IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, July 2023

A Data Analytics Strategy to the Underground Economy of Cybercrime

K H Sumanth[1] and Mr. Santhosh S G[2]
PG Student, Department of Master of Computer Applications[1]
Associate Professor, Department of Master of Computer Applications[2]
Jawaharlal Nehru New College of Engineering, Shivamogga, India
sumanthkh10@gmail.com and santhoshsgrao@jnnce.ac.in

Abstract: *People, organisations, and governments have tried to discover strategies to fight against the danger of large-scale cyberattacks (such as ransomware and distributed denial of service (DDoS) assaults) and criminality. In 2017, the WannaCry ransomware was to blame for approximately 45,000 strikes across nearly 100 nations. Governments are under pressure to enhance their cybersecurity spending due to the increasing effect of cybercrime. As part of his 2017 budget, U.S. President Barack Obama suggested allocating more than $19 billion on cybersecurity, a more than 35% increase over 2016. As a result, the cybercriminal underground has changed into a brand-new kind of group that runs underground marketplaces and fosters the growth of cybercriminal conspiracies. Cybercrime networks, in contrast, are lateral, diffuse, fluid, and dynamic. Governments, organisations, and people are typically unaware of the threat posed by the development of highly professional network-based cybercrime business models, such as crime ware-as-a-service (CaaS). Despite the quick rise in cyberthreats, little is known about the basics of the field or the approaches that can help practitioners and researchers in information systems who are interested in cybersecurity. Additionally, little is known about Crime-as-a-Service (CaaS), the illegal business model that supports the shadowy world of cybercrime.*

Keywords: Data analytics, Machine learning, Visualization tools, Cybersecurity, Privacy protection

REFERENCES

[1]. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2012). Measuring the cost of cybercrime. In WEIS (Vol. 12, pp. 1-22).
[2]. Christin, N. (2012). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd international conference on World Wide Web (pp. 213-224).
[3]. Eckert, C., &Söllner, M. (2018). Detecting and preventing insider threats: A literature review and integrative model. Computers & Security, 77, 326-350.
[4]. Holt, T. J., &Kilger, M. (2016). The darknet: A digital copyright infringement hub?. Deviant Behavior, 37(10), 1193-1205.
[5]. Marziale, L., & Fischer, T. (2018). Using data analytics to identify darknet marketplaces. Digital Investigation, 26, S92-S99.
[6]. Ramakrishnan, N., & Upadhyaya, S. (2019). Big data analytics for cybercrime investigation. In Big Data Analytics for Cyber-Physical Systems (pp. 155-175). Springer.
[7]. Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In Proceedings of the 24th international conference on World Wide Web (pp. 641-651). ACM.
[8]. Zhang, J., Zhang, Y., & Cheng, Y. (2018). A deep learning framework for cyber threat intelligence in underground forums. IEEE Transactions on Big Data, 4(2), 196-206.