Literature review

Research Methods and Professional Practice

**Table of Contents**

[Abstract 3](#_Toc118750444)

[Malware and other cybercrime disruption 4](#_Toc118750445)

[Methods 6](#_Toc118750446)

[Challenges 6](#_Toc118750447)

[Conclusion 7](#_Toc118750448)

[References 8](#_Toc118750449)

# Abstract

In the following paper, I will be going over in-depth over malware and cybercrime disruption in general in the form of a literature review. I will be looking at existing research on cybercrime with a focus on malware, what tools are out there, and why it is essential, as well as the target audience and overall aim of such research. I will also be going over the strengths and limitations but also on what specifically needs to be done in the field.

Keywords: Malware, Disruption, Cybercrime, Network, Internet Service Providers.

# Malware and other cybercrime disruption

According to Ye, Y. et al. (2017), malware currently poses a serious and evolving security threat to all the users that have online activities regardless of whether it varies from generic online browsing to financial activities such as internet banking or, in more current times, involving home automation and access. Having new samples constantly of malware code that can make it harder to detect is a constant battle between security companies such as Comodo, Kaspersky, Kingsoft, and Symantec against different threat actors developing such new code. (Ye, Y. 2017)

Malicious software, also known as malware, is a type of computer program intended to have adverse effects. It is considered one of the most common threats affecting active internet users, and the most frequent types of malware are rootkits, botnets, worms, spyware, and Trojan horses, each with their own particularities, as the name suggests. (Ab Razak, M. F, 2016)

There are many research papers done on malware, and in particular, the one done by Abdallah, I. et al. (2020) goes over how critical energy infrastructure can also be affected by malware and not just regular internet users. This, in turn, creates e National Security concern for the country being affected as it can subsequently affect as well different emergency services, such as hospitals not being supplied with energy when needed.

A study on how malware is spread was done by Ife, C. C. et al. (2021), which covers highlights the use of tools such as botnets in order to perform malware delivery more effectively. According to Ife, C. C. et a,l. (2021) botnets takedowns are counter-operations activities that focus on disrupting malware delivery networks which subsequently enable their growth. The same study shows that having good security practices and procedures as a company can generally help these counter-operations, making them more effective by doing regular security checks on their own infrastructure.

Another good example of a malware disruption study is one done by Javed, A. et al. (2022) with a focus on how Twitter is working on its own network to remove malicious URLs using different characteristics to flag specific tweets that need filtering such as network, user account, and tweet content characteristics.

As technology evolves and with the appearance of IoT, Malware also adapts to new environments, as Al Kindi, A. et al. (2019) study show where new flavors of malware utilize such new technologies and environments to propagate better and faster rates of transmissions. Cloud computing is also a constant target for cybercriminals trying to find effective attack vectors, which later on can be used for botnets or malware propagation. A new study on the flavor of cloud computing done by Monika, A. & Eswari, R. (2022) regarding such vectors looks into ways of counter hidden malware attacks proposing Stegware Neutralization where the hidden item is identified and neutralized with the help of nonlinear transfer function.

As our homes also become more competent and interconnected as well as with home working becoming a norm in our days, there is a higher need for security in such environments. As we connect to the corporate environment from the comfort of our homes, there is a need for a Malware VPN filter to protect businesses and organizations from becoming a target. (Sapalo Sicato, J. C. et al. 2019)

# Methods

As the diversity and usability of malware are vast, so are the research methods looking into the topic for a better understanding of the topic where we can find studies such as Abdallah, I. et al. (2020), which uses an experimental approach to learning by clustering and bootstrap aggregation and combining the output of all the simulations into Multivariate Normal Aggregation method. Others, such as Analysis of malware propagation behavior in the Social Internet of Things (Al Kindi, A. 2019), use simulation methods in order to build relations between components and observe the outcome.

Marked for Disruption: Tracing the Evolution of Malware Delivery Operations Targeted for Takedown (Ife, C. C. et al. (2021) uses a comparison methodology to analyze activities between 3 different sets of malware types while Disrupting drive‐by download networks on Twitter (Javed, A. et al. 2022) is focusing on subsampling of data randomly.

Another efficient way of detecting malware has been explored whiting the following article, Deceiving AI-based malware detection through polymorphic attacks (Catalano, C. et al. 2022), which looks into using machine learning algorithms to classify the malicious code with little human interaction accurately and uses a comparative method in order to conduct the research.

# 

# Challenges

Most of the research used here also has limitations and challenges that vary from a piece of limited baseline information to concerns about privacy and also the complexity of the algorithm employed.

In Disrupting drive-by download networks on Twitter. Social network analysis and mining by Javed, A. et al. (2022) was that the study was performed with a scarcity of baseline datasets, and many of the data that could be gathered was disappearing in seconds

In Marked for Disruption: Tracing the Evolution of Malware Delivery Operations Targeted for Takedown by Ife, C. C. et al. (2021), the study is based on data and techniques used in previous research thus. Data limitation is in place, and thus there could not be any flexibility in adjusting the scenario based on the needs.

VPNFilter Malware Analysis on Cyber Threat in Smart Home by Sapalo Sicato, J. C. et al. (2019) considers an exciting aspect when looking at the limitation. When using a VPN, all the traffic originating from the users utilizing the services is, in fact, privacy. The provider controls the endpoint VPN and thus has having visibility on the traffic being handled. This doesn’t necessarily mean that the provider can decrypt particular end-to-end traffic to capture, for example, banking details. Still, it can gather statistical data on users without their consent.

Although the data on malware is vast and there is plenty of research on the topic, there is substantially less academic work done on the possible benefit outcomes of such code or cybercrime techniques, which can be used for positive and moral consequences. The primary use of such research is for us to better understand the security challenges we face when dealing with these threats and how to better protect from them.

# Conclusion

Due to the extensive usage of malware in cybercrime and as a tool for facilitating botnets as well as exploiting different vulnerabilities in a system and creating multiple attack vectors in the cyber world, malware is a high topic of interest when it comes to research based on the academic sources found so far on the subject there are many questions answered but plenty of targets to explore such as how can we use different cyber techniques and tools with altruistic outcome and intent.

References

Ab Razak, M. F. et al. (2016) The rise of ‘malware’: Bibliometric Analysis of malware study. Journal of network and computer applications. [Online] 7558–76. Available at: <https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_webofscience_primary_000386406300005CitationCount>

Abdallah, I. et al. (2020) Unsupervised local cluster-weighted bootstrap aggregating the output from multiple stochastic simulators. Reliability engineering & system safety. [Online] 199106876–14. Available from: <https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_webofscience_primary_000534159800036CitationCount>

Al Kindi, A. et al. (2019) Analysis of malware propagation behavior in Social Internet of Things. International journal of communication systems. [Online] 32 (15), e4102–n/a. Available from <https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_proquest_journals_2303093947>

Catalano, C. et al. (2022) Deceiving AI-based malware detection through polymorphic attacks. Computers in industry. [Online] 143. Available from <https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_gale_infotracacademiconefile_A716008338>

Ife, C. C. et al. (2021) ‘Marked for Disruption: Tracing the Evolution of Malware Delivery Operations Targeted for Takedown’, in arXiv.org. [Online]. 2021 Ithaca: Cornell University Library, arXiv.org. p. Available from <https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_proquest_journals_2509120881>

Javed, A. et al. (2022) Disrupting drive-by download networks on Twitter. Social network analysis and mining. [Online] 12 (1), 117–117. Available from: <https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_pubmedcentral_primary_oai_pubmedcentral_nih_gov_9391206>

Monika, A. & Eswari, R. (2022) Prevention of hidden information security attacks by neutralizing Stego-Malware. Computers & electrical engineering. [Online] 101107990–. Available from:

<https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_crossref_primary_10_1016_j_compeleceng_2022_107990>

Pais, F. E. (2017) ‘Resilience Enhancement in Cyber-Physical Systems : a Multiagent-Based Framework’, in [Online]. IntechOpen. p. Available from: <https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_biblioboard_openresearchlibrary_oai_biblioboard_com_e985a1de_659a_4ab2_ac84_75f1486cd42a>

Sapalo Sicato, J. C. et al. (2019) VPNFilter Malware Analysis on Cyber Threat in Smart Home Network. Applied Sciences. [Online] 9 (13), 2763–. Available from <https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_doaj_primary_oai_doaj_org_article_0ec610ad4fd14c2fbb03bb0994ff337b>

Ye, Y. et al. (2017) A Survey on Malware Detection Using Data Mining Techniques. /ACM computing surveys/. [Online] 50 (3), 1–40. Available from: <https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_proquest_journals_1969923838>