Artificial Intelligence / Machine Learning Challenges and Evolution

Mircea-Constantin ŞCHEAU[1], Adrian-Liviu ARSENE[2], Gabriel POPESCU[3]
[1] "Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
[2] Bitdefender, Bucharest, Romania
[3] Independent Cybercrime Intelligent Researcher, Bucharest, Romania
mirceascheau@hotmail.com, arsene.liviu@gmail.com, popescu.gabriel@outlook.com

Abstract

For 2018, one of the big challenges is the construction of security systems based on AI. However, it should take time and considerable resources to verify the effect of technologies involving machine learning and driving patterns. We can say that these structures are, conceptually, a computerized replica of their developers. While the trend is interesting, it does not provide any real guarantee as long as the same steps can be performed by criminals. The two armies faced in the virtual environment are in a continuous arms race, as faithful copies of their creators. Even if efforts seem to be hampered by the dynamics of the criminal spectrum, they are necessary precisely because of their mobility. Malware and ransomware attacks have targeted disparate and seemingly unrelated targets, globally. Condensing huge amounts of data at certain points or in mega-cloud spaces offers management advantages, but it can also be the premise of future offensive, not at all desirable. The confrontation engages the brightest minds on the planet, from both camps [5].

Index terms: cloud computing, cybercrime, vulnerabilities, cryptocurrencies, authentication, regulations, governance

References:

[1]. Arsene, L. (2018), "Cybersecurity Threats and Trends", Bitdefender, pp. 5-6.
[2]. Arsene, L. (2018). Le Machine Learning exploité par les cybercriminels, Cybercriminalité, Cybersécurité (Experts Invités, Hacking, Globb Security) [Online]. Available: http://globbsecurity.fr/machine-learning-exploite-cyber criminels-44130/.
[3]. Benedikt, C. F. and Osborne, M. A. (2013), "The Future of Employment: How Susceptible are Jobs to Computerisation?", University of Oxford.
[4]. Botezatu, B. (2018). Bitdefender, Europol, Romanian Police, DIICOT team up for GandCrab decryption tool (Bitdefender LABS) [Online]. Available: https://labs.bitdefender.com/2018/02/bitdefender-europol-romanian-police-diicot-team-up-for-gandcrab-removal-tool.

[5]. Chauhan, A. (2018). Six Cyber Threats to Really Worry About in 2018 (Article) [Online]. Available: https://www.linkedin.com/pulse/six-cyber-threats-really-worry-2018-aman-chauhan.

[6]. Dangi, R. (2018). FWaaS, Explained! (Coud28+) [Online]. Available: https://www.cloud28plus.com/emea/content/FWaaS--Explained-.

[7]. Deloitte LLP. (2015)," From brown to brains; The impact of technology on jobs in the UK", Official site.

[8]. Deloitte LLP. (2016), "Talent for Survival: Essential skills for humans working in the machine age", Official site.

[9]. Erenhouse, R. (2018). New Mastercard Service Speeds Adoption of Artificial Intelligence (Mastercard Communications, Business Wire) [Online]. Available: https://www.businesswire.com/news/home/20180604005462/en/New-Mastercard-Service-Speeds-Adoption-Artificial-Intelligence.

[10]. Evans, K. (2018). Artificial Intelligence: The Technologies That Will Change Education In 2030 (CSO, IDG Communication) [Online]. Available: https://www.cso.com.au/article/642982/artificial-intelligence-technologies-will-change-education-2030/.

[11]. Goncharov, M. (2015), "Criminal Hideouts for Lease: Bulletproof Hosting Services", A TrendLabsSM Research Paper, Trend Micro, Incorporated.

[12]. Granville, V. (2017). Machine Learning Summarized in One Picture (DataScience Central) [Online]. Available: https://www.datasciencecentral.com/profiles/blogs/machine-learning-summarized-in-one-picture.

[13]. Guszcza, J., Lewis, H. and Evans-Greenwood, P. (2017), "Cognitive Collaboration: Why humans and computers think better together", Deloitte University Press.

[14]. Hill, M. (2018). #Infosec18: How Ransomware-as-a-Service Offerings are Changing in 2018, (News, The Magazine, Infosecurity) [Online]. Available: https://www.infosecurity-magazine.com/news/infosec18-ransomwareasaservice-2018/.

[15]. Howells, L. (2018). AI: It's all about the humans (PA in the media, PA Knowledge Limited) [Online]. Available: https://www.paconsulting.com/newsroom/expert-opinion/police-professional-ai-its-all-about-the-humans-11-june-2018/.

[16]. Kanal, E. (2017). Machine Learning in Cybersecurity (SEI Insights, Software Engineering Institute, Carnegie Mellon University) [Online]. Available: https://insights.sei.cmu.edu/sei_blog/2017/06/machine-learning-in-cybersecurity.html.

[17]. Karapanos, N. (2018). Cyber Security and Artificial Intelligence (Deutsche Telekom AG) [Online]. Available: https://www.welove.ai/en/blog/post/cyber-security-and-artificial-intelligence.html.

[18]. Kumar, M. (2018). IoT Botnets Found Using Default Credentials for C&C Server Databases (The Hacher News) [Online]. Available: https://thehackernews.com/2018/06/iot-botnet-password.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+TheHackersNews+(The+Hackers+News+-+Security+Blog)&m=1.

[19]. Lin, F., Kun, W. C., Song, C., Xu and W., Jin, Z. (2018), "Brain Password: A Secure and Truly Cancelable Brain Biometrics for Smart Headwear", MobiSys.

[20]. Memoria, F. (2018). $1.5 Million: Cryptocurrency Trading Platform Taylor Suffers 2,500 ETH Hack (Ethereum News, CryptoCoinsNews (CCN)) [Online]. Available: https://www.ccn.com/1-5-million-cryptocurrency-trading-platform-taylor-suffers-2500-eth-hack/.

[21]. Morgan, S. (2017). 2017 Cybercrime Report (Cybersecurity Ventures) [Online]. Available: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

[22]. Mu-Hyun, C. (2018). South Korean cryptocurrency exchange hack sees $40m in altcoin stolen (ZDNet, CBS Interactive) [Online]. Available: https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/south-korean-cryptocurrency-exchange-hack-sees-40m-in-altcoin-stolen/.

[23]. Paganini, P. (2018). Chinese state-sponsored hackers steal 600GB U.S. Navy data (Cyber Warfare, Security Affairs) [Online]. Available: https://securityaffairs.co/wordpress/73365/cyber-warfare-2/u-s-navy-data-breach.html.

[24]. Paganini, P. (2018). Crashing HDDs by launching an attack with sonic and ultrasonic signals (Security Affairs) [Online]. Available: https://securityaffairs.co/wordpress/73128/breaking-news/ultrasonic-signals-hdds-dos.html.

[25]. Paganini, P. (2018). Crooks used a KillDisk wiper in an attack against Banco de Chile as diversion for a SWIFT hack (Cyber Crime, Security Affairs) [Online]. Available: https://securityaffairs.co/wordpress/73372/cyber-crime/banco-de-chile-killdisk.html.

[26]. Paganini, P. (2018). Experts warn hackers have already stolen over $20 Million from Ethereum clients exposing interface on port 8545 (Cyber Crime, Security Affairs) [Online]. Available: https://securityaffairs.co/wordpress/73436/digital-id/ethereum-scanning-port-8545.html.

[27]. Paganini, P. (2018). Operazione Prowli: 40.000 server, modem e dispositivi IoT già compromessi (Sigurezza, Security Affairs) [Online]. Available: http://cybersecurity.startupitalia.eu/61244-20180608-operazione-prowli-40-000-server-modem-dispositivi-iot-gia-compromessi.

[28]. Saini, E. A. (2018). Cybercrimes !!! (JST Business Solutions Pvt. Ltd) [Online]. Available: https://www.linkedin.com/pulse/cybercrimes-er-anurag-saini.

[29]. Spring, T. (2018). Mirai Variant Targets Financial Sector With IoT DDoS Attacks (Hack, Threat Post) [Online]. Available: https://threatpost.com/mirai-variant-targets-financial-sector-with-iot-ddos-attacks/131056/.

[30]. Taddeo, M. and Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race (News & Comment, Nature International Journal of Science, Macmillan Publishers Limited) [Online]. Available: https://www.nature.com/articles/d41586-018-04602-6.

[31]. Townsend, K. (2018). The Malicious Use of Artificial Intelligence in Cybersecurity (Security Week, Wired Business Media) [Online]. Available: https://www.securityweek.com/malicious-use-artificial-intelligence-cybersecurity.

[32]. Williams, D. (2018), "The Symbiotic Relathionship Between Humans and Machines", Official site.

[33]. https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html?utm_source=linkedin&utm_medium=cpc&utm_campaign=analytics-global&utm_content=US_skills.