APT detection system using honeypots

ROMAN JASEK, MARTIN KOLARIK, TOMAS VYMOLA
The Faculty of Applied Informatics
Tomas Bata University in Zlín
Nad Stráněmi 4511, 760 05 Zlín
CZECH REPUBLIC
jasek@fai.utb.cz; martin.kolarik@email.cz; vymola@gmail.com

Abstract: - Recently emerged threat type of Advanced Persistent Threats (APTs). APTs continuously gather information and data on specific targets, using various attack techniques examine the vulnerabilities of the target and then perform the data obtained by hacking. APTs are very precise and intelligent. Perform specific attacks on specific targets, and so differs from traditional forms of hacking. APT is precisely focused on specific targets, according to the knowledge of the environment and selects appropriate types of attacks. Therefore, it is very difficult to detect APT attacks. This article describes the methods and procedures APT attacks, analysed and proposes solutions to detect these threats using honeypots system.

Key-Words: APT, honeypot, computer security, attack, Advanced Persistent Threat

1 Introduction

Institutions and businesses always face new threats. One of the biggest problems lately is type of APT threats, which are sophisticated, multiple attacks at a specific organization. Threats type of APT (Advanced Persistent Threat) belongs to the category of cyber-attacks, their goals most often as commercial entities, political and state institution and the individuals. These types of threats require long-term high secrecy. They carried a group of attackers who are well privy to the problem. They use more types of vulnerabilities to break the key security systems. In the initial stage of the APT focus on getting information about the network configuration and server operating systems. Later, focus on installing rootkits and other malware to gain control and communication with C&C (Command & Control Server) attackers. The contested objects are long compromised to steal intellectual property, copying of confidential and sensitive data, or financial gain. Individual systems are often long infected, and the achievement of the objectives striker ever taken out of service.

2 APT

Definitions of precisely what an APT is can vary, but can be summarized by their named requirements below:

Advanced - Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it.

Persistent – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it.

Threat – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well-funded.[3],[1]

ISBN: 978-960-474-316-2

.

2.1 Lifecycle APT

APT has been firmly defined methodology that has been proven in recent years. It begins phishing and social engineering ends and export large volumes of stolen data to the attacker's server. Attackers use techniques and methods are constantly evolving and have a great ability to adapt effectively. They keep their tools a step ahead than the current status of infected systems.

Attackers can have multiple campaigns running in parallel. Every consists of one or more operations. These operations are usually distributed into phases. For example, in the initial phase, the aim is to provide a striker initial entry point to the target system. The following phases are then usually parallelized and distributed among individual cells due to more efficient attacks. The subsequent section describes the basic operation phases within a single APT intrusion. The following section describes the details of these phases and their possible detection. [4], [2]

Initial compromise - This is done using conventional practices of social engineering, spear phishing emails, and with zero-day virus. Next option is to infections websites, and forced the victim to visit them. Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it.[8]

Establish Foothold – install remote administration software in victim's network, create network backdoors and tunnels allowing stealth access to its infrastructure. Connection communication with the Command & Control server the attacker and as he controls remotely contested keeps updating machines and used malware.

Escalate Privileges – use exploits and password cracking to acquire administrator privileges over victim's computer and possibly expand it to Windows domain administrator accounts.

Internal Reconnaissance — collects information on surrounding infrastructure, trust relationships, Windows domain structure.

Move Laterally — expand control to other workstations, servers and infrastructure elements and perform data harvesting on them.

Maintain Presence — ensure continued control over access channels and credentials acquired in previous steps.

Complete Mission — exfiltration stolen data from victim's network

Furthermore, in this article we will focus in detail on the stage Move laterally. Previous phase is detectable by standard quality tools. But if the attacker gets up to the current stage, it means that standard security techniques have failed. This phase is a standard security technique almost undetectable. The attacker behaves as a normal user and using common tools. One of the methods to detect the attacker is using the honeypots.

3 APT Honeypots

While there are many solutions to detect APT, are not all 100% effective. With the honeypot are able to some extent combat APT attackers. In this section we will discuss this problem and propose practical solutions that would form part of a system to detect APT. The concept of the honeynet first began in 1999 when Lance Spitzner, founder of the Honeynet Project, published the paper "To Build a Honeypot": "A honeynet is a network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discreetly regulated." [6]

Honeypot is an information system whose purpose is to attract potential attackers and record their activities. Honeypot is used to detect and analyse attacks on computer networks and systems. Honeypots servers are dedicated servers, workstations and the network collects information about attackers and intruders who attack systems. Honeypots are most often used for the early detection of malware and subsequent analysis of its behaviour. Malware is constantly changing its strategy of attack and different ways to hide and avoid finding. For these reasons, the malware somehow lure and then analyse their behaviour. It is important to remember that the honeypot does not replace traditional security systems, but only complements it. Based on design criteria, honeypots can be classified as pure honeypots, High-

interaction honeypots and Low-interaction honeypots.[5]

Two or more honeypots on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion detection systems. A honeyfarm is a centralized collection of honeypots and analysis tools

For detection system using APT with High-interaction honeypots, Low-interaction honeypots and Honeypot on production systems.

High-interaction honeypots - Honeypot with a high degree of interaction shows a complete real system, with all services and functions. Unfortunately, this method of implementation allows the attack the whole system, including the honeypot.[7]

Low-interaction honeypot - These honeypots simulate only a few features transport layer operating system. In these systems, it is easy to identify the mapped threats, unfortunately detection of new types of attacks is impossible in most cases.[7]

Honeypot on production systems - It is a special version of honeypots, implanted in a production system. If the user does not have access to production systems, allow him to produce the system log. After verification, but is not admitted to the productive version, but in the sandbox, with imaginary data. The attacker feels that operates within the contested system, but is found only in the sandbox, which is monitored. All information about the activities striker transferred to the control system. Depending on the system administrator if this will be a honeypot to inform the user. It can also serve as an opportunity to capture unauthorized access to authorized systems.

Monitoring APT attacks honeyfarm used with any number of High-interaction honeypots, Low-interaction honeypots and Honeypots on production systems, according to the current situation.

3.1. Honeypot agent

Next complement the above solution is a honeypot agent.

The original design of honeypots has one major limitation. Honeypots are waiting for the attacker. Role honeypot is passive. The design of this solution becomes the attacker honeypots notice and carries out its activity without being detected by the system. Therefore, this solution we extended the agent who directs the attacker to the system honeypots. As these types of attacks simulate the behaviour of users, the attacker slip agendas and users little trap. The essence trap lies in the difference between continuous user behaviour and bot. The user of the system is using the agent set a trap. The average user is hidden at first sight, or not interesting for his work. For example, a typical user ignores file system, various TMP directories, and the like. Bot trying to do the contrary, collecting information about invaded system, it searches every corner of systems. This is the stage where they come onto the scene Honeypot systems that offer interesting information for bots. The next chapter will present all the steps of how the system works.

3.1. Step-by-Step Description

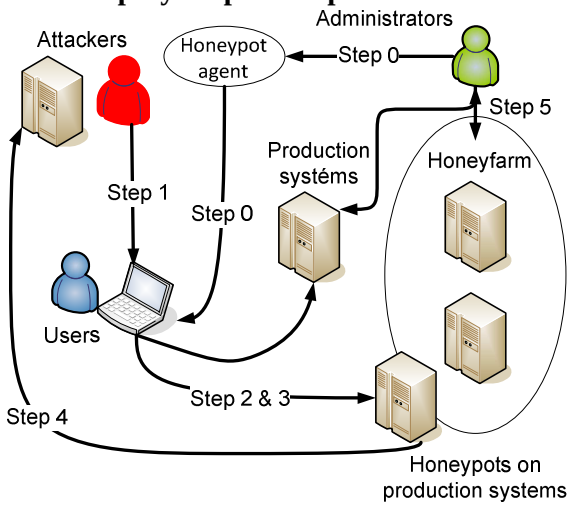

Fig.1 The procedure the attack on Honeyfarm

3.1.1 Step 0

Institutions will connect own network with Honeynets, containing various types of honeypots. Activated systems on Low interactive honeypot, High interactive honeypot and Honeypot on production systems. Agent activates a trap for attackers on selected systems.

3.1.1 Step 1

The attacker had risen to attack the weakest phase Internal Reconnaissance and compromised systems. Subsequently seeks to expand its activity to other parts of the network or systems which are the main interest of the attacker. It is highly likely that decodes any of the trap set by the agent. It explores the system, decodes passwords and collects a wealth of information. Standard command can find e.g.: List the services that have started on the victim system, list currently running processes, list accounts on the system, list accounts with

ISBN: 978-960-474-316-2

administrator privileges, list current network connections, list currently connected network shares, list other systems on the network, list network computers and accounts according and other.[2]
But for example in list currently connected network share finds the shared disks planted agent.
Once an attacker has any legitimate authority, subsequently proceeds to stage Lateral Movement. At this stage, according to the information obtained may legitimately be in the network. If he has the law, he can connect to shared resources on other systems, he can run commands on other machines without arousing suspicion.

3.1.2 Step 2
The attacker logs on to a honeypot systems, according to information obtained on compromised systems from the previous step.

3.1.3 Step 3
The attacker invades honeypot systems and compromises them.

3.1.4 Step 4
The attacker collects data from infected systems and honeypots. Furthermore sends the information to its Command & Control server.

3.1.5 Step 5
Administrator detects accesses to the honeypot system and applies safety rules on production systems, misused blocking honeypot, misused blocking accounts. It can then analyses the process of attack and establish rules and procedures to defend the weak spots.

3.2 The activity of attacks
The following chart recorded a number of anti-virus detection systems and antimalware a number of incidents captured by honeypots running in the selected time period for a non-homogeneous network. The environment consists of 400 systems under the control of the administrator, as well as about an average of 300 to 400 devices on private property without the possibility of influencing their management. Honeypot agent was installed about 15% of the stations.

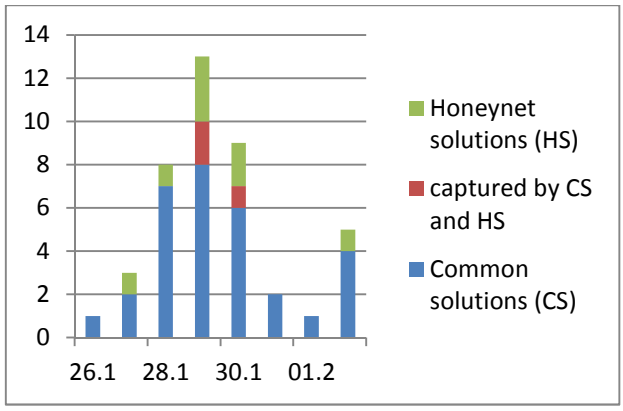

Fig.2 Number of incidents captured during the period

Incidents, are marked as blue, captured by conventional anti-virus and anti-solutions. The green marked attacks are detected only by the honeypots. Red is marked by the intersection of the two types of detection. The attack was detected using the Common solutions and Honeynet solutions. More successful Common solutions is expected, an attack captured in the beginning. These attacks are mostly in documented and there is a defence for them. Unfortunately, some new types can bypass this protection, and then it can only be detected using the honeypots. These intersections are the most targeted, more destructive and more dangerous.

3.2 Some Interesting Features
Compared with other antimalware and anti-spyware solution, the solution proposed some interesting features:

Function 1
Standard detection solution is supplied from external suppliers, and directly targeted attacks are to learn to do without. APT attacks can in some cases outperform. Honeypot system offers an additional level of defence and detection, after overcoming a standard solution. It is able to detect the effects of charge from the 0-day exploits on days vulnerabilities, for which standard solutions can not react in time.
Function 2
This solution can be independent of the operating systems of individual users. Omitting the agent is decreasing its ability to detect, but on some systems cannot use any standard solutions. For example: operation systems in printing devices.
Function 3
This addition to the standard security solutions can, in combination with other systems to improve their

ISBN: 978-960-474-316-2

performance and increase the efficiency of detection of the attack.
Function 4
By intercepting attacks on honeypots can be analysed for the attack and using the information collected we can better secure vulnerabilities of systems.
Function 5
After analysing captured on honeypots can determine which accounts were compromised, then you can only block the system. We do not exclude the operation of the whole system, just fix the compromised section. Saving considerable financial resources.
Function 6
Basic setup honeypots without an agent does not have any additional requirements (software or hardware) to the user. Users do not even know about this defence system. This solution is for him invisible, which is the case of standard detection systems, the exact opposite.
Function 7
Possibility of detection of attacks on mobile devices, which are beyond the control of the administrator network segment. Detects attacks that are not specifically targeted.

Detection solution using honeypots is unnecessarily expensive and complicated as most systems to detect attacks. Is the use of standard techniques and instruments. To detect APT use their own shortcomings in system APT.

4 Conclusion

APT attackers will always have an interest in your data. They are highly adaptable and monitor deficiencies in the security of your systems. If they are able to penetrate the defence can monitor your systems and collect data. This data is then used to infiltrate into other systems. The information obtained could be used for business meetings, and can have economic and strategic implications. Analysis of incidents will help us improve our infrastructure and can focus on fixing vulnerabilities. We can then better focus on the monitoring and audit of specific systems. Planning these strategies forward, it will be much harder for attackers to infiltrate systems and obliterate his tracks. Maintenance IT environment, effective patch management are important steps to eliminate opportunities for initial penetrations. With increased awareness of users can mitigate attempts by social engineering. Removing local admin rights to users, we can reduce the risk of privilege escalation.
Migrating users to a cloud environment with thin clients may be a remedy, though cloud solutions currently face their own challenges.[9]
Simulation threats through penetration testing and test exercises are good grounds for the creation of effective security strategies. Without a thorough understanding of the threats and good security strategy, security spending will be ineffective and an inefficient.

References:

[1] *Advanced Persistent Threats (APT): What's an APT? A Brief Definition*. DAMBALLA. [online]. 2010 [accessed on 2013-05-11]. Available at: https://www.damballa.com/knowledge/advanced-persistent-threats.php

[2] APT1 Exposing One of China's Cyber Espionage Units. [online]. p. 74 [accessed on. 2013-05-11]. Available at: http://www.mandiant.com

[3] COMMAND FIVE PTY LTD. *Advanced Persistent Threats: A Decade in Review*. [online]. 2011, p. 13 [accessed on 2013-05-11]. Available at : http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf

[4] DELL SECUREWORKS. *Lifecycle of the Advanced Persistent Threat*. [online]. 2012, p. 16 [cit. 2013-05-11]. Available at: http://go.secureworks.com/advancedthreats

[5] Honeypot Background. PROVOS, Niels. *Honeypot Background* [online]. [accessed on 2013-05-11]. Available at: http://www.honeyd.org/background.php

[6] SPITZNER, Lance. *Honeypots tracking hackers*. Boston: Addison-Wesley, 2003. ISBN 0-321-10895-7.

[7] SPITZNER, Lance. *Honeypots: Definitions and Value of Honeypots. Virtual honeypots: from botnet tracking to intrusion dedction* [online]. Upper Saddle River: Addison-Wesley, 2008 [accessed on 2013-05-11].

[8] TREND MICRO. Targeted Attack Entry Points: Are Your Business Communications Secure?. [online]. 2012, p. 5 [accessed on 2013-05-11].

[9] SARGA, Libor. *Is it Going to Rain From the Cloud? Challenges of Ubiquitous Computing Models*, Proceedings 8th International Bata Conference for Ph.D. students and Young Researchers, 19th April 2012, Zlín, Czech Republic.