Position papers of the Federated Conference on Computer Science and Information Systems, pp. 113–117
DOI: 10.15439/2017F488
ISSN 2300-5963 ACSIS, Vol. 12

Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection

Artur Rot
Wroclaw University of Economics
ul. Komandorska 118/120
53-345 Wroclaw, Poland
Email: artur.rot@ue.wroc.pl

Boguslaw Olszewski
University of Wroclaw
Pl. Uniwersytecki 1
50-137 Wroclaw, Poland
Email: boguslaw.olszewski@uni.wroc.pl

***Abstract*—According to Kaspersky Lab research, APT – Advanced Persistent Threats – are one of the biggest threats in IT as of 2016. Organised groups, keeping contact in various languages, have attacked the IT systems of financial institutions, government, military and diplomatic agencies, telecom and power supply companies, politicians and activists, and private companies, and these attacks were global in scope. APT should be seen as a complex phenomenon, an existing danger to companies, organisations and public entities. This article showcases the problem of APT, the biggest threats related to them, and chosen methods and tools that can be effectively used to counter APT attacks. An effective, multi-layered defence model is outlined in the article as well.**

I. Introduction

The term "cybersecurity" has become very popular nowadays, and the problems of Internet security and of protecting internal networks of various organisations are discussed widely, not only in everyday life, but also in various business sectors. Despite hundreds of millions of PLN spent by companies annually on cybersecurity, most organisations are constantly under threat of APT, which remain undetected for months and cause tangible losses in company functioning and image [15]. Companies and government institutions are increasingly often the target of APT attacks, difficult to detect and leaving no traces. In 76% of organisations harmed by APT, antivirus software and breach detection systems did not block the attack. Examples of effective attacks on not only international companies, but Polish government agencies as well, show that APT attacks are a new field of battle for the government, commercial companies and criminal organisations. During *the Infosecurity Europe 2011* conference, APT were included among the biggest cyber threats of the modern world, and their character requires a different approach than the one usually in use. According to the Deloitte *report Cyber Espionage – The harsh reality of advanced security threats* [4], the key factors in fighting the newest cyber threats, including APT, are: constant risk evaluation, implementing offensive security means, and training staff to appropriate responses [5] [18]. The subject of cybersecurity suffers, however, from insufficient research and literature, due to its constantly changing environment and designates – this, in turn, caused by its changing technological, social, military and political aspects. A similar problem can be observed with APT, a phenomenon that is still developing and as such should be considered in more depth. Thus, the authors of this article aim to present the phenomenon of APT and to fill the gaps in subject literature as to the APT dangers for practically any organisation and company, and the methods and means of defence against the attacks. Authors have also presented an effective, multi-layered defence model.

II. APT Attacks – A New Form of Cyber Threats

APT attacks are a complex, long-term set of actions aimed against specific persons, organisations or companies. They are most often instigated by attackers who study a given company and its staff for months before initiating the attack. They use tools which minimise the chances of detection, and can thus steal data over a long period, perhaps over many months. The APT attacks differ from security breaches hitherto known by exactly that – the difficulty in detection and the wide scope [5].

APTs are defined as a new and more sophisticated version of known multistep attack scenarios and they are targeted specifically to achieve a specific goal, most often espionage [7]. They are "advanced" in that the malware they use is advanced, but also the character of the danger they pose. APTs use complex tools and are aimed to sabotage, steal confidential data, to defraud or blackmail. Hackers causing APTs are not only very well educated, but also have tools and funding necessary for making these threats effective. Their complex methods of introductory research and background checks are not, however, revolutionary and make use of known social engineering. These remain universal, despite a large body of knowledge and counter-strategies. It's the network access and the attack itself that make the persistent threats advanced.

The other distinctive trait of APTs is their Persistency, related to the character of operations. APTs are not incidental, they form a cohesive strategy that aims to fulfil a larger goal. The priority is to remain undetected as long as possible, systematically fulfilling this goal. These goals are

usually financial profits. The threat is mostly related to the human factor, the highly organised groups. They are strongly motivated (by their hierarchy or by financial possibilities), they create command chains and specialised subgroups dealing with specific parts of an APT attack. The APT attackers are usually specialised teams of IT professionals and their clients – usually governments – using advanced technologies and obscure points of attack to obtain sensitive data. APTs are also called directed attacks, since the targets are chosen deliberately and studied beforehand to find the best point of attack.

III. Crucial Points of an APT Life Cycle

A typical APT life cycle (see Fig. 1) is divided into four stages: reconnaissance, initial compromise, establishing foothold and infiltration. Reconnaissance allows to find effective points of attack, evaluate target susceptibility and the people within the organisation who can, actively or passively, facilitate security breaches. These may be employees without any crucial access credentials, but who can allow for further infiltration of a given system in the long run.

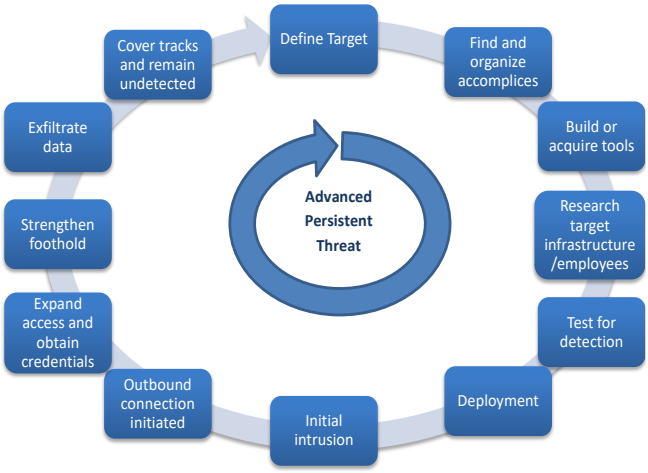

Fig. 1. APT life cycle [20]

The preparation stage allows for the second stage of an APT life cycle. An initial compromise is the result of the attackers gaining access to some element of the internal network: a desktop computer, a network device, a PC, pendrive or smartphone of a specific person who has high credentials, or someone who uses such hardware in their professional or private life. This is facilitated by unauthorised use of private devices within the professional network, and an inclusion thereof into the corporate IT system. Social engineering is important at this stage, as it is at the previous stage: APT attackers usually introduce malware, Trojan horses or apps that allow for further remote actions within the network with help from social engineering.

A negative attempt at detection allows further intrusions and malware introduction, which in turn creates a communication channel for the attackers (Command&Control Server, C&C). The third phase is assuming control over the desired parts of a system and possibly over other users, in order to gain access to whatever data is the main objective. The fourth stage entails a long term infiltration process based on credentials obtained, and later on, escalating access privileges to gain more power and at the same time make the breach less noticeable. Obtaining or destroying the crucial data is initiated - whatever was the objective of the hackers or their clients. When it's done, the attackers retreat and cover their traces, deleting signs of their presence and any data that might allow for identifying the source of the attack.

IV. Exploiting Vulnerabilities

Treating APT as cheap sensationalism or another marketing campaign is underestimating and misrepresenting the phenomenon. Thus, the first source of vulnerability to APT is the human factor, especially the low awareness of APT danger and the techniques used by APT attackers. Lack of this awareness leads employees to behaviour they themselves don't know is irresponsible, both in the workplace and their private life, opening entrance points for an APT attack [17]. Knowledge and awareness on the part of network admins, IT security teams and especially decision-making personnel, who assign funds and implement procedures, is also important.

Social engineering and widely available information about specific employees (blogs, social media, company websites) allow the attackers to pinpoint the individuals with high level credentials, allowing access to strategic data or network resources, or simply individuals who can inform the attackers about the next target on their way towards these credentials, towards their objective and the next APT stage. Knowing an employee's profile, the attackers evaluate their weaknesses and possible means of approaching them, including blackmailing or bribing them into offering their abilities and means to the attackers.

A directional APT means a complex, multi-faceted process aimed at achieving the goals of specific stages. From the social engineering angle, this means spear phishing – an unauthorised access to data, network resources or hardware, through a specific person, including accessing resources belonging to another employee or even organisation. Spear phishing begins right at the reconnaissance stage, and culminates in a personalised phishing attack, wherein the victim receives a personalised email and, convinced about its safety and trustworthy source, opens attachments or clicks provided links.

Social engineering, exploiting personal vulnerability, is one of the most important means of initiating an effective infection of the target network, and is the most popular method of accessing the necessary resources. The second

most effective type of attack is the zero-day attack, exploiting software vulnerabilities. Hackers use them to circumvent classical defences, based on software signatures in antivirus and firewall programs. Numerous vulnerabilities can be also found in hardware, and these are increasingly used with the spread of wireless devices. Hardware vulnerabilities complement software vulnerabilities, especially in microchips, where manufacturers often leave an access point on purpose, to use in post-manufacturing tests [11].

Business organisations and companies are the most popular targets of APT attacks, with education, finance, technology, space exploration and aviation, power supply, chemistry, telecom, medicine and consulting being the most often targeted branches.

V. Defence Against APT Attacks

The most successful form of defence against APT is constant monitoring and reaction to as many APT attempts as possible. Identifying an attack attempt through any channel makes that channel obsolete. Strategies of defence based on one or two APT levels are insufficient: as mentioned before, in 76% cases, antivirus software was no obstacle at all to APT attacks [4]. Therefore, first generation security means are not enough to protect valuable targets, and prevention systems do not guarantee protection anymore. Experts confirm that "any effective approach to defending against APTs must include defence in depth, a detection capability, an APT incident response plan, a recovery plan, and security awareness and training" [2].

The basic means of countering APT attacks are a set of basic procedures that limit the relatively simple elements of the APT process. When APT is divided into its basic elements, these usually prove to be well known and easy to counter. It is their combination, especially in a sequence created specifically for a given target, that makes defence against APT difficult. This is why even the best means of network security, including proxy servers, firewalls, VPN and antivirus software cannot defend against an APT on their own. Initial protection methods include implementing a vulnerability management process, system updates and penetration tests. These should be complemented by detailed documentation on influence and risk evaluation. Determining the crucial resources and the elements in need of special protection is vital, especially for business targets.

Pro-active protection allows to eliminate a point of attack right at the preparation phase, excluding it at the planning stage. The more points of attack are blocked, the more time, effort and resources must the APT attackers spend. Protecting vulnerabilities, using antivirus software and blacklisting requires modification and real time protection: in-line bi-directional scanning and behavioural analysis. Among desirable solutions is SSL protocol scanning, allowing for advanced detection of potential intruders. Similarly to APT threats themselves, means of protection must be long-term and persistent, especially given the rising use of wireless devices, the presence of which within the organisation must be constantly monitored.

Another type of means of protection is detecting an ongoing APT. This entails chiefly the ways of detecting malware already introduced – programs that keep up and speed up an APT attack. The biggest problem with APT malware is the fact that neither antivirus software nor IDS (Intrusion Detection System software) will have its signature in their databases. Attackers use evasion techniques to hide malicious code, which is polymorphic and customised to a given target, or dynamically modified during the attack. Detecting APT will activate the means used to contain and isolate it, and to return to the state from before the attack. This is the third category of APT protection. Its main components are an online analysis (determining the traits of a specific APT), real time reporting and correlated log analysis, for example based on SIEM (see below), in order to recognise and neutralise a threat in the future. The last element is evaluating the entirety of implemented methods.

Two main types of APT defences can be distinguished today: hardware-based and cloud-based [17]. In the first case, a dedicated device is placed on the edge of the protected network, monitoring and informing about suspicious traffic basing on reputation indexes (it does not block transmission in real time). More advanced models perform behavioural analysis and sandboxing.

Hardware-based solutions have certain limits. Despite high costs – which limit their numbers, and restricts use to big companies, especially for models that monitor encrypted traffic – these devices are not able to register the entirety of network traffic, given the rising use of mobile devices and remote workstations. The alternative cloud-based solutions are supposed to eschew most of the limitations of hardware-based solutions. These are supplied as a multi-user platform and offer more effective traffic monitoring, threat intelligence in real time on every APT stage and are scalable. The hardware approach is replaced by holistic analysis (behavioural, vulnerabilities, address filtering, SSL transmission monitoring, active content etc.) Practise shows that mere observing procedures and basic protection is not nearly enough to shield from APT, hence the importance of advanced, multi-layered protection methods described below in the end-to-end strategy.

A. Multi-layered APT Protection Model

Another solution for APT protection is the so-called defence-in-depth. It's a multi-layered strategy that entails careful protection of each layer of the network: the people, the devices and applications. It's complex character significantly increases the chance of successfully resisting an APT attack, since it's based on permanent monitoring of the network and security control.

Defence-in-depth means, therefore, a layered approach to network security, and taking steps to detect a threat, react to

it and eliminate it, in every layer. The seven-layer model based on OSI creates an environment where none of the layers protects against an APT on its own, but their combination is a cohesive barrier. The model also entails physical security means, carried out through protecting the organisation space – protecting facilities where devices are stored, eliminating vulnerabilities caused by nature or by contact with outsiders, etc.

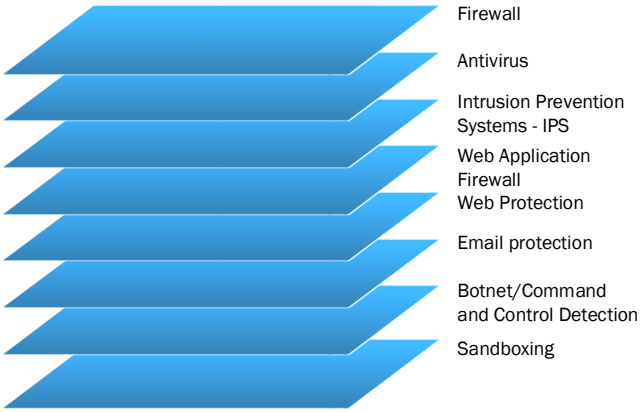

Fig. 2. Layered APT defence model [9]

In the end-to-end strategy presented below (see Fig. 2), a firewall software is the first line of defence against an APT, blocking ports and filtering packets. Next generation firewalls (NGFW) usually combine the typical functions of firewalls (packet filtering, website blocking, virtual IP addresses) with IPS, application control and context protection (e.g. Cisco ASA 5500-X Series). Antivirus software is another layer that limits potential system breaches, since it scans all packets (not just their headlines), as well as compressed and encrypted files.

The next element, an Intrusion Prevention System (IPS), allows for an in-depth monitoring of network traffic and vulnerabilities, especially if equipped with zero-day threat minimising mechanisms. It's a successor of the Intrusion Detection System (IDS), which was based on passive monitoring and danger reporting based on an analysis of network traffic copy, remaining integrated into the data flow and allowing for blocking. The two systems also differ by their functioning: IDS uses exploit signatures, while IPS included detection based on anomaly statistics and vulnerability signatures.

A Web Application Firewall is a transparent system of vulnerable web app protection, which works basing on whitelists and blacklists – a database of permitted and banned elements. This allows to protect the servers working in the demilitarised zone, which most often host organisation websites.

The multi-layered model is complemented by the web protection layer, the email monitoring component, and the sandbox – an isolated test environment, either virtual or supplied by hardware.

B. SIEM Platform as a Form of Defence Against APT Attacks

Another suggested method of APT defence is implementing second generation SIEM tools (Security Information and Event Management) – a platform allowing for managing information relating to security and incidents (see Fig. 3). Monitoring diffused system logs, network devices and applications in real time allows for more effective control over processes and resources, and for intercepting proof of an ongoing APT in the operative risk management phase, basing on compromise indicators. Forensic analysis allows to determine the origin, character and type of a given event on a given device, as well as other components indicating a vulnerability.

SIEM platforms, available on the market since the late nineties, are still in development and currently await upgrades in their report and correlation functions. However, implementing an SIEM system even in its current form is a significant upgrade of an APT defence. SIEM functional components offer "collection and archiving data, detailed event and normalisation analysis, reports, queries, and usually some form of a real-time analysis module" [14]. Until fully developed SIEM tools appear, implementing them in their current state should be an auxiliary measure, and clients should selectively define their priorities and choose the most adequate mechanisms. Data volume is a separate question, requiring the use of terabyte disks or data clouds, and influencing response time. A typical SIEM will process several hundred thousand events per second.

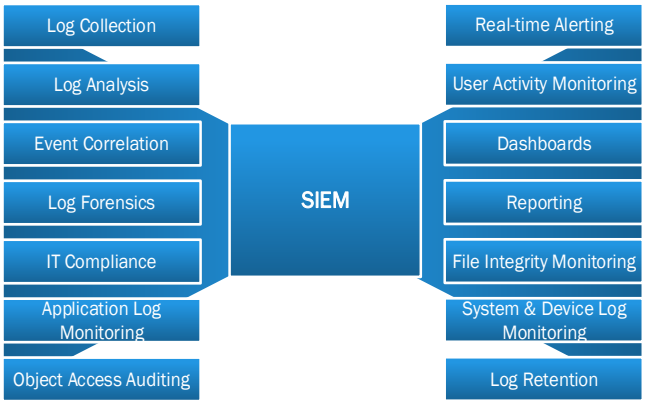

Fig. 3. Security Information and Event Management [21]

Among the most important platforms are, for example, QRadar IBM, Q1 Labs Qradar, and NetIQ Security Manager. These solutions have limits as far as analysing data gathered for months or years is concerned [1], which means that a new generation of APT defence becomes crucial.

C. Big Data Technology in Detecting and Resisting APTs

The third generation tools are technologies of large-scale data management: Big Data, also called second generation SIEM. It allows to analyse large quantities of data and can generate and transmit it quickly, as well as search for

variables and unstructured resources. This means it fits APT protection processes very well. Technologies such as Apache Drill or Dremel allow to analyse streaming data in real time, and therefore propose to use an APT detecting mechanism through an integrated log analysis and anomaly detection based on a typical pattern customised for a given organisation [8], or behavioural analysis based on Big Data. It has been proven that solutions based on MapReduce, Hadoop or Hive allow to shorten the analysis time about twenty times [1]. IBM combines their Qradar SIEM system with a Big Data platform [10], sending data collected even over several years to further analysis in SOC. Zscaler company offers a Zscaler Cloud Sandbox [22]. Big Data technologies are currently one of the most promising ways of APT defence, especially given the rapidly increasing amount of data: in 2013, the Hewlett-Packard network alone generated 12 million events per second [3].

I. Conclusion

The above is not an exhaustive presentation of means and technologies of preventing, detecting, and eliminating APTs. The market offer expands dynamically, as do the theoretical foundations of such defensive actions. Among other offers of APT protection are such technologies as deep learning (SignalSense), requiring a new approach to network security, constant monitoring, adaptation and learning through experience [19]. PwC, in its *Global State of Information Security Survey 2015* notes that within organisations, it was the current (31%) or former (27%) employees are the source of insider threats [13]. Therefore, more attention should be paid to monitoring internal traffic, in this particular example, based on Neural Network (scalable detectors, host classification, IP, packets and traffic reputation), which searches for divergences from the usual pattern of network behaviour.

To summarise, strategies for organisations include integrated information exchange between security points, advanced prevention and detection, including a broad strategic approach (tactical hardware configuration and attack scenarios), SSL traffic monitoring and ensuring full protection.

References

[1] *A Case Study In Security Big Data Analysis*, 2016, http://www.darkreading.com/analytics/security-monitoring/a-case-study-in-security-big-data-analysis/d/d-id/1137299

[2] Ashford W., "How to combat advanced persistent threats: APT strategies to protect your organization", 2016, http://www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation

[3] Cárdenas A.A., Manadhata P.K., Rajan S. (eds.), *Big Data Analytics for Security Intelligence*, Cloud Security Alliance, 2013, https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_ Intelligence.pdf

[4] *Cyber Espionage: The harsh reality of advanced security threats*, Deloitte: Center for Security & Privacy Solutions, 2016, https://www.isaca.org/chapters1/phoenix/events/Documents/cyber_espionage.pdf

[5] Gajewski, M., „Cyberataki typu APT nowym frontem wojny", Chip.pl, 2013, http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa /2013/03/cyberataki-typu-apt-nowym-frontem-wojny

[6] *Cyberbezpieczenstwo 2016: 5 trendow, jakich powinnismy sie obawiać*, http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/914855,cyberbezpieczenstwo-2016-5-trendow-jakich-powinnismy-sie-obawiac.html

[7] Ghafir I., Prenosil V., "Advanced Persistent Threat Attack Detection: An Overview", *Proceedings of International Conference On Advances in Computing, Electronics and Electrical Technology*, Kuala Lumpur, 2014 p. 154

[8] Kim H., Kim J., Kim I., Chung T., "Behavior-based anomaly detection on Big Data", *The Proceedings of the 13th Australian Information Security Management Conference 2015*, Perth, 2015, pp. 73-80

[9] Hudson B., "Advanced Persistent Threats: Detection, Protection and Prevention", Sophos, 2013, p. 6. https://www.lifeboatdistribution.com /content/vendor/sophos/whitepaper-sophos-advanced-persistent threats-detection-protection-prevention.pdf

[10] *IBM Security Intelligence with Big Data*, http://www-03.ibm.com/security/solution /intelligence-big-data/

[11] Jover R.P., Giura P., "How vulnerabilities in wireless networks can enable Advanced Persistent Threats", *International Journal on Information Technology (IREIT)*, No.1 (2) 2013, p. 145- 151, http://www.research.att.com/techdocs/TD_100739

[12] Kim J., Lee T., Kim H., Park H., "Detection of Advanced Persistent Threat by Analyzing the Big Data Log", *Advanced Science and Technology Letters* 2013, vol. 29 (SecTech 2013), p. 32

[13] *Managing cyber risks in an interconnected world. Key findings from The Global State of In-formation Security Survey 2015*, PWC, 2014, http://www.pwccn.com/home/webmedia/635527689739110925/rcs_info_security2015.pdf

[14] Muszynski J., Shipley G., "Narzedzia SIEM (Security Information and Event Management)", 2016, http://www.computerworld.pl/news/325855/Narzedzia.SIEM.Security.Information.and.Event.Management.html

[15] Pietrzak P., „Jak skutecznie obslugiwac zaawansowane ataki APT (Advanced Persistent Threats)", https://magazyn.mediarecovery.pl/jak-skutecznie-obslugiwac-zaawansowane-ataki-apt-tzw-advanced-persistent-threats

[16] Rot A., Sobinska M., "IT security threats in cloud computing sourcing model", M Ganzha, L Maciaszek, M Paprzycki (eds.) *Proceedings of the 2013 Federated Conference on Computer Science and Information*, PTI, Cracow 2013, fedcsis.org/proceedings/2013/pliks/fedcsis.pdf

[17] Rot A., "Zarządzanie ryzykiem w cyberprzestrzeni – wybrane zagadnienia teorii i praktyki", *Projektowanie i realizacja systemow informatycznych zarzadzania. Wybrane aspekty*, Komorowski T.M., Swacha J. (eds.), Polish Information Processing Society PTI, Warsaw 2016

[18] Rot A., "Enterprise Information Technology Security: Risk Management Perspective", *Proceedings of the World Congress on Engineering and Computer Science 2009*, Vol II, 2009, pp. 1171-1176

[19] *Using Deep Learning To Detect Threat, SignalSense*, White Paper, p. 2. http://www.ten-inc.com/presentations/deep_learning.pdf

[20] Virgillito D., "Cyber Crime Security Risks for Healthcare Companies", 2013, http://massivealliance.com/2013/12/18/cyber-crime-security-risks-healthcare

[21] Why Should Enterprises Choose EventLog Analyzer as Their SIEM Solution? https://www. manageengine.com/products/eventlog/manageengine-siem-whitepaper.html

[22] Zscaler Announces Comprehensive Cloud-based APT Solution, https://www.zscaler.com/press/zscaler-announces-comprehensive-cloud-based-apt-solution