CONCLUSION

This study contributes to the DSR literature in a broader IS context in several ways. Because it takes a DSR approach, it contributes to the design artifacts, foundations, and methodologies in this area. First, by creating example front-end applications, we have demonstrated how our design artifacts (the proposed framework and classification model) can be implemented in practice. Because this study takes a DSR approach, we have focused mainly on building and evaluating artifacts rather than on developing and justifying theory: "Actions are usually considered to be the main focus of behavioral science". We have therefore proposed two artifacts: a data analysis framework and a classification model. We have also conducted an ex-ante evaluation of our classification model's accuracy and an ex-post evaluation of its implementation using example applications. In line with the initiation perspective of DSR, these four example applications demonstrate the range of potential practical applications available to future researchers and practitioners.

Unlike previous studies that have presented general discussions of a broad range of cybercrime; our study has focused primarily on CaaS and crime ware from an RAT perspective. We have also proposed sets of definitions for different types of CaaS (phishing, brute force attack, DDoS attack, and spamming, crypting, and VPN services) and crime ware (drive-by download, botnets, exploits, ransomware, rootkits, Trojans, crypters, and proxies) based on definitions taken from both the academic and business practice literature. Based on these, we have built an RAT-based classification model. This study emphasizes the importance of RAT for investigating the cybercrime underground, so these RAT-based definitions are critically important parts of our framework. In addition, unlike prior research that discussed the cybercrime underground economy without attempting to analyze the data, we have analyzed large- scale datasets obtained from the underground community. Looking at the CaaS and crimeware trends, our results show that the prevalence of botnets (attack-related crimeware) and VPNs has increased in 2017.This indicates that attackers consider both the preventive measures taken by organizations and their vulnerabilities. The most common potential target organizations are technology companies (28%), followed by content (22%), finance (20%), e-commerce (12%), and telecommunication (10%) companies. This indicates that a wide variety of companies in a range of industries are becoming potential targets for attackers, having become more vulnerable due to their greater reliance on technology.

FUTURE WORK

Although our study has made several significant findings, it nevertheless has several limitations that will need to be addressed in future studies. These will be able to add more analysis and significant further insights.

First, we only collected data from the largest hacking community and did not consider other hacking communities. Future studies will therefore need to generalize our findings by investigating a wider range of hacking communities.

Second, this study has focused on the CaaS and crimeware available in the cybercrime underground, but much in-depth analysis remains to be done on the configurations of cybercrime networks. Future research could cluster keywords and threats by industry to provide a deeper understanding of the potential vulnerabilities, and it could attempt to discover the network effects involved or the leaders of the cybercrime underground.For example, they should be aware that there are cybercrime underground markets where hacking tools are sold.

Third, this study calls for researchers, companies, antivirus vendors, and governments to collaborate in the fight against cybercrime using civil resources. Rather than acting alone, these groups should unite to maximize their efficiency and effectiveness.

Finally, this study also has important implications for society. Over the last few years, the world has been facing cyber terrorism and cyberwar threats from nation-sponsored attackers [70]. Pollitt [71] defined cyber terrorism as “the premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by subnational groups or clandestine agents.” Unlike most cybercrime, which is primarily motivated by monetary gain [72], cyber terrorists are politically motivated. As a result, governments should, for example, strengthen their ability to protect their citizens in online virtual environments by enhancing their immediate responses to threats such as cyber espionage and cyber terrorism.

REFERENCES

BIBILOGRAPHY

[1] A Data-Analytics Approach to Cyber Crime Underground Economy Jungkook An and Hee-Woong Kim Graduate School of InformationIEEE Transactions on Information Forensics and Security (Year : 2018)

[2] A. K. Sood, S. Zeadally, and R. Bansal. “Cybercrime at a Scale: A Practical Study of Deployments of HTTP-Based Botnet Command and Control Panels,” IEEE Commun. Mag., vol. 55, no. 7, pp. 22– 28.2017.

[3] Z. Shi, G. M. Lee, and A. B. Whinston, “Toward a Better Measure of Business Proximity: Topic Modeling for Industry Intelligence,” MIS Quart., vol. 40, no. 4, pp. 1035–1056, 2016. “FACT SHEET: Cybersecurity National Action Plan,” ed: The White House, 2016.

[4] V. G. Tasiopoulos and S. K. Katsikas, “Bypassing Antivirus Detection with Encryption,” in Proc., 18th Panhellenic Conf. on Informatics - PCI '14, New York, New York, USA, 2014, pp. 1–2: ACM Press.

[5] G. Giacomello, “Close to the Edge: Cyberterrorism Today,” in Understanding Terrorism, Emerald Group Publishing Limited, 2014, pp. 217–236.

[6] A. K. Sood and R. J. Enbody, “Crimeware-as-a-service—A survey of commoditized crimeware in the underground market,” Int. J. Crit. Infr. Prot., vol. 6, no. 1, pp. 28–38, 2013.

[7] A. Majchrzak and S. L. Jarvenpaa, “Safe Contexts for Interorganizational Collaborations Among Homeland Security Professionals,” J. Manag. Inf. Syst., vol. 27, no. 2, pp. 55–86, 2010.

[8] S. W. Brenner, “Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships,” N. C. J. Law & Technol., vol. 4, no. 1, pp. 1-50, 2002.

[9] R. Venkateswaran, “Virtual private networks,” IEEE Potentials, vol. 20, no. 1, pp. 11–15, 2001.

[10] M. M. Pollitt, “Cyberterrorism — Fact or Fancy?,” Comput. Fraud Security, vol. 1998, no. 2, pp. 8–10, 1998.