AARMS Vol. 17, No. 3 (2018) 101–113. 10.32565/aarms.2018.3.7

Analysis of Cyberattack Patterns by User Behavior Analytics[1]

Csaba KRASZNAY,[2] Balázs Péter HÁMORNIK[3]

Targeted attacks cause the most serious problems nowadays in the cyberspace, as in most cases they are used for cyber espionage, in cyber warfare activities and have a significant role in data leaks both in the governmental and private sector. Meanwhile, it is very difficult to detect such attacks in time, due to the strategy, tactics and chosen tools behind them. Therefore, a new way of cyber defense is needed to reduce risk caused by Advanced Persistent Threat (APT). In this paper we review the process of targeted cyberattacks, focusing on the challenges of authentication, then we introduce user behavior analytics (UBA) as a potential countermeasure. We also emphasize through a case study, how devastating a cyberattack can be for a company and why UBA would be a good candidate in a modern cyber defense system.

Keywords: *user behavior analytics, cyberattack, targeted attack, authentication*

Introduction

Per definition, information security is a reactive activity, as it has to manage those risks that may have a serious effect on the organization, if they happen. Historically, the Pareto principle is true here. It states that, for many events, roughly 80% of the effects come from 20% of the causes. Therefore, departments responsible for information security try to focus their limited resources to those 20%. Sometimes it works, sometimes not. In the past decades, a simple firewall or an antivirus software was enough for preventing the vast majority of attacks. Meanwhile, tools and tactics on the attacker side were continuously evolved and evaded the already implemented measures. Moreover, IT usage patterns of employees and customers has also been changed that resulted an infinite loop in the risk management process with constant re-evaluation of threats and finding the right countermeasures for the identified risk. The Pareto principle cannot be used anymore in cyber security. All hardware and software elements with or without network connectivity can be the source of an attack. There are various motives and strategies on the rogue side that are unpredictable from the CISO's chair. In this paper we analyze how new technologies can tackle this challenge. We are focusing on the problems of authentication and behavior analytics as a good example of future technologies that can reduce the risk of some specific but serious cyber security threats.

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-entitled "Public Service Development Establishing Good Governance" in the Ludovika Cybersecurity Workshop.

[2] Ph.D., Associate Professor, National University of Public Service, Faculty of Science of Public Governance and Administration; e-mail: krasznay.csaba@uni-nke.hu

[3] Ph.D., Associate Professor, Budapest University of Technology and Economics, Faculty of Economic and Social Sciences; e-mail: hamornik@erg.bme.hu

Cyber Security Challenges of our Time

Challenges of security professionals can be described best with two definitions. A few years ago, they had to deal with the questions of information security. As the ISO 27000:2018 standard states "The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable." [1] Nowadays, it has to be understood that cyber security is much more complex. The International Telecommunication Union defines this term as: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- availability;
- integrity, which may include authenticity and non-repudiation;
- confidentiality." [2]

If we are trying to keep the topic simple, we can say that there are two major types of cyberattacks. The first one is similar to a shotgun. Attackers shooting out their virtual bullets to the internet not knowing who the victim will be, if any. Ransomware is a good example for this. Cybercriminals own or rent a botnet and spreading their malware through this network, using those e-mail or social accounts that were stolen before from an internet service provider's large database and were sold on Darknet. Their investment is quite low, but the income can be very high, if they are able to mislead a lot of unsuspecting internet users with a well-constructed message. With the ransomware-as-a-service model, virtually everyone can create his own code, spread it to the target audience and harvest the paid ransom in Bitcoin. In such cases the motive is fairly simple: earn as much money as possible. As they are usually targeting end users, they are building on their ignorance, the fact that they do not understand how things are going in the cyberspace. Unfortunately, those home users are many times sitting in an office and use corporate devices connected to the corporate network. From the defense perspective, this type of attack seems to be manageable, although still causes huge problems for those companies who did not invest into human awareness or latest technologies.

The second model is similar to a sniper's rifle. It targets only one organization with a special cyber weapon crafted and sharpened against its weaknesses. Many times, this attack is indirect as attackers hack a trusted third party first and reach the target organization from their network. Rogue actor has the necessary resources, such as time, money and expertise and it has a special motivation why it does this intrusion. We can call this type of activity targeted attack or Advanced Persistent Threat (APT). The National Institute of Standards and Technology in the USA defines this term as "an adversary that possesses sophisticated

levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives." [3: 6] As the intruder can use any vulnerability in the infrastructure, from the defense perspective this is similar to find the needle in the haystack. Meanwhile the initial steps were usually taken months or years before and usually stay under the radar, exfiltration needs seconds or minutes. Victims do not have time to even realize that something bad has happened.

The Process of Cyberattack

To understand why commonly used security measures, fail, we have to understand the nature of targeted attacks. Lockheed Martin in its well-known Cyber Kill Chain [4] model defines an APT in the following seven steps:

- *Reconnaissance:* Attacker defines its target, gets as much information as possible from it, and tries to find vulnerabilities in the target infrastructure.
- *Weaponization:* Attacker creates a cyber-weapon that enables remote access to the target infrastructure. This is usually a malware, such as a virus or worm, which exploits one or more identified vulnerabilities.
- *Delivery:* Attacker delivers weapon to victim. It can be transmitted via e-mail attachments, websites or USB drives.
- *Exploitation:* Cyber weapon takes effect and exploits relevant vulnerabilities on the target network.
- *Installation:* Cyber weapon opens a remote connection, usually a backdoor and lets attacker access the target infrastructure.
- *Command and Control:* through the already opened access, cyber weapon lets the attacker to persist its presence on the victim's infrastructure.
- *Actions on Objective:* as the attacker has goals, it takes the necessary actions towards them, such as data exfiltration, data destruction, or encryption for ransom.

Naturally, those seven steps cover hundreds of tactics, thousands of known tools and the same amount of currently unknown tools. With that wide variety of tools and technics only imagination sets limits to attack strategies. NotPetya ransomware is a good example how well-known tools and tactics enable a new strategy. [5] Based on experts' opinion, the motivation behind this malware was to influence Ukraine's normal daily operation and to test the resistance of maritime industry, though it seemed like an ordinary ransomware. It utilized the same EternalBlue vulnerability like Wannacry did a month before and used the hacker's favorite Mimikatz tool to extract privileged accounts from the memory. Nothing what we did not see before. But the malware is believed to be originated from

the software update mechanism of M.E.Doc, a Ukrainian tax preparation software, widely used in the country. No one expected that the source of a global malware campaign would be a local software's update, that by definition, has to be installed due to security reasons. Masterminds on the attacker side did their job perfectly as they built on known vulnerabilities, both on the human and technology side and utilized already existing tools and techniques to reach their strategic goals, whatever those might be.

The MITRE Corporation, which is a not-for-profit organization that operates research and development centers sponsored by the federal government, published a huge database on cyberattack tactics and techniques. MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. It fits well to Lockheed Martin's Cyber Kill Chain and provides a good insight as to how those seven steps can be carried out. During the pre-attack phase, that is Step 1–4, 173 different techniques were identified under 17 attack categories. In the attack phase, between Step 5–7, 10 categories were set up for 169 techniques. The attacker can freely use these techniques, meanwhile implementing countermeasures against all of these steps is virtually impossible in a complex environment. [6]

In a targeted attack, the turning point is when the rogue actor tries to break out from the already hacked computer. This is the so-called lateral movement. MITRE's framework enumerates several potential techniques how an attacker can extend its footprint. Back to NotPetya, the ultimate goal of gathering credentials from an infected computer was to enable lateral movements. Credentials of privileged accounts mean the keys to the kingdom, if the intruder can e.g. steal such passwords, it is very difficult to find him as from that point, he will do apparently legitimate activities. This can be presented through the Remote Desktop Protocol (RDP) example.

FireEye's Mandiant, that deals mostly with investigation of targeted cyber security incidents, writes the following on its blog: "While performing incident response, Mandiant encounters attackers actively using systems on a compromised network. This activity often includes using interactive console programs via RDP such as the command prompt, PowerShell, and sometimes custom command and control (C2) console tools." [7] Usage of RDP is also confirmed by MITRE as based on its information, even the most advanced cybercriminal groups, such as APT1 or Lazarus used this protocol many times. In practice, Windows servers usually enable remote connection through RDP as they need to be managed somehow. Those servers can be on premise or in the cloud, as well. Therefore, if the attacker has a privileged account, he has a great chance to access the whole Windows infrastructure.

Challenges of Authentication

How can RDP connections be secured? If we browse for this topic on the internet, we can find several good advices of strong password usage to enable Network Level Authentication, but none of them solves the issue of stolen credentials, even password managers can be tricked with an authorized privileged user account. Only multifactor authentication seems to be an effective measure, but many times, this is unfeasible due to infrastructure restrictions and attacks against multifactor authentication can be seen before.

As Mashable highlighted from the previously leaked NSA files, some governmental employees were attacked by "hacking" their two-factor authentication at Google through intercepting and forwarding their verification code. Although, in fact that is not a "hack", rather a good example of how social engineering can help in a man-in-the-middle attack. [8] The two-factor authentication scheme is still unbroken, but not as secure as we could imagine due to the human factor. We also have to emphasize that this attack method is not something new. We should just go back to 2009 and recall the breach at Ferma: "The theft happened despite Ferma's use of a one-time password, a six-digit code issued by a small electronic device every 30 or 60 seconds. Online thieves have adapted to this additional security by creating special programs—real-time Trojan horses—that can issue transactions to a bank while the account holder is online, turning the one-time password into a weak link in the financial security chain." [9]

As many examples prove, passwords do not mean a sufficient protection. As most information security standards and recommendations contain the need of secure password usage, we need to review the basic rules! As it is widely known, an 8 characters long password, with small and capital letters, numbers and special characters in it is essential. According to the state-of-the-art, this is a little bit outdated. Not so long ago the National Institute of Standards and Technology in the United States has closed the comment period of their NIST SP 800–63–3 on Digital Identity Guidelines and made a huge step towards user-friendly, password-based authentication. Its 800–63B part deals with the questions of Authentication & Lifecycle Management and recommends a new approach of password usage that is well-summarized by Infoworld. [10] According to this document, the new style of password creation rules are the following:

- "Users should be able to choose freely from all printable ASCII characters, as well as spaces, Unicode characters, and emojis;
- increase the minimum length of passwords to eight;
- check passwords against blacklists of unacceptable credentials, including previously breached databases, dictionary words (monkey), common passwords (letmein), and passwords with repeating or sequential characters (pass123);
- lock accounts after several incorrect attempts to login;
- hash passwords with a salt when storing passwords to prevent cybercriminals from acquiring passwords that are stored in plaintext or with weak hash algorithms." [10]

Make a step further! NIST SP 800–63B also recommends the usage of multi-factor authentication, because "password managers only solve the password challenge; they don't address the overall authentication problem when attackers already have the password" as it is stated in the Infoworld article. [10] Password managers are useful tools for storing the memorized secrets, but they are insufficient to address the full user authentication problem, especially in case of privileged users' access management. There are several user-friendly multifactor solutions that utilize the smartphone's capabilities, e.g. its fingerprint scanner and NIST recommends using such solutions, with only one exception. According to Infoworld, "NIST warned against relying on sending one-time passwords via SMS messages as a form of two-factor or multifactor authentication. SMS can easily be intercepted, so NIST suggests using software-based one-time-password generators, such as apps installed on mobile devices." [10]

The SS7 vulnerability in mobile networks[4] reminds us that SMS based authentication is risky, but the suggested software-based solutions are also vulnerable from the human direction as it was described above. Bruce Schneier was right in 2005: "Two-factor authentication solves this problem. It works against passive attacks: eavesdropping and password guessing. It protects against users choosing weak passwords, telling their passwords to their colleagues or writing their passwords on pieces of paper taped to their monitors. […] What two-factor authentication won't do is prevent identity theft and fraud. It'll prevent certain tactics of identity theft and fraud, but criminals simply will switch tactics." [11] Changing tactics is very common. As Schneier continues: "Security is always an arms race, and you could argue that this situation is simply the cost of treading water. The problem with this reasoning [that]is it ignores countermeasures that permanently reduce fraud. By concentrating on authenticating the individual rather than authenticating the transaction, banks are forced to defend against criminal tactics rather than the crime itself." [11]

The Cost of Cyberattack – Analysis of Maersk's Case

It is very rare that we hear exact numbers from companies who were victims of a cyberattack. Although the Ponemon Institute publishes a research report annually on this topic that gives an insight on a global perspective, it is anonymized and does not expose the details of unique cases. That is why the quarterly report of A.P. Moller – Maersk is an extraordinary reading for security professionals. A.P. Moller – Maersk was one of the major high-profile victims of NotPetya malware at the end of June 2017. According to Splash247.com report that time "in the two days since the Maersk Group was hit by the Petya ransomware attack, operations at many of its sites across the globe have returned to manual". [12] As the company's press release states "in the last week of the quarter we were hit by a cyber-attack, which mainly impacted Maersk Line, APM Terminals and Damco. Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect the cyber-attack will impact results negatively by USD 200–300m." [13] That is approx. 1% of the global yearly revenue of the Danish shipping behemoth.

As it turns out from the Ponemon research, US organizations have the highest average cost of cybercrime ($17.36 million), and Australia has the lowest ($4.30 million) as shown on Figure 1. [14] In that case the numbers are 10 times higher. As Maersk is the 558th on Forbes Global 2000[5] list we can be sure that there are many more companies who had, have or will have the same amount or even higher loss due to cybercriminals. Meanwhile, we have not spoken about those thousands of smaller companies who may have a loss around Ponemon's average. Therefore, we can state that cyberattacks are costly and expenses are rising according to the report.

[4] Security researchers identified some critical security holes in the Signaling System 7 (SS7) that could allow rogue attackers to listen in phone calls and access text messages, despite the encryption used by mobile networks.

[5] Forbes Global 2000 list can be found at www.forbes.com/global2000/list.

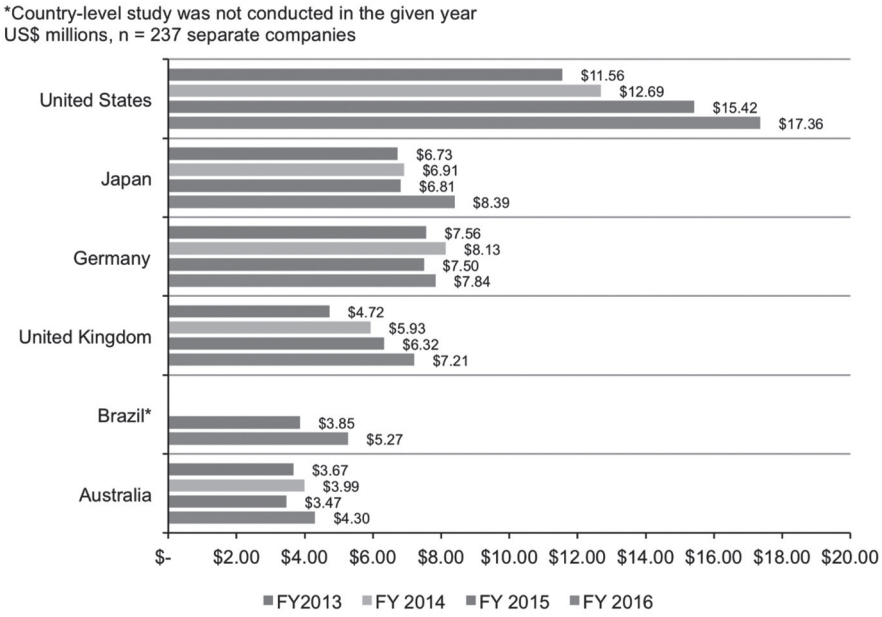

Figure 1. *Total cost of cybercrime in six countries over four years.* [14]

But there are various solutions to reduce this loss. First of all, cybersecurity should be a priority for all companies. There are no verticals or companies whose daily operation does not rely on IT, but there are verticals and companies who do not care about IT security as they are unregulated or simply, they follow the "nothing has happened yet" principle. We have to emphasize that a whole industry can suddenly get into trouble, as it has happened with the shipping industry in the Summer of 2017. Besides the Maersk case, HMS Queen Elizabeth is running outdated Windows XP and theoretically she is exposed for exploits; industry reports say that some crucial nautical infocommunication systems, such as Ecdis and VSat also have vulnerabilities. Moreover, when two modern, highly equipped US Navy ships collide with vessels in 3 months (4 in total last year), cyberattack is one of the first thing that come into the experts' mind.

Amongst others, Ponemon highlights some key factors from the technical perspective of successful companies that are also essential to reduce the cost of cybercrime (excerpt):

- *Detection and recovery.* To reduce the time to determine the root cause of the attack and control the costs associated with a lengthy time to detect and contain the attack, these organizations are increasing their investment in technologies to help facilitate the detection process.
- *Third-party risk.* These organizations are able to reduce the risk of taking on a significant new supplier or partner by conducting thorough audits and assessments of the third party's data protection practices.
- *Insider threat.* A possible negative consequence of reorganization or acquisition of a new company can be disgruntled or negligent employees. These organizations ensure

that processes and technologies are in place to manage end user access to sensitive information. Further, there are training and awareness programs in place to address risks to sensitive data caused by changes in organizational structure and new communication channels.

- *SIEM*. These companies deploy advanced *security information* and *event management* (SIEM) with features such as the ability to monitor and correlate events in real-time to detect critical threats and detect unknown threats through user behavior analytics.

These are just some examples of the challenges that need to be solved. As attackers improve their attack strategies, companies should also improve their defense strategies and the supporting toolset. There are some new technologies that are very promising and hopefully restore the balance between attackers and defenders. According to Gartner's Hype Cycle for Emerging Technologies 2017, Machine Learning or Software-Defined Security are very close to mainstream adoption and we can already see some cyber security solutions that utilize these technologies. [15]

User Behavior Analytics in Cyber Security

Finding a targeted attack nowadays is quite challenging. Cyber security industry tries to react with several new technologies to the above-mentioned challenges. One of the most promising techniques is User Behavior Analytics. Gartner has the following definition for this technology: "User and entity behavior analytics offers profiling and anomaly detection based on a range of analytics approaches, usually using a combination of basic analytics methods (e.g., rules that leverage signatures, pattern matching and simple statistics) and advanced analytics (e.g., supervised and unsupervised machine learning). Vendors use packaged analytics to evaluate the activity of users and other entities (hosts, applications, network traffic and data repositories) to discover potential incidents commonly presented as activity that is anomalous to the standard profiles and behaviors of users and entities. Example of these activities include unusual access to systems and data by trusted insiders or third parties, and breaches by external attackers evading preventative security controls." [16]

We have to emphasize that this countermeasure combines traditional security approach using rules and known patterns with machine learning as an emerging technology. Why is this mixture necessary? As attacking strategies and tools are developing, human beings responsible for cyber defense are less able to define predictable rules from the past events. Although incident management process ends up with a learning phase, when security teams can define a new rule and eliminate the chance of similar attacks for the future, a targeted attack by its nature will be slightly different from all previous attacks. "There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know" said Donald Rumsfeld, former Secretary of Defense of the United States about the types of threats. [17] This became very popular among cyber security experts and data scientists. Most traditional security products deal with known unknowns by looking for things like malware in the system, using already existing patterns and rules. The real problem, however, is the case where the attacks are previously

unknown, commonly referred to as 0-day or 0-hour attacks. We need some way of handling the "unknown unknowns" of cyber security, which are the main challenges for the future.

On the human side the existence of "unknown unknowns" also causes a huge challenge. Security teams should deal with "known unknowns" as a daily routine, but the risk of such attacks is much lower than the risk of "unknown unknowns". Goodall, Lutters, Komlodi highlighted that in such workplaces the major issues are time pressure, monotony of time consuming but not cognitively demanding tasks, and information overload. They defined the usual tasks of security teams as follows (excerpt): [18]

- *"Monitoring:* the first phase of intrusion detection (ID) work involves the ongoing surveillance of systems and network activity looking for indications of anomalous or malicious activity. This process is centered on the intrusion detection system (IDS), but is augmented by other monitoring tools and vulnerability scanners. In addition, analysts monitor an extensive set of resources, including web sites and mailing lists, for news of new attacks and vulnerabilities. These are the mundane daily tasks of ID. One analyst described how "keeping up with everything" constituted the majority of her time.
- *Analysis:* the transition from the monitoring phase to the analysis phase begins with a security trigger event. For network monitoring, this event is usually an IDS alert or recognition of an anomalous event occurring in the environment, such as a sudden spike in traffic or user complaints of slow systems. Analysis of alerts involves not only the alert itself, but many sources of data that provide the contextual information necessary to determine whether or not the alert is an actual intrusion and if so, to assess its severity. For external resource monitoring (e.g., mailing lists), the announcement of a new vulnerability or attack method necessitates further research to determine its applicability and possible severity to one's network environment.
- *Response:* the most common forms of response in ID are intervention, feedback, and reporting. Intervention depends on the role of the analyst in the organization and organizational policies. […] Feedback is usually directed at the IDS or other elements of the security infrastructure. It includes tweaking or removing IDS signatures that generate an excessive amount of false positives, even if the signature was not guaranteed to always generate a false positive."

"Unknown unknowns" can't be identified with such routine easily. With the help of machine learning from the big data set collected by cyber security tools, there is a good chance to automatically identify strange events that deviate from the normal behavior. Gartner describes the feature set of user behavior analytics as follows:

- "Profile, baseline and make visible the activity of users, peer groups and other entities.
- Detect anomalies using a variety of analytics approaches—primarily statistical models, machine learning, rules and signatures, delivered as prepackaged analytics used to create and then compare user and entity activity against their profiles.
- Correlate user and other entity activity and behaviors, and aggregate individual risky behaviors, to highlight anomalous activity.
- Rely on information about users obtained from IT directories (e.g., Active Directory) as a primary data source to feed analytics as well as provide context on users.
- Primarily address security-and-risk-management-oriented use cases, focusing on the activities of "trusted" users inside an organization, whether they are users demon-

strating abusive, noncompliant or illegal activity, or internal users who have had their accounts and hosts compromised by external hackers.
- Perform near-real-time monitoring and alerting." [16]

From the scientific perspective, Eldardiry et al. wrote a remarkable paper on the question of identification of insider attackers using machine learning. [19] In their work they prove that data from multiple sources can be used to efficiently identify anomalies of internal users' activities. They used the following data for analysis that are all related to a targeted attack as well:
- "Logon and logoff events.
- Use of removable device such as USB thumb drives or removable hard disks. Device name and type are logged with each usage event.
- File access events: e.g., file created, copied, moved, written, renamed, or deleted. For each file access the record, file name, path, type, and content are logged.
- Http access events, tagged with URL and domain information, activity codes (upload or download), browser information (Internet Explorer, Firefox, or Chrome), and whether the website is encrypted.
- Email sent and viewed are tagged with from address, to/cc/bcc addresses, subject line, sent date, text, attachment info, and whether the email is encrypted." [19]

Therefore, it is not surprising that user behavior analytics is getting a widespread technology in cyber security. There are two common product types that are unimaginable without this solution. Security Incident and Event Management or SIEM systems are widely adopted UBA as they are the center of the organizational security data collection, in that sense they have everything that is needed for machine learning. Identity and Access Management systems also started to implement UBA as they also have a huge amount of data on user activities that give a good basis for behavior analytics. As Figure 2 shows, the general interest on user behavior analytics has been increased in the last couple of years and our intention is that this curve raise in the forthcoming years as well.

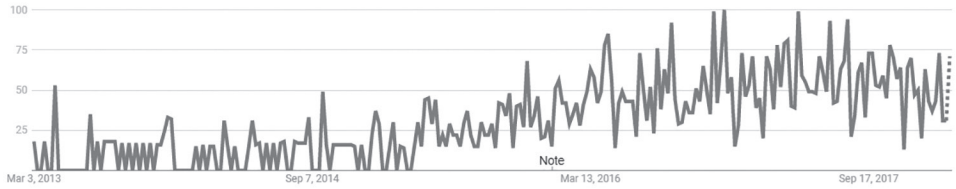

Figure 2. *Report on "User Behavior Analytics" search expression.*
[Google Trends]

Conclusion

In Hungary, the Good State and Governance Report 2017 gives an overview on cyberattacks reported for CERT-Hungary which is responsible for managing the IT security related incidents in the governmental sector. Based on this report only 0.3% of the reported incidents were classified as a targeted attack. [20] In order to identify an APT, several specific countermeasures are needed in addition to the high quality cybersecurity culture in an organization. As an example, well-prepared organizations used to have the following technical solutions:

- central security incident and event management (SIEM);
- network flow analysis;
- threat intelligence;
- malware detection with sandbox technology;
- behavior based endpoint protection;
- anti-phishing solutions;
- continuous cybersecurity awareness training;
- vulnerability analysis with social engineering tests.

This low percentage is a good indicator of how difficult to discover an APT and how far the Hungarian public administration is from the adoption of latest cyber security solutions. The above-mentioned solutions are very expensive and require a mature cybersecurity culture to be able to adopt successfully. The Hungarian public administration lacks funding and cybersecurity is not the major pain point for them, therefore we cannot expect a rapid change in APT detection. Based on the literature review and case studies we investigated in this paper, we are arguing for the wider usage of machine learning based security solutions, as they are usually accessible for the already existing solutions, like endpoint protection or SIEM systems. This situation can ameliorate with more centralization in governmental IT security, e.g. by starting a governmental managed cybersecurity service for the whole Hungarian public sector.

Meanwhile, we want to emphasize the potential challenges as well, that needs further analyses. Among these open questions, data privacy is the prime concern. As user behavior analytics needs to process user activities, such information needs to be collected. Due to regulations of the European General Data Protection Regulation, this practice might be questionable. However, we want to emphasize, that according to Section 49 of GDPR: "The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by *c*omputer *e*mergency *r*esponse *t*eams (CERTs), *c*omputer *s*ecurity *i*ncident *r*esponse *t*eams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned." [21] Moreover, UBA can also be spoofed on many ways in theory, so that area should also be monitored. In our future researches we will keep in mind these aspects.

References

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: ISO/IEC *27000:2018, Information technology—Security techniques—Information security management systems—Overview and vocabulary*. ISO/IEC, 2018.

[2] INTERNATIONAL TELECOMMUNICATIONS UNION: *Definition of cybersecurity 2008.* www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (Downloaded: 17.01.2018)

[3] KISSEL, R.: *Glossary of Key Information Security Terms.* Washington D.C.: U.S. Department of Commerce, 2013.

[4] HUTCHINS, E. M., CLOPPERT, M. J., AMIN, R. M.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In. RYAN, J. (ed.): *Leading Issues in Information Warfare & Security Research.* Reading: Academic Publishing International, 2011. 80–107.

[5] FURNELL, S., EMM, D.: The ABC of ransomware protection. *Computer Fraud & Security*, 10 (2017), 5–11.

[6] MITRE CORP.: *Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™).* 29 January 2018. https://attack.mitre.org/wiki/Main_Page. (Downloaded: 30.01.2018)

[7] DAVIS, A.: *Monitoring Windows Console Activity (Part 1).* 1 September 2017. www.fireeye.com/blog/threat-research/2017/08/monitoring-windows-console-activity-part-one.html. (Downloaded: 16.01.2018) DOI: https://doi.org/10.1016/S1361-3723(17)30089-1

[8] MORSE, J.: *The leaked NSA report shows 2-factor authentication has a critical weakness: You.* 7 June 2017. https://mashable.com/2017/06/06/russia-hackers-nsa-2fa-leaks-election-2016/ (Downloaded: 16.01.2018)

[9] LEMOS, R.: *Real-Time Hackers Foil Two-Factor Security.* 18 September 2009. www.technologyreview.com/s/415371/real-time-hackers-foil-two-factor-security/ (Downloaded: 16.01.2018)

[10] RASHID, F. Y.: *NIST to security admins: You've made passwords too hard.* 5 May 2017. www.infoworld.com/article/3194705/security/nist-to-security-admins-youve-made-passwords-too-hard.html (Downloaded: 16.01.2018)

[11] SCHNEIER, B.: *Crypto-Gram.* 15 April 2005. www.schneier.com/crypto-gram/archives/2005/0415.html (Downloaded: 16.01.2018)

[12] CHAMBERS, S.: *Back to the future for Maersk in the wake of Petya attack.* 29 June 2017. http://splash247.com/back-future-maersk-wake-petya-attack/ (Downloaded: 16.01.2018)

[13] maersk.com: *A.P. Moller-Maersk improves underlying profit and grows revenue in first half of the year.* 16 August 2017. www.maersk.com/press/press-release-archive/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year (Downloaded: 16.01.2018)

[14] PONEMON INSTITUTE: *2016 Cost of Cyber Crime Study & the Risk of Business Innovation.* Traverse City: Ponemon Institute, 2016.

[15] PANETTA, K.: *Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017.* 15 August 2017. www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/ (Downloaded: 16.01.2018)

[16] BUSSA, T., LITAN, A., PHILLIPS, T.: *Market Guide for User and Entity Behavior Analytics.* Stamford: Gartner Inc., 2016.

[17] WIKIPEDIA: *There are known knowns.* 28 January 2018. https://en.wikipedia.org/wiki/There_are_known_knowns (Downloaded: 30.01.2018)

[18] GOODALL, J. R., LUTTERS, W. G., KOMLODI, A.: The Work of Intrusion Detection: Rethinking the Role of Security Analysts. In. *10th Americas Conference on Information Systems.* New York: AMCIS, 2004.

[19] ELDARDIRY, H., SRICHARAN, K., LIU, J., HANLEY, J., PRICE, B., BRDICZKA, O., BART, E.: Multi-source fusion for anomaly detection: using across-domain and across-time peer-group consistency checks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* 5 2 (2014), 39–58.

[20] KAISER T. (szerk.): *Jó Állam Jelentés 2017.* Budapest: Dialóg Campus Kiadó, 2017.

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).