than just through standard forensics methods.

– Destruction. A cleanup stage of intrusion may be designed not to remove just traces of attacker behavior, but the system in its entirety.

5 Open questions

Q1 – Do filesystems with reversible changes exist? Are they widely used for security and/or data preservence purposes? Filesystems or drivers that can prevent file deletion are known, but their presence can often by detected by an attacker. Regular backup solutions are too cumbersome for malware tracking purposes. Are virtual machines and snapshots a possible solution?

Q2 – How can virtualization make this method easier? Virtual machine introspection techniques enable monitoring of guest system calls, snapshots allow to compare between pre-cleanup and post-cleanup state and virtual switches can easily separate the closely examined network traffic from the rest of network. What other recent virtualization advancements could impact the live honeypot in the near future?

Q3 – When to stop the intrusion? What is the list of conditions and costs that must be always considered for the decision (e.g., personal information in jeopardy, observed attack spreading, criticality of accessed information, monitoring-related costs)? Can the decision be quantified, e.g., with checklists and conditions weights? What roles in organization will likely have to have a word in the decision?

Q4 – Will this method be still effective if the attacker learns about it? The attacker can react by planting dummy traces and baits. Can his behavior in such situation be also considered as attacker profiling? Is it possible to distinguish between true attacker behavior and simulated attacker behavior with anomaly techniques and a preliminary knowledge?

Q5 – Can this method be justified from the legal perspective? Is there a difference between US and EU? Does different rules apply for company data and for personal data of users who are using the computer during their work? What are differences between company internal policies and the law? How the shortest possible time to mitigate the threat clause should be interpreted?

6 Summary

Kill chain is a promising concept to combat Advanced Persistent Threats. As for this concept, the key to a successful defense against APTs is to gain knowledge about APT actors' techniques, tools and procedures. We propose an extension to the kill chain concept which calls for prolonged monitoring of attacker activities. Allowing the attacker to continue with his activities even after he is detected can result in a significant gain – more threat intelligence.

Acknowledgment

Authors would like to express gratitude to the members of Centre for Research on Cryptography and Security of Masaryk University for their valuable ideas and feedback. Special thanks go to Andriy Stetsko, Zdenek Riha and Marek Sys. This work was supported by the GAP202/11/0422 project of the Czech Science Foundation.

References

[BY13] Parth Bhatt and Edgar Toshiro Yano. Analyzing Targeted Attacks using Hadoop applied to Forensic Investigation. In *Proceedings of the Eighth International Conference on Forensic Computer Science*, 2013.

[FA12] Stefan Frei and Francisco Artes. Cybercrime Kill Chain vs. Defense Effectiveness. https://www.nsslabs.com/reports/cybercrime-kill-chain-vs-defense-effectiveness, 2012. Available 29/5/2014.

[HCJA11] Eric M. Hutchins, Michael Cloppert J., and Rohan M. Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, Volume 1, 2011.

[HKP13] Bryan Harris, Eli Konikoff, and Phillip Petersen. Breaking the DDoS Attack Chain. Technical report, August 2013.

[HP13] Hewlett-Packard. HP Attack Life Cycle use case methodology. http://h20195.www2.hp.com/v2/GetPDF.aspx November 2013. Technical white paper, available 29/5/2014.

[ILCP13] Georgios Ioannou, Panos Louvieris, Natalie Clewley, and Gavin Powell. A Markov multi-phase transferable belief model: An application for predicting data exfiltration APTs. In *Information Fusion (FUSION), 2013 16th International Conference on*, pages 842–849. IEEE, 2013.

[Man10] Mandiant. M-Trends 2010: The Advanced Persistent Threat. https://www.mandiant.com/resources/m-trends, 2010. Report, available 29/5/2014.

[RSA12] RSA. Stalking The Kill Chain. http://www.emc.com/collateral/hardware/solution-overview/h11154-stalking-the-kill-chain-so.pdf, 2012. Research note, available 29/5/2014.

[Sec13] Dell SecureWorks. Advanced Threat Protection with Dell SecureWorks Security Services. http://www.secureworks.com/assets/pdf-store/white-papers/wp-advanced-threat-protection.pdf, 2013. Available 29/5/2014.