VOL 1 (2017) ISSUE 3

EUROPEAN CYBERSECURITY MARKET

RESEARCH, INNOVATION, INVESTMENT

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY MARKET

RESEARCH, INNOVATION, INVESTMENT

European Cybersecurity Market is a new publication designed to promote innovative solutions and tools in the field of cybersecurity. In order to raise awareness and increase cooperation in the developing digital economy, this periodical will be openly distributed to all interested parties and stakeholders.

ISSN: 2543-7259

European Cybersecurity Market is a quarterly publication.

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków, Poland

Phone: 00 48 12 632 97 24
E-mail: robert.siudak@ik.org.pl

www.ik.org.pl
www.cybersechub.eu

CO-FINANCED BY

European Funds
Regional Programme

KRAKÓW REGION
MAŁOPOLSKA

European Union
European Regional
Development Fund

FOREWORD

ROBERT SIUDAK
Chief Editor of European Cybersecurity Market
CYBERSEC HUB Project Manager
Research Fellow of the Kosciuszko Institute, Poland

We are gradually becoming more aware of the vulnerability of our networks and systems, as well as their expanding role in our daily lives. Many reports suggest that 2016 brought us a breakthrough in the popular perception of cybersecurity. It is no longer a distant and secondary problem important only to IT departments. It has become a vital part of our businesses, our financial activities and our personal lives. We now realise that cybersecurity will be one of the fundamental challenges of the coming decades. But this challenge might be also a huge opportunity for those who know how to use it.

The private sector is the main source of ICT solutions in the modern market. The prime cause is to be found in the structure of modern economy. The business sector is harvesting the accumulated fundamental and applied research by changing it into the experimental development of new products or services. Market needs and rules are the catalysts of innovation in the digital economy. How does all of this influence the security of cyberspace?

According to research from Symantec, roughly one million new malwares are released every day. Hackmageddon, which monitors larger network attacks, counted 1061 in the last year, which means more than three large-scale malicious cyber operations a day. Due to the rapidly changing threat environment, the cybersecurity sector is one of the fastest evolving realms of ICT. That is why nowhere else is the innovation so crucial. To keep up with their adversaries, cybersecurity companies have to be innovative by design.

This edition of the ECM presents business opportunities arising from the introduction of machine learning, automation, and other Artificial Intelligence technologies into the cybersecurity domain. It also analyses one of the most demanding environments to secure – the cloud. Last but not least, it also includes coverage of the Startup Pitch Contest, which took place during the Polish Cybersecurity Forum – CYBERSEC PL 2017.

I wish you an inspiring reading.

Robert Siudak

CONTENTS

We live in a new reality, when digital security has become more challenging than the physical one—not only to nuclear facilities or large enterprises, but also to regular companies and users. The amount of electronic services is overwhelming, as is the amount of sensitive data stored on every personal device. Information is the new gold and as such needs special care. Disk encryption, strong passwords, access policies, antivirus, firewall, and a lot of common sense are the absolute basics that have served us well so far. Unfortunately, they are no longer enough. Security has changed drastically, and cyberc riminals are setting the new rules. With easy access to the Darknet, where everyone can make transactions relatively anonymously, the malware market itself has turned into a considerable business and keeps growing. One can buy anything there, from basic how-to's to advanced malware or zero-day exploits, which can be used to create either new variants or completely new threats. We are going to see a wave of targeted attacks, which will no longer be limited to the big guys. Depending on the attacker's motivation, skill, and budget, these new threats may easily render the current protection mechanisms useless. We have to understand the risks, and learn how to recognise and address these new cyber issues.

Cybercrime-as-a-Service

2016 was the year of ransomware and targeted attacks, and 2017 has so far continued this trend. Cybercriminals keep releasing new versions of their software, not only to evade existing protections but also to improve the overall "usability". A great example here is Cerber, one of the most successful ransomware variants. The first version of Cerber appeared in March 2016, and as of April 2017 we have already seen multiple iterations, which fixed various bugs in the code, eliminated the ability of file decryption with third-party tools, improved the encryption performance, but most importantly offered a Ransomware-as-a-Service (RaaS) platform. It provides newbie cybercriminals with a quick way to generate their own customised copies of Cerber, which are well-suited to target their specific victims. In case they are successful and the ransom is paid, the Cerber authors keep 40% of the profits and the rest gets transferred to the RaaS user's bitcoin address. The platform was a big success and resulted in hundreds of ransomware e-mail campaigns being run all around the world. New players on this specific market are appearing all the time. The RaaS named Satan and released in January 2017 tries to attract new users with lower charges (30% fee), more translations (20 languages), and an ability to create fully customised droppers.

TOMASZ KOJM
is a computer security veteran with over 20 years of experience. Co-founder and Head of Technology at Armaio. Tomasz worked with the biggest security companies and is best known for creating ClamAV, the most popular open source anti-virus technology and the de facto standard for e-mail scanning. For over decade Tomasz was developing one of the leading solutions the entire cybersecurity depends on. Currently, ClamAV protects more than 2 billion users worldwide and was acquired by Cisco. Implemented in hundreds of security solutions and used by the largest enterprises, including: Google (GMail, Drive), Apple (macOS), Facebook, and more. Tomasz co-authored books, articles and lectured as invited and keynote speaker on major conferences all over the world. Named Security Thought Leader by the prestigious SANS Institute.

Fig 1. How to make money with Satan? The rules are simple.

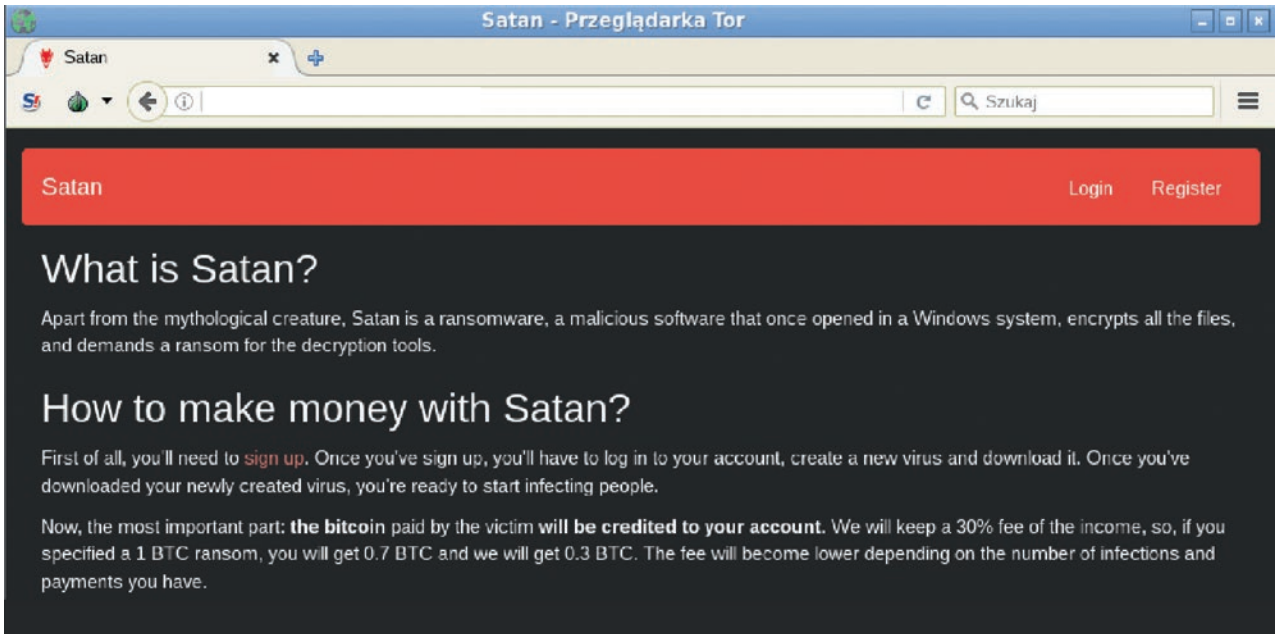
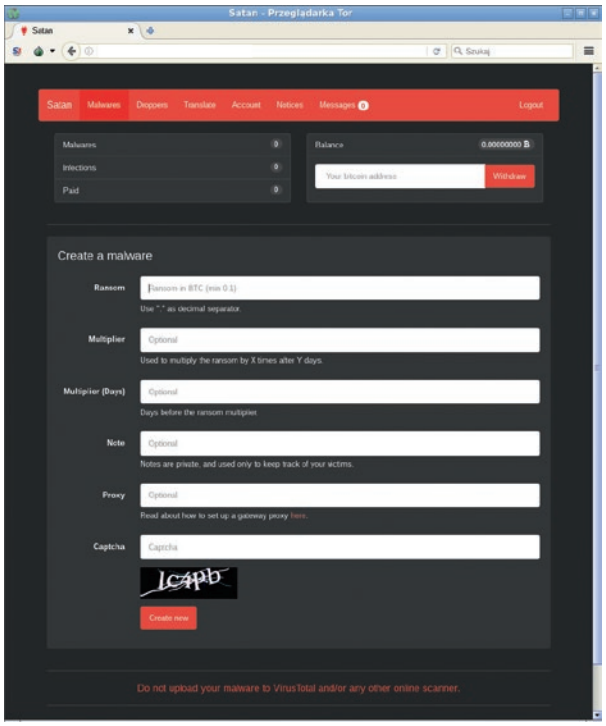
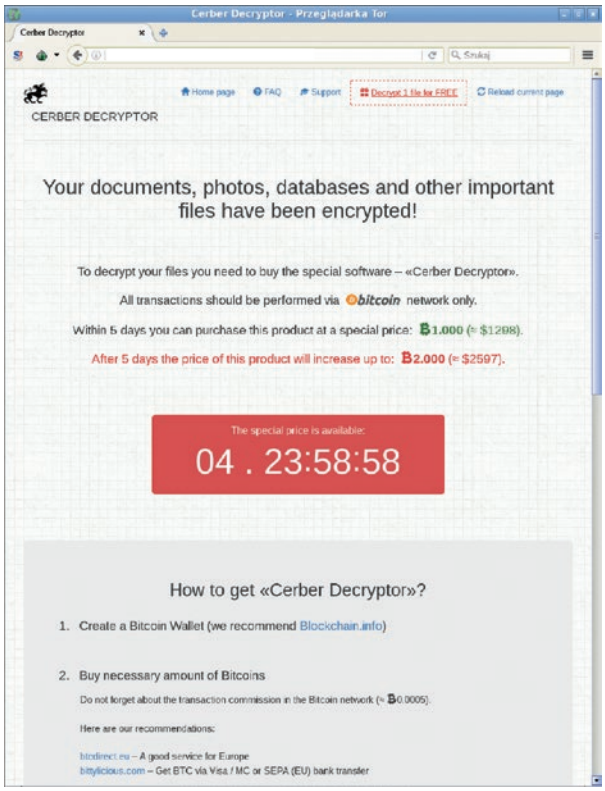


Fig. 2. Build your own malware with a few clicks.



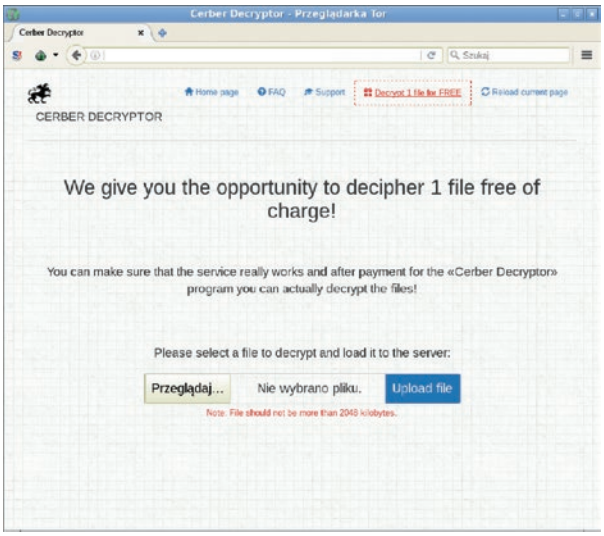
Ironically, not only the malware itself, but also the victim's experience gets constantly improved. The modern ransomware packages provide good-looking interfaces, translated into multiple languages, with FAQs and detailed instructions on how to obtain Bitcoins and pay the ransom. Those who are willing to pay early get a special price; last Christmas one ransomware even offered a holiday discount!

Fig. 3. The special price of Cerber Decryptor.



In some cases, such as Cerber, a victim is offered to decrypt a single file online. This is a smart move on the part of cybercriminals, as they not only make themselves credible in the eyes of the victim, but also collect potentially highly important and sensitive data.

Fig. 4. The single file decryption opportunity.



Cybercrime-as-a-Service in general is not a novel approach, and has been available on the Darknet for a few years now, offering access to malware samples, spam campaigns, illegal pen-testing, and other services. However, with its ease of use and zero entry cost RaaS takes it to the next level and each new variant will certainly attract thousands of potential attackers in the coming months, who might later target victims in their local neighbourhoods.

Advanced Persistent Threats Become Widely Available

The term Advanced Persistent Threat (APT) has been in use for many years to describe complex, multi-vector long-term threats, aimed at infiltrating or severely damaging their targets. For a long time, it was mostly associated with cyberwar and nation-state level attacks, and was highly popularised in 2010 after the discovery of Stuxnet, which successfully targeted uranium enrichment infrastructure in Iran. The worm was able to infect removable storage devices, such as pendrives, and it is believed to have been planted at an Iranian nuclear facility by one of the workers. The uniqueness of Stuxnet lies in its use of four zero-day exploits (previously unknown to the public) for privilege escalation and ability to infect Programmable Logic Controllers to alter how the device motors controlled by them are operated. Moreover, the rootkit drivers used by Stuxnet were digitally signed with stolen certificates of two renowned Taiwanese corporations: Realtek and Jmicron. Obviously, preparing such a sophisticated attack required many resources and likely had a budget in the range of multiple million dollars. Since that time, much more APTs have been spotted in the wild, and mostly used for digital espionage. Thanks to the relatively high privacy level offered by the Tor network and Bitcoin transactions, over the last years the advanced threats became available to a wider audience. Additionally, the Tor-enabled malware, which does not communicate via standard channels, makes it even harder to identify the attacker.

The secret CIA documents published by Wikileaks[1] in March 2017 and code-named “Vault 7” shocked the public by revealing how the agency is able to bypass antivirus engines, exploit remote devices, or spy on people using Smart TVs. Many media called the revelations bigger than Snowden’s, however the truth is that most of these techniques have already been known and used not only by CIA but also by cybercriminals. Perhaps the most interesting bits of the leak were those related to CIA’s efforts to infect Macs, as some tools were designed to perform firmware-level infections and provide persistent access to affected machines, even if their operating system was reinstalled from scratch. We are going to see more threats of this kind, especially since the newest laptops no longer provide a “dumb” charging port and require the user to use the USB-C one. Using an untrusted charger might soon have effects similar to inserting a suspicious USB key.

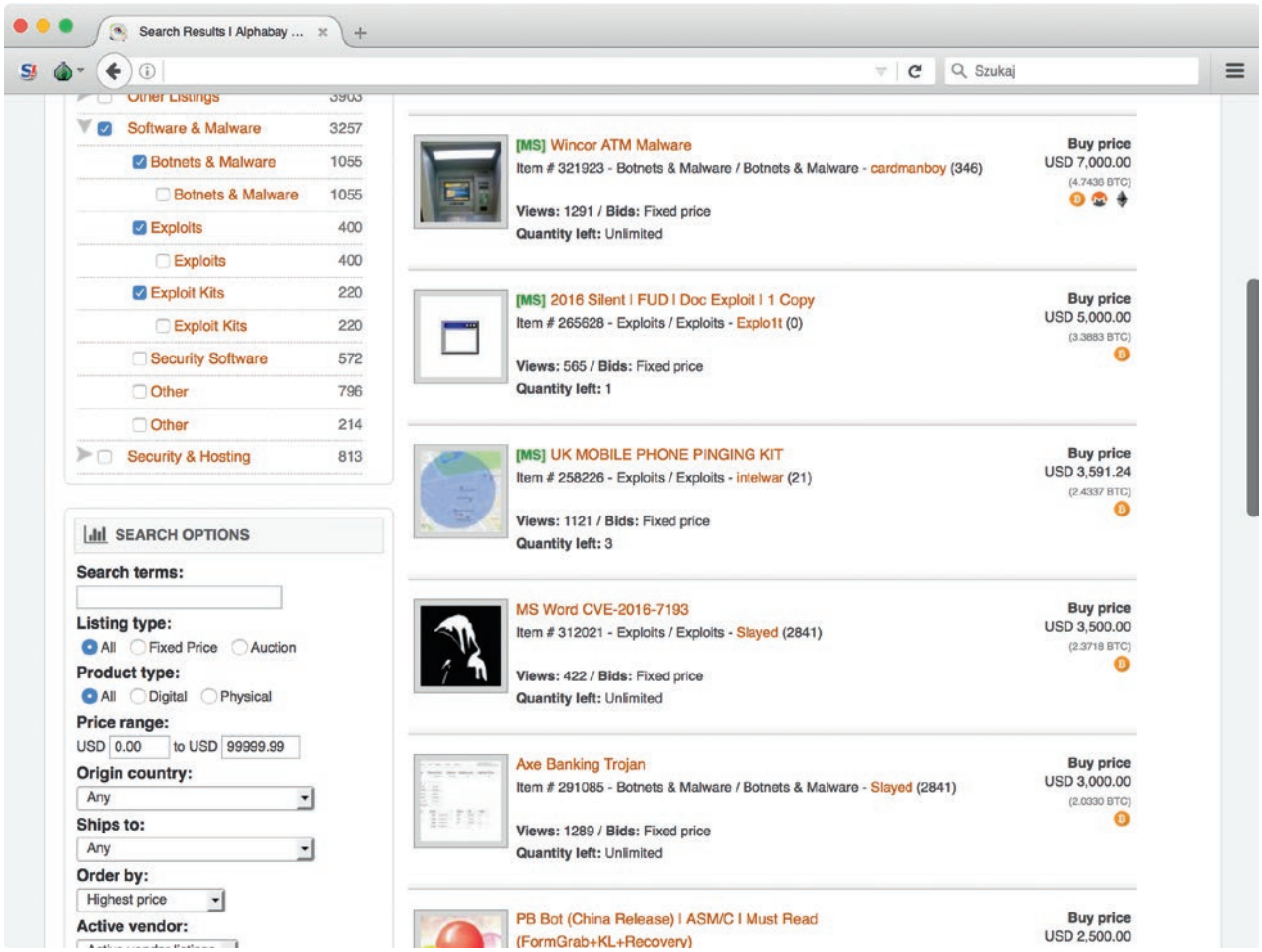
More Targeted Attacks on Individuals

Imagine an ongoing APT attack against a high-profile person, during which the attacker has a long-term stealth access to the victim’s computer. Over time,

1 | Wikileaks, Vault 7: CIA Hacking Tools Revealed, https://wikileaks.org/ciav7p1/, March 2017.

the attacker fills the computer with illegal content, such as child pornography, initiates remote connections to suspicious websites, and performs other actions at specific times of day or week to make them look credible. If the attack is not detected and stopped in time, the attacker might clean up and cover the infection tracks. As one can imagine, the results of the intrusion could be devastating, with the victim risking not only disqualification from public office, but also a prison sentence. The major problem is that today's small-scale targeted attacks are unlikely to get spotted. One of the reasons is the lack of next-generation threat detection software available on the consumer market. The solutions which stand a chance to detect APTs are usually both very expensive and only available to large enterprises. The malware market is growing rapidly, and with the wide availability of "professional services" on the Darknet the attacks on individuals and scenarios like the one above will become, or have already become, a reality. Unfortunately, the black market is developing much faster than computer users' awareness, meaning the cyber criminals will be not one step, but a mile ahead.

Fig. 5. A typical Darknet market offering exploits and malware.

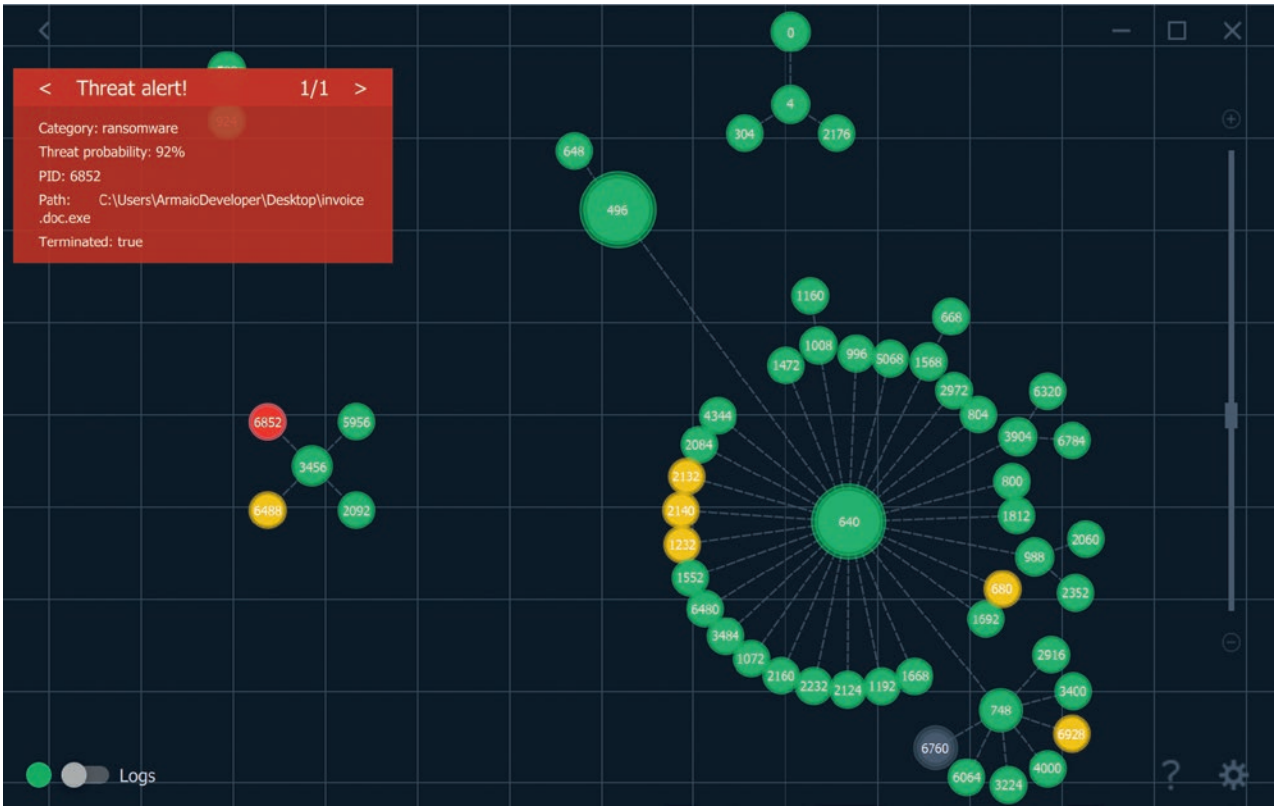


You Can't Fully Prevent an Attack, But You Can Prepare For It

If the attackers are determined enough, they will sooner or later find a way to enter your computer or company network. The number of possible infection vectors is virtually unlimited, and the Darknet is full of ideas and instructions for exploiting software, hardware, and human factors. While you cannot fully prevent the intrusion, you can and should be prepared to response to a cyber incident. Early detection, proper response policies in place, and the ability to quickly estimate the damage and recover the affected services will play an invaluable role in getting your operations back to normal. If your company does not have a plan on how to act after a cyber incident, it risks further chaos and damage to its business. If you are personally targeted, and cannot prove your innocence, you risk a conviction and a lot of life-altering problems.

At Armaio, we are working on a new technology, which comes into play when the first layers of defence—such as firewall, antivirus, or simply common sense—fail to stop a threat from entering and executing in the system. Our mission is to minimise the time window in which the system is exposed to the attacker. Armaio Core uses artificial intelligence and advanced algorithms to detect unknown threats as soon as possible, so their impact on the system and data is limited.

Fig. 6. Armaio Core detecting and classifying unknown threat as ransomware.



After it detects a threat, it provides a detailed summary of all the actions the threat performed over its lifetime. This information is extremely important in estimating the damage and loss of data, and understanding how and when the malware entered the system. Most importantly, Armaio Core is the only technology on the next-generation security market to be available as open source, free for home users, and providing the highest level of transparency. ■

ARMAIO

NETHONE Wins Startup Pitch Contest at CYBERSEC PL

Hubert Rachwalski (Nethone)

The Startup Session powered by the CYBERSEC HUB was one of the side events of the 2nd Polish Cybersecurity Forum CYBERSEC PL organised by the Kosciuszko Institute in Warsaw on 6 April 2017.

Michał Malanowicz (Wheel Systems), Tomasz Huś (PZU), Bartłomiej Rozkrut (2040) and other participants.

Robert Siudak (The Kosciuszko Institute)

CYBERSEC PL
POLSKIE FORUM CYBERBEZPIECZEŃSTWA

The aim of the event was to present innovative cybersecurity solutions developed by the Polish startups and facilitate their access to investors and large state-owned companies, including the defence or critical infrastructure sectors. Each of the 7 selected startups got three minutes to pitch their ideas to the panel consisting of Karel Obluk (Evolution Equity Partners), Adam Kapitan Bergmann (Mjølnir Ventures) and the representatives of PGZ, PZU and Exatel. In order to make the presentations more attractive, the pitch session was also a contest; the investors not only provided feedback to the companies, but also chose the winner who will get the opportunity to present their ideas to a wider international audience on the main stage of the 3rd European Cybersecurity Forum CYBERSEC, 9-10 October 2017 in Kraków. The investors' verdict was preceded by a heated discussion. Nonetheless, the jury unanimously picked Nethone. This Warsaw-based startup facilitates advanced data science, providing a truly individual approach to each client's unique challenges, goals, and vision. Nethone creates custom AI-driven solutions that convert threats into profitable decisions. It helps online merchants sell more, earn more, and maximise each dollar they spend on business intelligence and fraud prevention. Thanks to Nethone's unique blend of AI and human ingenuity, it protects clients' bottom lines against fraud and streamlines their risk management processes. Nethone provides unique, data-driven business insights that clients can leverage to get ahead of the game in the competitive world of online commerce. The company employs diverse state-of-the art technologies, including in-depth User Profiling (3000+ data points), Behaviour Analytics, Device Fingerprinting, and more. It gathers, enriches, extends, and crunches all of this data to provide clients with actionable information.

Nethone

PITCH COMPETITORS

Other startups that took part in the Session during CYBERSEC PL were:

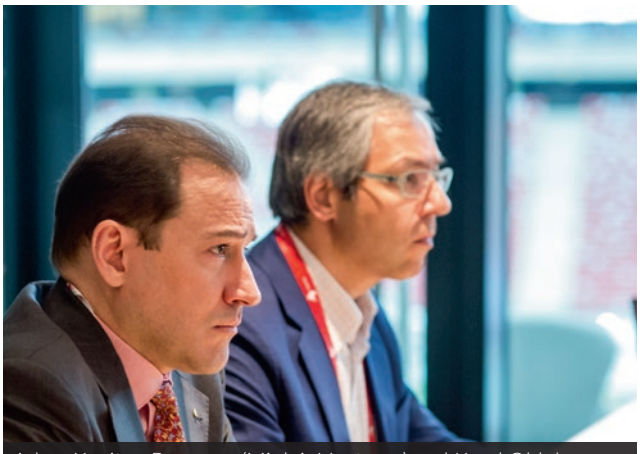
· Sher.ly: a SaaS data smart syncing & collaboration service for business. It delivers a new way of sharing your sensitive files with your co-workers and business partners by creating a secure, invite-only network on demand. It works similarly to a cloud, but all the data stays on your own storage. Sher.ly is a startup launched in 2013, dedicated to creating innovative software for file-sharing among business organisations, on both desktop and mobile devices. The main development centre is based in Kraków, Poland. The company gained traction in June 2014, mainly thanks to a crowdfunding campaign on Kickstarter. The financial target was met in 223% and Sherlybox became a huge success even before hitting the market in August 2015. Sher.ly is a recipient of prestigious awards, e.g. "ICT Visionary", one of the "50 most creative in Poland", "Good Design 2015", "Must Have 2016". Sher.ly offers the Sher.ly application, for secure and fast data sharing, as well as the Sherlybox device – the embodiment of a private and secure storage cloud for your files, available 24/7.

· Autenti: the first Polish platform for approving documents and signing contracts online. It offers a secure solution which guarantees that no one can get access to users' documents, which are encrypted using a 256-bit key and archived securely on any medium the client chooses. This is an advantage over regular and electronic mail. Users can also store contracts and documents on Autenti in several places at the same time. The Autenti platform uses an SSL certificate to encrypt data sent electronically between the server and the user, which makes it impossible to intercept confidential information. For mobile devices, clients are also encouraged to use an additional PIN code. It is worth mentioning that Autenti meets top-of-the-line standards for storing documents in accordance with the European personal data protection law. The server room hosting their infrastructure is one of the most secure and modern in Poland.

· Cyberus Labs: a new kind of Polish company that is global in its DNA. Co-founded by Silicon Valley and Polish entrepreneurs, Cyberus Labs has taken a different approach to finding a solution to the user authentication challenge and dilemma: the right balance between the user's need to have a fast and convenient way to log into their online account and the need of the company to have a secure and effective user authentication system. At its core lies the elimination of the username/password combination as a user authentication methodology. The result of 3 years of research and development in Silicon Valley, CA and in Poland is the CYBERUS KEY password less log-on platform, launched in September 2016 at CYBERSEC 2016 in Kraków, Poland. With the CYBERUS KEY, users access their online accounts by activating the Cyberus Key mobile application on their smartphones and with one-click log into their banking or e-commerce accounts on their laptops. CYBERUS KEY creates a truly secure log-on experience and verifies both sides of an online transaction, eliminating the risk of phishing, key-logging, "man-in-the-middle" or "man-in-the-app".

· Wheel Systems: The company focuses on privileged access management, user authentication and authorisation, and SSL/TLS traffic inspection. Wheel Systems' products combine innovation and an intuitive user experience with strong security features. These are the hallmarks of the future designs of the company. Wheel Systems remains a leader of user authentication in Poland, as well as one of the few producers of privileged access management solutions globally. Wheel Systems' customers are financial institutions, energy companies, and the public sector. Their distribution channels cover a network of 80 partners across 30 countries. In 2016 Wheel Systems set up a new office in Silicon Valley and began their expansion into the US market. In 2012 they launched Wheel Fudo PSM, the very first session manager in the world to enable real-time supervision, voted the best solution for the financial sector in 2015. In 2016 they created the most advanced privileged access management solution – Wheel Fudo PAM. Currently, the company is launching the fastest SSL/TLS traffic inspector – Wheel Lynx SSL Inspector Infinity.

Oliwia Drożdzik and Błażej Marciniak (Sher.ly)



Adam Kapitan Bergman (Mjølnir Ventures) and Karel Obluk (Evolution Equity Partners)

· 2040: using technology based on deep learning algorithms, 2040 has created a new category of software that helps dealing with most of daily business activities. Their solution gives the entrepreneurs an IT tool to better organise their worktime, as well as providing dedicated advice and suggestions to help. It watches company's e-mails, contacts and meetings, making suggestions about upcoming possibilities. By connecting various data sources and learning from them, the tool is able to provide the best advice possible. And the more it is used, the better it will work in the future.

· IDENTT: offers preparation and development of dedicated technology in the field of computer security. Their i.a.idenTT Verification System is a tool supporting the verification process of a client's ID documents. The system verifies correctness, integrity, and authenticity of the document. The implementation of this tool will increase the rate of detection of using a false identity. Advanced data analysis provides high credibility of the verification result. Another product is the SecPass, which basic task is storage of sensitive data such as passwords, cryptographic keys, or access data. Data can be stored in folders with hierarchical structure, shared with co-workers and quickly found. The big advantage of this system is the security of data, which is encrypted while being stored. IDENTT offers also SAT – safe authoristation tool, and the Estamp system for verifying authenticity and integrity of printed documents. While many official documents still have to be printed and sent in traditional form, applying a special code on the document allows the recipient to verify it. Using their smartphone or scanner they can then check who the author is or if the content has not been changed.

Find out more about the European Cybersecurity Forum CYBERSEC and the Polish edition CYBERSEC PL: www. cybersecforum.eu. ■

Ziemowit Jóźwik (The Kosciuszko Institute), Michał Malanowicz (Wheel Systems), Tomasz Huś (PZU), Bartłomiej Rozkrut (2040), Jan Szajda (IDENTT)

CYBERSEC
EUROPEAN
CYBERSECURITY FORUM

Krakow

9-10.
10.
2017

3rd European Cybersecurity Forum

Dealing with cyber disruption

#CSEU17 | www.cybersecforum.eu

CYBERSEC 2016
IN NUMBERS

1
Emerging Public Policy Challenge

2
Days of Thought Provoking Debates

4
Thematic Streams

>400
Articles about CYBERSEC

40
Accredited Journalists

35
Interviews for CYBERSEC TV

79K
Twitter Impressions

20
Hours of Networking Opportunities

>120
Speakers

10%
Academy & NGO

30%
Public Administration

50%
Private Sector

10%
Military & Police

LEARN MORE ABOUT @CYBERSECEU:

DO VIRTUAL ASSISTANTS DREAM OF ELECTRIC SHEEP?

Bartosz Ziółko

CYBERSECURITY IN THE CONTEXT OF AUTOMATIC CUSTOMER SERVICE

Nowadays, customer service is one of the fastest developing business branches. According to a report prepared for the AGH University of Science and Technology, the estimated yearly cost of running call centres just in Poland is around USD 350 million.

Rapid growth also leads to large competition. The companies compete in terms of prices, range of services, operational capabilities, and customer satisfaction level. This last field comprises availability, reaction time, consultant expertise, and quality of conversation in the sense of social norms. While business focuses on those factors, the security aspects are usually of secondary importance. This is why it is vital to get a closer look on this topic, both in the context of possible threats and optimal solutions. One of such solutions is the automation of conversations by applying ASR technology (Automatic Speech Recognition).

▶ **Empathetic robots: interview with Jolanta Karny, Vice-President of the Board at Aviva General Insurance Company**

B.Z. Is automated customer service a necessity or still a thing of the future?

J.K. *It is definitely a thing of the present. Companies that have not yet implemented process automation will lag behind the competition. Robots are taking over simple, repeatable tasks, allowing us to focus on delivering value to our clients. Of course, there are several exceptions, as not every business or process can be automated. The thing of the future, although we are witnessing the beginning of this future right now, is the use of artificial intelligence. In this area, possible benefits are even more far-reaching. Artificial intelligence does not only repeat our actions, but is also capable of making independent decisions.*

B.Z. How important is the factor of human error when it comes to security?

J.K. *It is crucial in every aspect. Current security systems are very advanced but there are two main reasons for security breaches: employee error or fault in system design. Unfortunately, it is usually the former. There is still too little awareness of how important it is to choose a strong password and guard it carefully in terms of secure access to a system.*

B.Z. How do customers respond to automatic consultants?

J.K. *Some customers appreciate human service. Others, especially the younger generation, are fascinated by new technologies and social media, they like to experiment. They also put a higher value on their time. A well-designed team of automatic consultants can quickly and efficiently help them deal with any issue they might be facing. Our role is to adjust the method and form of communication to the customer's expectations. Introducing automatic consultants does not necessarily imply eliminating traditional ways of service, if this is what the customer prefers.*

B.Z. What poses the biggest challenge in terms of customer service automation?

J.K. *Insurance business relies to a large extent on empathy. It might be some time before robots are able to express it, or rather imitate it. We need to be careful not to lose track of the human factor with the current automation craze. It is thus crucial not to let automation take away from the customers what they appreciate about the service provided for them, for example personal advisory when acquiring more complex or long-term financial services, such as mortgage loans or life insurance. Human assistance and empathy are also priceless and irreplaceable at the time of reporting a damage, a difficult situation which is usually stressful for the customer.* ◀

Scalability? No problem

One of the common risks for an organisation in the matters of cybersecurity is scalability and expansion. Rising employment leads to an increase in operational costs, but it is not only a question of money. Every hired person increases the risk of incidents, safety-related breaches or "simple" data theft. With a digital employee created by computer software, these problems disappear almost completely. Automatic customer service systems are also easily adaptable to traffic changes. It has crucial meaning especially in emergency or response centres in case of failure or mass threat. A typical example of such use is the energy sector.

Human factor

A machine never tires. This simple fact can have an important impact when it comes to human workers. This concerns especially call centres. Growing expectations (as mentioned above, this business is more and more competitive), stress or simply tiredness can lead to serious mistakes: omission of important procedures, errors in introducing data or breaking regulations in order to meet the parametrised work goals, not to mention intended wrongdoing as a result of frustration or anger. An automatic system, by definition, does not allow activities that break any laws, behaving always according to the scheduled scenario. People do not necessary behave at work as they did during their job interview, while ASR always "speaks" in the same way as during the tests. The quality of service is constant and does not change over time; what is more, the competitiveness of service increases thanks to the availability and standardisation of certain procedures.

Implementing a computer system: obvious benefits

With an automatic system, the rate of user experience is much more predictable. Automatic speech recognition systems allow an easier and safer integration with voice biometrics, which is more user-friendly when compared to PINs and much safer than authentication by personal questions. A combination of ASR and voice biometrics is natural for users. It also enables work not only

on specific phrases but as a hidden extra security means in the background during the entire phone conversation. Last but not least, automation, due to its scalability, is much more resilient to a new kind of threat – phone DDoS attacks. A well-tailored automatic response centre is prepared for the potential overload. It is one of the greatest advantages of this solution.

Lack of trust for new solutions in security

New IT systems often cause low confidence regarding user safety. It is a common challenge when changing processes from traditional to new ones, safer than the old ones; however, as most systems, they too are not perfectly safe and often perceived by end users as less safe than those they are used to. People focus on possible security gaps in new solutions while ignoring those in well-known systems, even though they are also more familiar to hackers. It seems hard to believe that in the 21st century, when biometrics-based systems are available in various different modes, several companies still use questions about our mother's maiden surname as a means of authentication.

Telephone: secure access channel

Another security aspect, which should not be ignored in the case of call centres operating on IVRs with ASR, is the safety of the channel. Telephone communication is much safer from the IT point of view, especially in comparison to mobile apps. The ASR server always operates on remote hardware, often located physically in a safe environment, and all fragile data are stored there. Only audio on dialogue grammars is sent over the network to the client. Most of the recent successful attempts at breaking communication channels were focused on smartphone applications.

How does Techmo solutions respond to these issues?

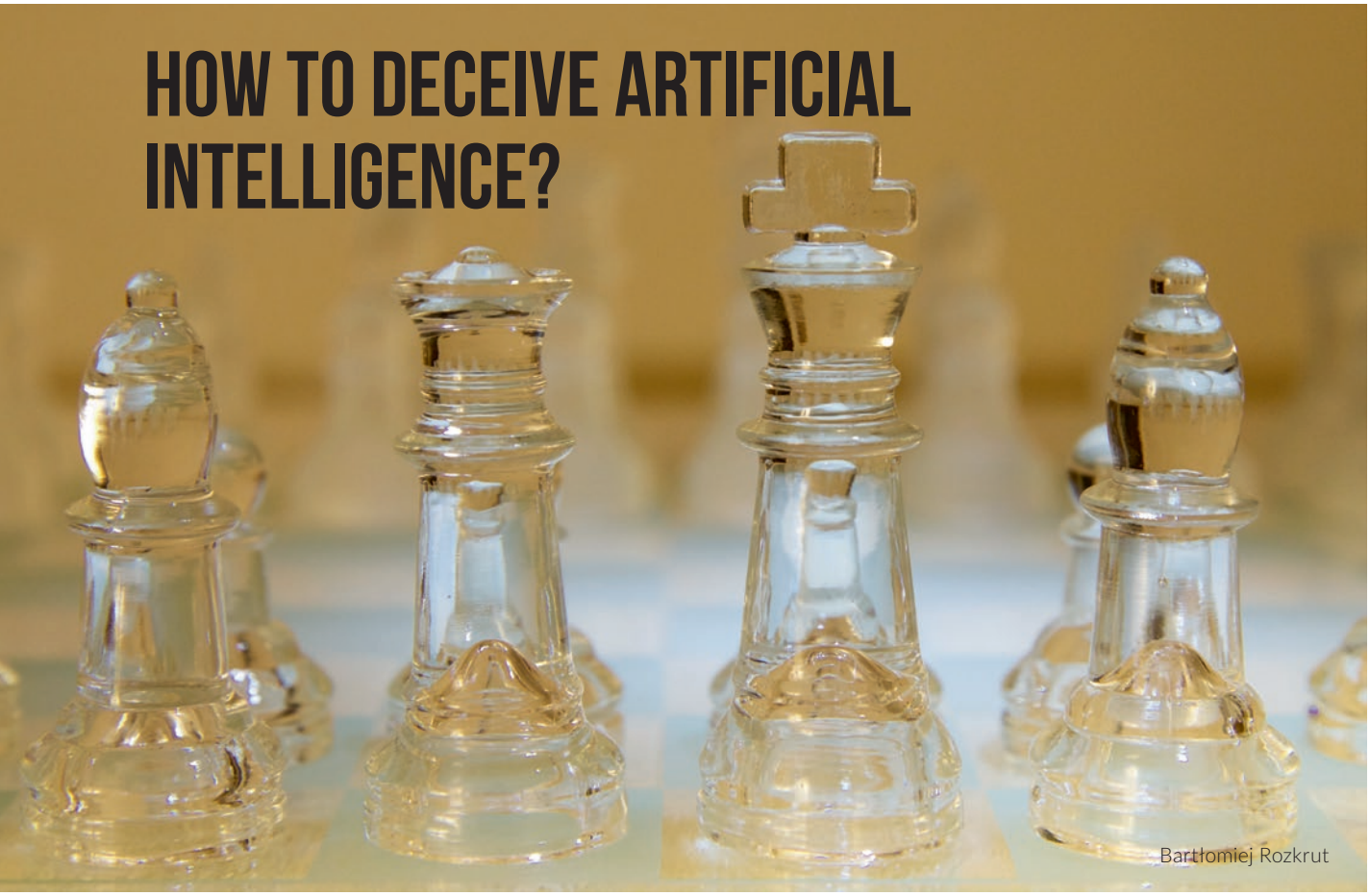
The Techmo crew designed Sarmata 2.0 – a modern ASR solution – to respond to the issues mentioned above. We stay in touch with business owners and day-to-day runners. We are proud of our scientific foundations, knowing also that to adapt means to survive. That is why in Techmo we focus on solutions that are easily adaptable and open to changes. We ask, we learn, we implement what we have learned, and then we ask again... The customer always knows best, and thanks to such an attitude we know best, too. Sarmata is a secure and intuitive speech-recognition software. We believe in automation as another step to give humanity a chance to make a change, leaving undemanding jobs for robots. ■

TECHMO

BARTOSZ ZIOLKO

Dr Bartosz Ziolko is the CEO of Techmo and an assistant professor at AGH University of Science and Technology in Krakow, Poland where he graduated in 2004, in Electronics and Telecommunications. He did his PhD in Computer Science at the University of York, UK in 2010. His research interests focus on speech recognition, language processing and sound tracing for computer games and virtual reality. He is a member of the International Speech Communication Association. He participated in the TOP 500 Innovators programme at Stanford University and in the SIMS programme at Fraunhofer Institute and IBM Watson Centre.

HOW TO DECEIVE ARTIFICIAL INTELLIGENCE?



Bartłomiej Rozkrut

Artificial intelligence or another bubble?

Artificial intelligence development has been in progress since mid-20th century. Unfortunately, despite many predictions about quickly obtaining measureable effects of the development of these technologies, for many years this goal was impossible to achieve. From today's perspective, the periods of slowdowns in artificial intelligence development are called 'AI winter'. These periods were caused mainly by the clash of very high expectations and only minor progress in the development of this technology.

However, recent years have brought significant changes in the speed of artificial intelligence development. Thanks to a rapid growth of computational power, and most of all because of the implementation of graphic coprocessors (GPU) for calculation, the experiments could be conducted significantly faster, which resulted in a much faster solving of problems related to the machine learning algorithms application. Moreover, a dynamic increase in data amounts, which could for instance be used for training neural networks, helped obtain better results more quickly. At the same time, all these factors were affecting each other, which resulted in first significant breakthroughs comprehensible to the layman, e.g. computers received better results than humans in the area of image recognition during the ImageNet contest in 2015. The following years brought a series of spectacular events, such as the beginning of the era of autonomous cars, rapid improvement of the automatic translations, voice recognition, etc. It is very important to note that practical applications of the solutions have already returned the costs of the research, with Google's air-conditioning energy cost-optimisation system being a good example. The optimisation process was conducted by DeepMind, a company which Google bought several years earlier. Thanks to good publicity, all these achievements encouraged more people to get involved in artificial intelligence development and, what is even more important,

the demand for the practical application of AI has grown significantly.

Artificial Intelligence Democratisation

We will remember the year 2016 as the year of AI democratisation: the biggest companies developing the technology published their versions of libraries facilitating or speeding up the development of individual solutions. Moreover, first high-level tools allowing the use of selected machine learning algorithms in narrow applications started emerging, i.e. OpenNMT solution which was designed for training individual models of machine translations (e.g. from Polish to English). It seems that the coming years will bring even more libraries, especially of the high level, thanks to which the use of various algorithms of machine learning will be even easier, and as a result more available and used more often.

There is no alternative to machine learning: the limitations of our mind prevent us from writing highly complicated algorithms, as we cannot understand them ourselves. Voice recognition is a good example of such an algorithm; it is so complex that in order to make it work, one cannot rely on traditional methods. Fortunately, we are able to create algorithms which can in turn generate much more complicated algorithms.

„Mobile first to AI first"

In October 2016, Google started promoting the 'Mobile first to AI first' slogan in order to show that we are on the verge of the next important change in terms of software development. Elements of artificial intelligence will become a natural ingredient and a binding agent for IT systems. AI elements will enable us to solve problems which would be unsolvable or very expensive to solve without them. In order to maintain the competitiveness, software will have to be based on artificial intelligence elements.

Thanks to machine learning, software will become more transparent for the user: it will become proactive and will advice the user in the right moments. This is exactly the approach we adopted for the 2040.io intelligent sales assistant which works in the background. We developed a system which facilitates business trade relations and ultimately will replace CRM class solutions. Development of a sales assistant which acts proactively would not be possible without the use of artificial intelligence elements. The assistant makes assumptions based on data, including electronic mail and data found on the telephone, in order to learn about relations and suggest actions. All with minimum engagement of the user: entering data is not necessary.

Challenges related to the safety of applying elements of artificial intelligence

The growing number of solutions based on artificial intelligence should be accompanied by an increasing awareness about the challenges related to the safety of this technology.

Right now, there is a popular belief that artificial intelligence will one day 'get out of hand' and stand against us. There are numerous articles, books and movies about this concept. However, such course of action would only be possible after developing artificial intelligence that could compete with men.

Current AI systems can be classified as 'ANI' – Artificial Narrow Intelligence – meaning systems with narrow specialisation, which cannot use acquired knowledge in different areas of expertise without the creator's intervention. These systems can achieve better results than people, i.e. they can beat the world's best players in the highly complex Go game. However, a system trained to do so would not be capable of doing other tasks, e.g. play chess. This would be time-consuming and require an appropriate retraining of the system.

Artificial General Intelligence (AGI) class system is the next stage of AI development. These are hypothetical systems which could compete with us in various areas and use knowledge regardless of the field. According to some predictions[1], such systems may not be

1 | https://arxiv.org/abs/1705.08807.

available until 2040. Predictions in regard to the time of creation of such systems vary: scientists from Asia seem to be the most optimistic on this subject, while American scientists are more pessimistic. Interestingly, Elon Musk, the famous entrepreneur, believes that the years 2030–2040 are a probable perspective.

The last stage of development will be the Artificial Super Intelligence class systems: AI which exceeds human capabilities. According to numerous theories, this stage may come quickly after we reach Artificial General Intelligence, because AGI-equipped machines will be able to self-develop much more quickly than with the help of men.

Challenges related to Artificial Narrow Intelligence

ANI class systems are now being used in more and more solutions. In the coming years, these solutions will be applied in autonomous cars, which require the highest safety standards. Unfortunately, techniques of preventing attacks on machine learning algorithms were not developed as fast as the dynamically developing AI technologies.

In order to better understand the description of the dangers, we should learn two important definitions. Firstly, machine learning, which is a subdomain of artificial intelligence. Currently it is often treated as synonymous with artificial intelligence, while in reality it is a collection of techniques which allow the development of a model that realises the assigned task (goal) based on the supplied data. There are different approaches which can rely on elements of artificial intelligence, i.e. autonomous cars using rules-dependent systems apart from machine learning.

The second term is a model. A model is simply a collection of values which describe specific characteristics of data used to train the model. The training itself is based on the selection of appropriate values of the model in order to achieve better results using reasoning based on the model. The model in conjunction with software may serve as a kind of algorithm or even a program realising a specific task. What is important is the fact that the model is not created by a programmer but by a machine learning an algorithm based on data.

The following sections describe selected types of attacks on machine learning algorithms, especially deep neural networks, which is one of machine learning techniques.

1) Model training based on user data

Training the model, meaning running a program which creates the model (an algorithm) based on external data, can be very dangerous. Very often, data coming from users is used to train machine learning models. In classic program defence against intentionally compromised user data, the problem is much simpler since the program is usually static – developed by a programmer. In case of neural networks, the situation is much more complex, since the user data may be used to train the model, which facilitates the creation of the algorithm/program. The programmer is only responsible for the manufacturing of the software which creates the model. Appropriately prepared data may cause aberrations of the model in favour of the users who have intentionally compromised the data for their profit. The technique of influencing the activities of the model with compromised data is called poisoning the model.

2) Reasoning using user data

Trained models are used for reasoning – meaning to get answers based on supplied parameters/data, which usually come from users. Unfortunately, even if the model has been trained in sterile conditions – based on non-compromised user data – there is still a considerable danger of the model being deceived by user's data during the reasoning process. Right now, we know about attack techniques used on image recognition algorithms which allow corruption of the image classification during the inference process. The OpenAI organisation, which focuses on AI safety issues, published a very interesting paper on this subject. The paper presents a technique which utilises the so-called 'Adversarial Machine Learning' – a technique which adjusts the colour values of pixels so that humans do not see any difference

on the altered image, while the neural network gets a wrong classification result – which is in line with the attacker's expectations. Additionally, the result has a high probability, which means that the model is quite sure about its assumption. This type of attack is very dangerous for autonomous cars that analyse a very large number of images in a short time. In the course of the research it was proved that such attacks could be conducted by using a printed compromised image, and then taking a picture of it using a regular camera, which is also wrongly classified – in line with our expectations.

Unfortunately, right now no effective technique to defend the model from such attack is known – this applies to passive identification of corrupt entry data and the active protection technique. All attempts to identify or defend against such attacks were overridden in the course of the research.

3) Additional model training using user data

In order for the model to adjust to the changing situation or users' expectations, it needs to be constantly trained. This means that the model (algorithm), which we have created in sterile conditions, may be degraded in the course of exploitation due to additional training using intentionally compromised data. The additional training process usually takes place in a completely automated environment and in short cycles, which makes it even more difficult to analyse the system's behaviour anomalies associated with the introduction of new data.

4) White- and black-box methods

Having access to the program's code accelerates the search for vulnerability and the preparation of the attack on classic software. Similarly, the access to the neural networks' model enables faster preparation of data which will deceive the model. Access to the contents of the model is often forbidden, however there are plenty of techniques which can be used to work around this problem. One of them is to develop a substitute of the model; this means training your own model which reasons similarly to the attacked one. Several papers describe the transferability of the wrong classification attack between different models realising the same task – despite the differences in the training methods and model's architecture, such an attack is possible. This leads to a situation in which the attacker trains the substitute model in order to speed up the preparation of the white-box attack.

5) Data privacy

Data used for model training is not copied to the model. However, the model may adopt too many of the data's features – especially if there emerges the so-called overfitting problem. This problem means that the model delivers very good information for the data used in the training process, but it does not work so good using data it has 'not seen'. In order to prevent this problem, a series of precautions to achieve better generalisation ability are taken. Unfortunately, for now deep neural networks are a black box for us – they work, but we are not sure how. Currently, the analysis of their behaviour is difficult. It is related to the data privacy problem – if we do not know how exactly the trained network works, it is possible for the data used in the training process to be partially reproduced if someone comes into possession of the model or gets the opportunity to take advantage of the model's reasoning without limits. One of the defensive techniques for such situations is supplying the model with training data that was already generalised by another model – creating additional layers. Unfortunately, it was proved that this technique is not fully effective.

Anonymization of the training data is one of the common defensive techniques – for example, if we are using electronic mail for training, it should be anonymised first in order to prevent a situation in which the model can learn the characteristics that enable it to identify specific persons.

6) Availability of the model

The attacker who is able to supply compromised data to the training process or to perform additional training may try not only to distort the results of the model's reasoning, but also to block it completely, which may

have effects similar to the 'Denial of Service' attacks and result in a complete deactivation of the service.

7) Stealing the model

The abovementioned method of substitute model training for preparing attacks using the white-box method may also be used to steal the model. If the attacker has access to the results of this model's reasoning, they may be able to recreate the model. The risk is high if the attacker has unlimited access to the model, which they can use to supply reasoning data. In the course of reasoning, the attacker achieves a collection of data which they can use to train their own model that will have similar characteristics to the original model.

Artificial General Intelligence: future challenges

Right now, there is a popular belief that Artificial Intelligence will pose a threat after its intelligence is comparable to that of humans. We should, however, first take care of the safety of Artificial Narrow Intelligence solutions which are currently used in practice.

While the discussion about the defensive mechanisms which must be implemented in AGI is important, it does not, however, guarantee any safety. The development of artificial intelligence that could compare to human intelligence is simultaneously conducted in many different places, in different political, military and economic conditions. It is not possible to develop uniform regulations for a technology like that, because the limitations of physical world will not apply to it, since it will be mainly a digital being.

Right now, there is no technique or a collection of regulations which would prevent us from losing the control of AGI. However, the development of interfaces connecting the human brain and software looks promising. Thanks to such solutions, artificial intelligence may be complementary to our mind, giving us additional capabilities.

Summary

The use of artificial intelligence will soon be a common thing – in order to prevent serious problems related to the safety of these systems, we should be aware of the problems machine learning may become for the creators of new solutions. In the case of traditional software, a correction of an error is often very easy – all you need to do is correct one line of code or run a patch. Unfortunately, it is much more complicated when it comes to trained models, since the model was not programmed by a person, but by a training program. It is not possible to simply repair a part of the model. Usually, a repeated training is necessary, which may take a long time. Additionally, many models, especially those based on deep neural networks, are a black box to us, which makes finding the cause of problems a lot harder.

Currently, the materials about machine learning safety are scarce; at the same time, scientific papers and articles related to the subject are worth following – a bigger awareness of the problem will help us build solutions that are better prepared for new types of attacks. ■

BARTLOMIEJ ROZKRUT

Bartlomiej is the CTO & co-founder of 2040.io. He began his IT career as network administrator and further on as web application developer. Based on his experiences, he was able to run entire IT projects. As CTO, he has been responsible for the technology development of the Empathy Internet Software House since 2005. He became a Board member in the Unity Group in November 2012, as the e-commerce development Director of the company.

Currently, he works on artificial intelligence projects in business, as 2040.io CTO. He specializes in the analysis of projects regarding their technical architecture and integration with external systems.

Bartlomiej is also a lecturer for postgraduate studies at the Wroclaw University of Economics, earlier on involved at the European Higher School in Krakow.

Adopting the new. What Risk Managers Should Know about Artificial Intelligence driven Anti-Fraud Solutions

Gareth Leggett

The threat landscape facing organisations is growing more complex as fraudsters employ the latest advances in technology to achieve their goals. Organisations themselves are also embracing new technologies to drive revenues.

This arms race is one that Risk Managers cannot afford not to take part in. Both the fraudsters and the organisations themselves are adopting new solutions, approaches and paradigms. Risk Managers now also have an opportunity to play a part in this process by implementing Artificial Intelligence driven Anti-Fraud Solutions.

Changing Business Landscape

The channels used by digital e-commerce and financial services continue to grow and develop on an almost daily basis as mobile and web applications are used by an ever-increasing number of customers. New business models evolve across multiple verticals. Customers demand that physical goods are delivered in hours, not days. Digital content must be available instantly. Travel must be available with time to departure of 24 hours, not 72 hours. For organisations to grow, these customer demands must be met in a seamless omnichannel environment across all device types.

Key Messages

- Online fraud is becoming more sophisticated due to rapid advances in the technology available to fraudsters.
- Digital merchants and financial services are vulnerable due to evolving business models.
- Artificial Intelligence (AI) and Machine Learning (ML) provide organisations with the tools to effectively detect and prevent fraud.

There is a Price to Pay

The downside to this growth is the increase in fraud and the associated losses from chargebacks. Fraudsters have evolved their approach by targeting not only payments, funds transfers and goods shipments, but also account opening, loyalty card transactions and gift card purchases. New fraud attack patterns and technologies are advancing at a faster rate than the traditional risk systems deployed by organisations. Faster and cheaper computing resources are available and are giving fraudsters the power they need to mount ever more sophisticated attacks. The increasing ability to detect and exploit system vulnerabilities means that risk systems built on static rules no longer provide the necessary protection. With fraudsters using distributed networks and utilising the dark web to source both vulnerability data and stolen credential data, the profile of an organisation can change from apparent safety to being at the brink of a massive breach in the blink of an eye.

Real Time Protection

The ability for an organisation to defend itself requires the ability to react in real time by deploying dynamic risk solutions. Rule-based risk management solutions are not able to cope in the face of this sophistication, power and speed. In this environment of increasing risk, AI- and ML-based risk management offer real world, real time, responsive and dynamic solutions that are easy to deploy, use and maintain. For most of the e-commerce era, risk management has focused on using business intelligence (BI) and predictive analytics to power static rule-based systems. AI- and ML-based technology have entered the public consciences and have become a part of our daily lives thanks to consumer products and technologies such as music and shopping recommendation services. But due to media reporting and overly ambitious marketing departments, there is some confusion around the subject. This leads risk managers to ask how AI- and ML-based systems will help in risk management.

Artificial Intelligence/Machine Learning

AI and ML are current trending buzzwords that are often talked about but poorly understood, and therefore the relationship between them should be established. AI is described as a computer system that can react to changes in its environment in an intelligent way (intelligence in this context is where the outcome of the reaction can be measured against an objective function). ML is a branch of AI. ML enables systems to automatically learn, predict, and act. Combined with the power of the big data (including data that exists within organisations, data collected as part of the transaction and external data sources), organisations can use ML powered risk management systems to perform analytics and generate risk scores in real time with high accuracy. ML uses models that are applied whenever data is used for decision making, including account opening, transaction approval and identity verification.

AI- and ML-based risk management tools enable organisations to:

- Reduce fraud and the associated chargebacks by using data to identify new attack patterns that are unknown to the organisation

GARETH LEGGETT

Gareth is a seasoned Cybersecurity professional with 20 years of experience in the Information Security sector. He has held roles in the UK and overseas helping organisations to secure their information assets and reduce fraud.
As a former PCI SCC Qualified Security Assessor (QSA) Gareth has worked with clients across multiple verticals. He brings a global perspective and with experience in security, compliance and incident response he has assisted executives at leading international companies meet their Information Security challenges. Before joining Nethone Gareth held senior positions at leading Information Security vendors including Verizon Business, BehavioSec, Lockheed Martin and Axent Technologies.

- Reduce costs by replacing ineffective, resource intensive static rule-based risk tools with self-learning systems
- Improve the user experience by reducing false positives and manual reviews

These abilities enable risk managers to deploy systems that make better decisions relating to fraud.

Risk Management

Risk management is defined in many ways, but the goal is the same: to maximise the realisation of objectives. Existing risk management systems based on static rules are no longer capable of lowering both false positive and false negative rates. Faced with the choice between high chargeback levels or high levels of declined transactions and manual reviews, Risk Managers must follow the example set by the fraudsters by using the latest technology to reduce chargebacks, manual reviews, and declined transactions.

The risk management model has always focused on complex calculations and static rules. The application of AI offers the possibility to draw on large datasets using models that evolve and keep the system one step ahead of the fraudsters. The risk management function currently uses systems designed on rules to monitor transactions leading to alerts, manual reviews or denials. Risk Managers use rules and thresholds to set these alerts, and tuning these takes a great deal of time and effort.

Challenges of Static Rule-Based Systems

Static rule-based systems present challenges. The first of these are the false alerts generated by existing systems. Settings that are too sensitive mean more manual reviews and declined transactions. If the settings are not sensitive enough, then chargebacks will increase. Static rule-based systems create alert fatigue as systems are tuned to ever more conservative levels. When alert fatigue sets in, operators expect false alerts, miss genuine frauds, and allow these transactions to proceed. Every transaction that is sent for manual review comes at the expense of the user experience and risks losing not only that purchase but also future purchases.

Comprehensive risk management uses real-time and historical data, but the weakness of static rules stems from the fact that these rules are defined by humans. While humans are good at interpreting simple patterns, we have limitations when it comes to complex patterns. The solution is to deploy AI-based systems to decipher complex attack patterns. Computers have always been able to complete calculations faster than humans, but with AI and ML these systems now have the ability to learn.

The next challenge is that static rule-based systems do not change unless they are reprogrammed by the risk team who are already overworked because of the alerts generated by the system. AI-based systems automate this process by learning and using this knowledge to update the system rules. Static systems simply do not evolve at a rate to match the threats and business objectives leading to more chargebacks and more manual reviews.

AI/ML-based Risk Management Systems

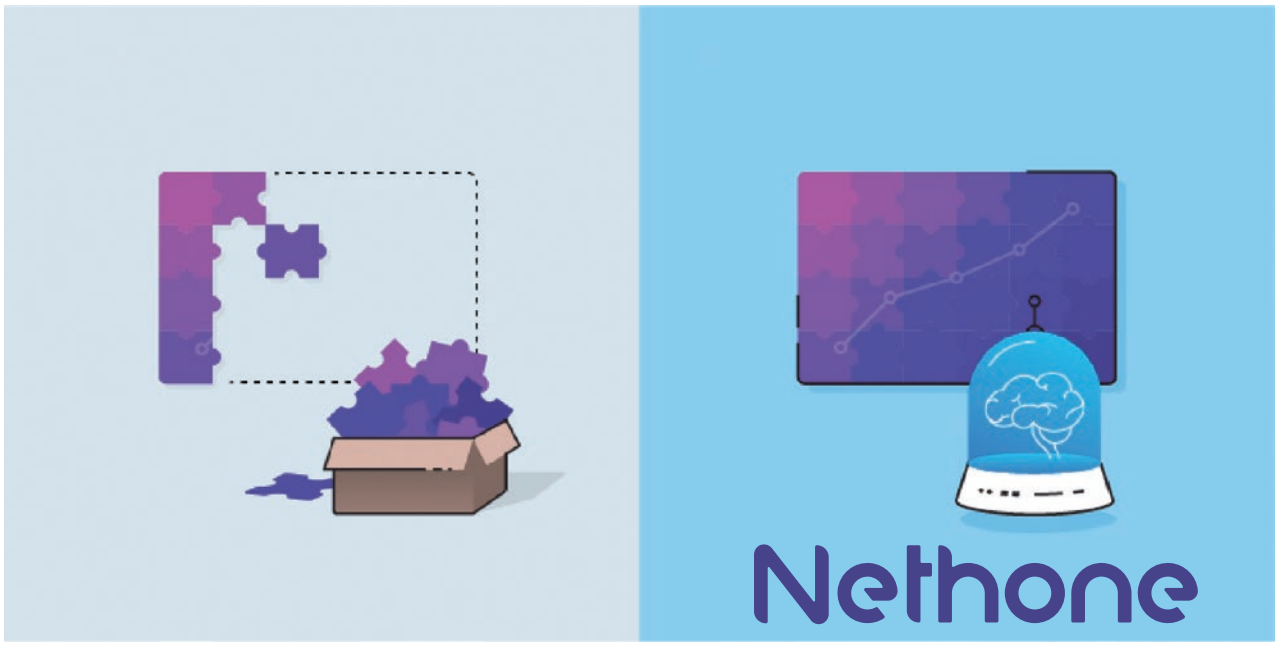
AI/ML-based systems address complex environments that are driven by uncertainty and ambiguity. These systems are being deployed to empower business decisions and to enable greater accuracy in risk scoring by complimenting human resources and traditional analytics. Risk management is particularly suited to the adoption of AI/ML-based systems, because the risk environment includes unknown and seemingly unconnected events. Various organisations have begun to use large amounts of data in order to improve their risk posture; however, static rule-based systems have become increasingly unable to handle this volume of data. By using AI/ML-based risk systems, organisations are able to use this data to find indicators of known and unknown risk and to find the connections between seemingly unconnected events. Just as online music services learn and recommend based on what we listen to, AL/ML-based risk systems learn and are able to recognise and prevent fraud.

The use of AI/ML-based systems to manage risk is particularly helpful when used for the handling and analysis of large volumes of data. As the data volumes get larger, the ability to define simple rules decreases. ML models use self-learning to constantly improve the performance of the systems to gain insights from large volumes of data. By using AI/ML-based anti-fraud systems, organisations can use transactional and historical data and enrich this with external feeds. The Nethone anti-fraud solution, for instance, gathers, at a minimum, over 3,000 data points. As a side note, risk managers should always question data point collection numbers. As vendors claim ever-growing numbers of data points, questions should be asked in order to validate these claims. Using the mouse or touchscreen position as an example: is the mouse movement counted as one data point or is each change in the X/Y coordinate counted as a data point. If the latter is counted, then hundreds or thousands or data points can be claimed.

At Nethone, alongside high-quality data, a customised machine-learning solution is created and deployed for each organisation. The creation of these machine-learning models requires both technical and business expertise. Instead of deploying static rules that lead to labour intensive manual reviews, AI/ML-based systems can prevent fraud in real time by employing models capable of identifying the most advanced fraud attempts without affecting genuine customers.

Using thousands of data points for each transaction verification, ML can exclude the use of static rules. AI/ML-based systems learn continuously and are not bound by a list of fixed rules. ML models automatically adapt to the changing business landscape, recognise irregularities and anomalies and become more and more effective with each new analysis being carried out.

Organisations that leverage AI/ML-based risk management solutions are able to anticipate and proactively manage risk to gain a competitive advantage, as well as to maximise the realisation of their objectives. As these systems continue to learn on a daily basis, they can detect the ever more complex fraud patterns that are unknown today and therefore offer the biggest benefit to risk management. AI/ML systems are able to uncover emerging patterns that human resources are not able to detect. These new patterns are then added to the self-learning model, making the system more accurate and providing the ability to offer better protection.



Back to basics: AI/ML vs static rules in Risk Management Systems

Let us use fraud detection as an example. The existing method for fraud prevention was to analyse the transaction data against a list of static rules. As an example, a human fraud prevention operator would create a threshold for any transaction over EUR 2,000. This threshold would be loaded to the rules list and any transaction over that amount would be flagged for manual review by a human resource. The issue with this approach is the number of false positives and the cost of manual reviews. Even if the transaction is approved after the review, the customer may have cancelled the order and taken their business elsewhere. With an AI/ML-based system, large amounts of data and external data sources are used to make a robust and accurate decision based on this data and not just on one rule. Even if the system triggers a manual review and the results of this review determine that the transaction is genuine, then the system learns from those human insights, further increasing the accuracy of the system.

Features that risk managers should look for in AI/ML-based risk systems and vendors:

- Are the models trained per client and per business case? Is your business logic embedded into the model providing an exact fit to your needs, or does the vendor use a one-size-fits-all approach?
- Does the system rely on predefined rules?
- Is the system data agnostic?
- Can your internal and external data sources be used to enrich the gathered transactional data?
- Does the system learn over time or do the rules remain static?
- Does the system provide a comprehensive profiler to gather additional information to power the decision-making process?
- Does the solution prevent as well as detect fraud?
- Can the solution compliment your existing tools?
- Does the vendor employ world class AI/ML specialists or do they use third parties?
- Is the solution comprehensive? Does it include data gathering, API for custom payloads and transaction flow, data augmentation, ML, human readable feedback and a graphical panel, or will you need multiple components from multiple vendors?
- Does the system provide feedback and analysis for each recommendation or simply a recommendation?
- Is behavioural and behavioural biometric data gathering included?
- Does the vendor research and deploy detection of the latest fraud tools?
- Does the system detect deviations in browsers, devices, and operating systems, or does it rely on metrics that are easy to spoof?
- Does the vendor deploy multiple methods of fingerprinting to avoid cloaking techniques?
- Does the system automatically discover inconsistencies and associations, collect and enrich data, and build and test multiple ML models to create the most accurate production systems?

Fraudsters are embracing the latest technologies, so in order to keep one step ahead, Risk Managers also need to adopt the new – immediately. ■

More insights from Gareth Leggett to be included in the next issue of ECM.

FOREIGN BODIES WITHIN YOUR ORGANISATION: HOW TO MITIGATE THE RISKS OF SHADOW IT WITH CLOUD ACCESS SECURITY BROKERS (CASB)

MARCIN SZARY

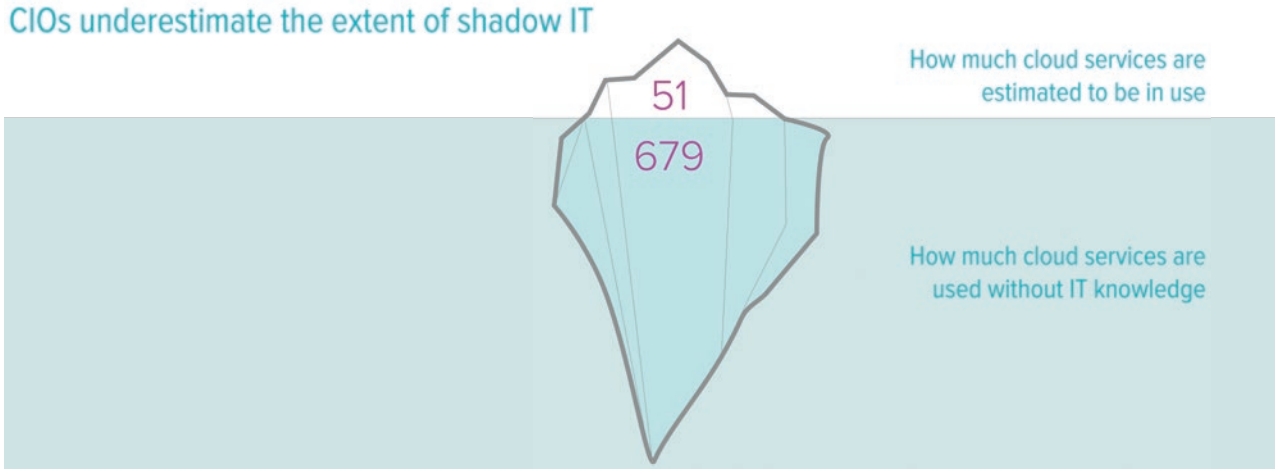
Experienced (15 years) tech professional with focus on information security and identity management specifically. Previously the CTO of multiple startups in mobile, telecom and security space. He was held responsible for R&D operations in the area of multi-factor authentication, mobile payments, notification services within GSM-networks and more. As a contractor, he conducted multiple projects on virtualization, storage architecture and data security for enterprise clients within telecom, banking and public sector. Currently, Marcin is the CEO of SESAME+ helping companies secure access to a highly distributed and growing user population.

Gone is the era of an IT perimeter determined by a firewall or corporate computers. In search of business agility, increased productivity and satisfaction, employees are bringing their personal technology to work. This unsanctioned software and hardware has also its darker side – a shadow casting over the security of an enterprise.

BYOD and BYOA: the rise of IT consumerisation

Great Britain, the 1970s. The rise of supermarkets offering alcohol cheaper than that in pubs permanently changes the drinking culture of the British. However, more and more people go out to eat. Owners of Indian restaurants react to these social changes by making it "legal" for their guests to bring their own drinks. The trend has been called "Bring Your Own Bottle". A few dozen years later, IT departments in companies of all sizes are facing two trends which apart from new opportunities pose a myriad of challenges. Those are namely BYOD (Bring Your Own Device) and BYOA (Bring Your Own Application).

The first trend is here to stay – as of now, 38% of IT directors decide not to purchase company devices for the employees. In 2020, that number may grow up to 45% (Gartner). The latter trend finds its origins in yet another one – EUDA (end-user developed applications) – where the more tech-savvy users created tools augmenting the functionality contained in the formal MRP/ERP systems. Those were usually tools built in Microsoft Access or Excel. Today BYOA means not only cloud services which the employees access from their private devices in order to accomplish business tasks. Recently, the bigger concern are the enterprise business units acquiring cloud services directly without IT's involvement and with little regard for cloud security. It is thus not surprising that Gartner expects 95% of cloud security failures to be caused by the customers by the year 2020.



You cannot manage what you cannot see

Not surprisingly, it is still the responsibility of IT to protect the data of an organisation, even beyond the sanctioned hardware and software. But how to manage something that cannot be seen? And actually, how big is that which cannot be seen? Cisco conducted a research in large companies from the USA, Europe, Canada, and Australia. The results show that, on average, the CIOs are aware of only 7% of cloud services that are being used at their companies. More precisely – IT departments estimated that their companies use an average of 51 cloud services, when in reality 730 cloud services were used. Furthermore, the trend is rapidly growing, so at the moment of writing this article the number of cloud services in the shadow of IT may be reaching 95%.

Prohibition never works

Attempts at blocking unwanted cloud services, using firewalls or proxy were often the first response of IT departments, shocked by discovering the size of "the shadow". However, the results proved to be the opposite of what had been intended. Blocking well-known services resulted in the users migrating to lesser-known and potentially riskier ones. As a result, this pushed users even deeper into the shadow, putting the company at an even greater risk.

CASB to the rescue

A tool helping to regain vision and control over both the shadow and the sanctioned cloud usage is the solution for which Gartner coined the name Cloud Access Security Broker (CASB). Basically, it is an on-premises or cloud-hosted software that is located between the users in an organisation and the cloud services which they access, acting as a control point for enforcing security policies. Initially, CASB is supposed to execute four main tasks: Visibility, Compliance, Data Security, and Threat Protection.

Logically, CASB appears always between the users and the cloud services. Architectonically speaking, it may act as a forward or/and reverse proxy, intercepting all traffic, or as a separate service integrated with the cloud providers that have exposed events and policy controls via their API. Increasingly, vendors have been providing both variants – calling it "multi-mode" or "mix-mode"

The four pillars of required CASB functionality

Visibility

Primary functionality providing administrators the consolidated view of all cloud usage within organization. Cloud services are categorized and labeled with risk scores. Some vendors provide information on recent security breaches of the applications in use. The monitoring and evaluation are are also conducted on end-user devices and locations, the traffic is coming from.

Data Security

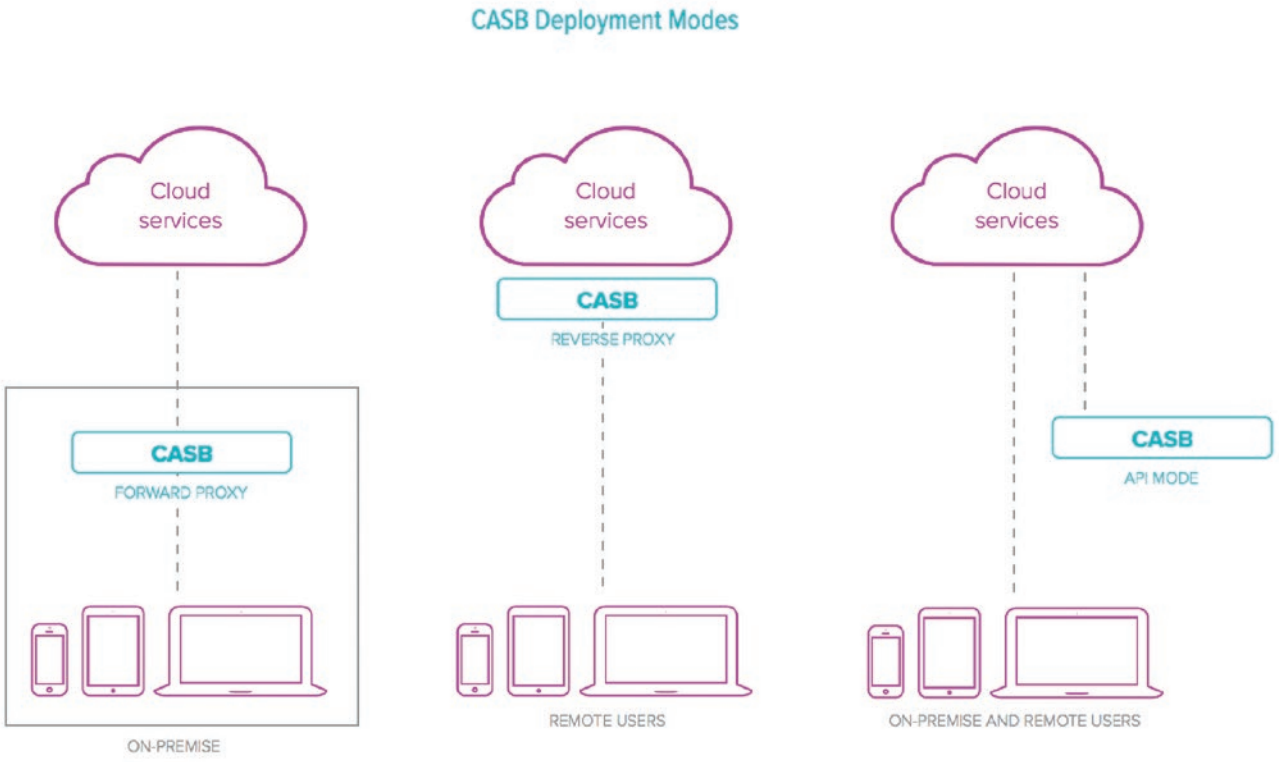
The enforcement of data-centric security policies. It's the ability to protect data leaving enterprise by applying encryption/tokenization, Data Loss Prevention (DLP) or sensitive content redaction. Both encryption key management and DLP may be integrated with external products already in place in the organization.

Compliance

Ensures compliance with standards and regulations related to privacy and sensitive data (including PCI DSS, HIPAA, HITECH). Identify risks of specific cloud services and prevents from falling out of compliance.

Threat Protection

Keeps unauthorized devices and users away from cloud services by using threat intelligence, malware identification, user and entity behaviour analytics (UEBA). Isolates compromised accounts and devices.



CASBs – because each has its advantages and disadvantages. However, from the perspective of reclaiming control over the shadow IT, only the implementation of a forward-proxy model matters, as it is the only one capable of monitoring the use of unsanctioned SaaS applications. The remaining two variants assume that IT already knows which resources in the cloud need to be secured.

Shadow IT and identities: the problem of unified SSO

CASB happily takes advantage of the intelligence already existing within the company. Powered by logs from the firewall, web proxy, integrated with MDM or DLP systems, it provides unparalleled possibilities. However, the issue of identity and access management outside the security perimeter requires an individual approach.

Centralised identity management and Single Sign-on, already implemented within an enterprise, need to be extended to cloud services. Obviously, most CASBs on the market provide such functionality either natively or by integration with partners.

Also, any enterprise-oriented SaaS application is capable of accepting identities coming from another domain, thus enabling SSO and central management. The problem lies beyond dozens of cloud apps recognised and integrated into the central user directory via SAML, WS-Fed or OAuth. It is in the 93% of the apps CIOs are unaware of. Weak, easily guessed, or duplicated passwords protecting enterprise data in unsanctioned cloud apps are the darkest spot of the shadow IT. To make matters worse, these apps do not support SSO, and even if they did, IT departments would have to integrate them over and over again, due to the nature of the dynamics within the shadow IT. And yet compromised credentials are the top concern for 90% of security professionals (RAPID7 Incident Detection & Response Survey), as most of them are incapable of detecting the attacks when compromised credentials are used.

The solution to this problem is taking control over all user passwords. Help your users track their logins, while complying with security standards. Password managers built for enterprises generate strong and unique passwords, integrate with Active Directory and build

compliance reports, but they all have one major flaw. They are not isolated from the users and their devices. Software agents need to be installed and maintained on every device, thus exposing passwords to theft or misuse.

Another way to manage passwords is to make it the CASB's responsibility. SESAME.ID is an example of such an approach. Using Deep Content Inspection and heuristics-based engine, it monitors and adapts authentication-related traffic across all cloud services. It effectively takes all shadow IT related passwords away from the users, replaces them with strong ones under the hood, and links them to the corporate identity.

As a result, users get an SSO passwordless experience across all apps and devices. At the same time, IT has the certainty that all passwords are strong, unique and never stored on user devices. And in the case of a terminating corporate account, all related cloud services accounts will be locked.

Final thoughts

Trends like cloud adoption and IT consumerisation will undoubtedly continue. The growing significance of apps in the SaaS model and penetrating companies with private devices, combined with growing concerns in terms of privacy, security, and compliance, do not leave any choice for both private and public enterprises.

CASB is becoming a must in the fight to reinstate balance between productivity and control over IT. According to Gartner, by the year 2020, 85% of large enterprises will use CASB within their organisation. It is, however, worth stressing out that the CASB landscape is currently very dynamic and matures quickly. A considerable degree of consolidation and acquisition by larger entities has already started, and within two years only seven key players are expected to stay. This means that some technologies may stay in the hands of just one or a few vendors. Therefore, it is wise to avoid long-term contracts, as you may need to use more than one CASB or switch to one that suits your environment better.

Finally, this solution has built-in flexibility – once implemented, a CASB may broaden its influences through further integrations with the rest of the infrastructure, providing more intelligence. And that in turn may help to reclaim the sense that the command over the environment is once again in the right hands. ■

KRAKOW

THE PLACE WHERE CYBER MEETS SECURITY

CYBERSEC HUB

In CYBERSEC HUB we believe that connecting means creating and that every network is more than the sum of its parts. That is why we launched our platform which brings together people from across boundaries. From the private to public sector, from the technical to political spectrum, we connect all those who want to forge a secure cyber future.

CYBERSEC HUB builds on the synergy between stakeholders from the Małopolska Region in Poland, with the city of Krakow as its strategic center. Krakow is one of the largest startup hubs in Europe with over two hundred ICT businesses, unparalleled investment opportunities, and access to talent, funding and the entire EU market. This unique environment is what attracts global IT companies to the area, many of whom have already moved their Research, Development and Security Operations Centres to Małopolska. Krakow also hosts the European Cybersecurity Forum – CYBERSEC, one of the main public policy conferences on cybersecurity.

We are open to those who want to build the CYBERSEC community with us. Whether you are in academia, a CEO, an investor or the owner of a startup, you are invited to become an important part of our network. If you are interested in the project visit our website www.cybsersechub.eu or contact us at cybersechub@ik.org.pl.

THE KOSCIUSZKO INSTITUTE

The Kosciuszko Institute is a Polish think-tank founded in 2000. As an independent and non-profit organization, it gives itself the mission to contribute to the social and economic development of Poland in the European Union and as a partner of the Euro-Atlantic Alliance.

The experts of the Institute regularly cooperate with national and international organizations in the process of policy-making and initiating public debate on strategic issues.

Among its various areas of research, the Kosciuszko Institute leads its flagship projects in the field of cybersecurity, among them CYBERSEC HUB and the European Cybersecurity Forum – CYBERSEC.

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl

THE KOSCIUSZKO INSTITUTE

is the publisher of

EUROPEAN CYBERSECURITY MARKET