BOOK CHAPTER | *"The Tricky Trio"*

# Security Measures Against Malware, Botnets & Ransomware

**Joseph Antwi Attoh**
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
**E-mails:** Jaattoh59@gmail.com
**Phone**: +233574346850

## ABSTRACT

The COVID-19 pandemic has witnessed a huge surge in the number of malware and ransomware attacks. Different institutions such as healthcare, financial, and government have been targeted. There can be numerous reasons for such a sudden rise in attacks, but it appears working remotely in home-based environments (which is less secure compared to traditional institutional networks) could be one of the reasons. Cybercriminals are constantly exploring different approaches like social engineering attacks, such as phishing attacks, to spread ransomware. Hence, in this paper, I explored recent advances in ransomware prevention and detection and highlighted future research challenges and directions.

**Keywords:** Ransomware, Cybersecurity, Antivirus, Malware, Ransomware prevention, COVID-19, Ransomware detection

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

**Citation**: Joseph Antwi Attoh (2022): Security Measures Against Malware, Botnets & Ransomware Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 345-352 www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P55

## 1. INTRODUCTION

Malware is an umbrella term that describes any malicious program or code that is harmful to systems. Malware attacks, have over the years, been rising globally and ransomware contribute a greater percentage to these attacks. These attacks affect government institutions, industries, and reputable organizations as well as small and medium scale businesses affecting confidentiality, integrity, and availability of such entities. A botnet is not a virus, rather a collection of automatically connected devices. When infected with malware, cyber-criminals can take control of them and distribute harmful programs like ransomwares or trojans.

Knowledge about motives, the modus operandi malicious actors use in Botnet attacks and malware distribution, security counter measures help individuals and organizations to reduce the risk of being a victim of malware attacks. The paper seeks to explore some security measures one can leverage on to protect systems and individuals from being victims of malware attacks.

### 1.1 Background to the Study

Malwares, especially ransomware attacks posses a greater risk when it is successfully executed. The impact from a ransomware attack can be enormous, few impacts from malware (ransomware) attacks includes extended downtime, damage to brand reputation and sensitive data exposure. Over the years ransomware attacks have been on the rise because the mode of attack is mostly through phishing, clickjacking and drive-by download attacks. The aforementioned attack vectors leverage on the weakest link in cybersecurity, that is end users (humans). Aside these attack vectors ransomware attacks are also propagated through supply chain attacks, Ransomware as a Ser vice and Unpatched systems. According to ncsc.gov.uk, ransomware attacks is the number one cyber threat for organizations and business globally. There is therefore the need to research into the security measures against malwares, ransomwares, and botnets. This paper aims to address the various security measures to help mitigate against malware, ransomware, and botnet. It also seeks find the gaps in these security measures and suggest areas for future research.

## 2. RELATED LITERATURE

During the research, I searched for and identified relevant surveys on ransomware prevention and summarized their contributions in Table 1. Papers were sourced on ransomware solutions from 2017 onwards. The papers came from the following article databases: IEEE Xplore, ACM, Science Direct, and Springer. My searches were made using combinations of the following keywords: 'ransomware detection', 'ransomware prevention', 'crypto-ransomware', 'malware detection', 'key backup', 'data backup', 'access control', 'honeypots', 'machine learning', and 'intrusion/anomaly detection'.

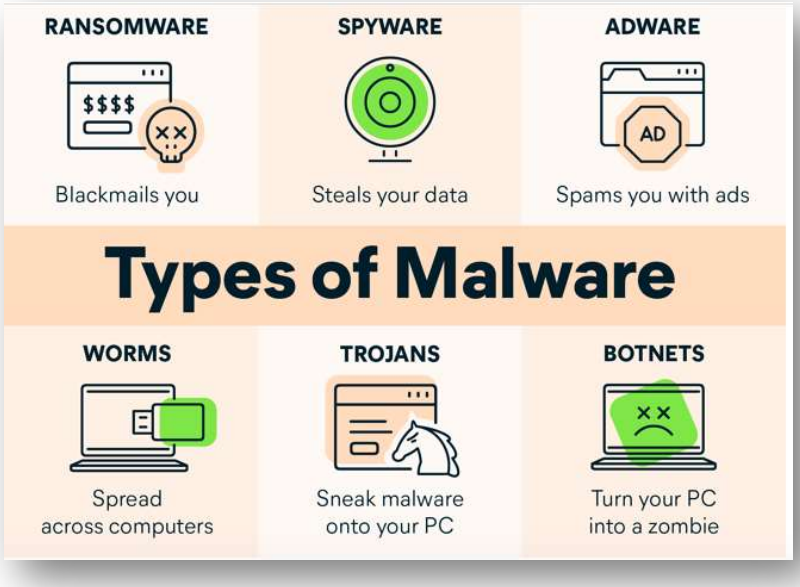


Fig 1: Types of Malware
Source: https://www.avast.com/c-malware

We categorized the surveyed papers into ransomware prevention techniques. Common preventative approaches include enforcing strict access control, storing data and/or key backups, and increasing user awareness and training. Raising user awareness of ransomware attacks and training users on how to avoid them can prevent attacks before they occur.

Table 1: related Literature

| Tool | Papers |
|---|---|
| Access Control | Kim and Lee (2020)[7]; Parkinson (2017)[11] |
| Data Backup | Continella et al. (2016) [4]; Huang et al. (2017)[6]; Min et al. (2018)[10]; Shaukat and Ribeiro (2018)[13]; Thomas and Galligher (2018)[14] |
| Key Management | Bajpai and Enbody (2020) [2]; Kolodenker et al. (2017)[8] |
| User Awareness | Chung (2019) [3]; Thomas (2018)[14] |

## Access Control

Access control prevents ransomware encryption by restricting access to the file system. Parkinson (2017) examined how to use built-in security controls to prevent ransomware from executing in the host computer via elevated privileges. One way that ransomware gains access to files is through a user's credentials if the user has a high level of permissions. He proposed implementing least privilege and separation of duties through role-based access control; restricting data access as far up the directory hierarchy as possible; and routinely auditing permissions and roles. Kim and Lee (2020)[7] proposed an access control list that whitelists specific programs for each file type. Only whitelisted programs are allowed to access files. This implicitly blocks malicious processes from accessing and encrypting files. Whereas a blacklist cannot stop ransomware that it does not contain a code signature for, a whitelist can effectively block new and unknown ransomware.

## Data Backup

Keeping regular backups of the data stored on a computer or network can greatly minimize the impact of ransomware. Instead, the damage is simply limited to any data that has been created since the last backup. There is overhead in backing up large amounts of data, and so choosing how often backups should be taken and how long they will be kept are important decisions to be made. Huang et al. (2017)[6] proposed a solution called FlashGuard that does not rely on software at all. Instead, it uses the fact that Solid State Drives (SSD) don't overwrite data right away - a garbage collector does this after a while. The authors modified SSD firmware so the garbage collector doesn't remove data as quickly, and hence lost data can be restored. When tested against ransomware samples, FlashGuard successfully recovered encrypted data with little impact on SSD performance and life span.

Thomas and Galligher (2018)[14] conducted a literature review of the ransomware process, functional backup architecture paradigms, and the ability of backups to address ransomware attacks. They also provided suggestions to improve the information security risk assessments to better address ransomware threats, and presented a new tool for conducting backup system evaluations during information security risk assessments that enables auditors to effectively

analyze backup systems and improve and organization's ability to combat and recover from a ransomware attack. Min et al. (2018)[10] proposed Amoeba, an autonomous backup and recovery SSD system to defend against ransomware attacks. Amoeba contains a hardware accelerator to detect the infection of pages by ransomware attacks at high speed, as well as a fine-grained backup control mechanism to minimize space overhead for original data backup. To evaluate their system, the authors extended the Microsoft SSD simulator to implement Amoeba and evaluated it using realistic block-level traces collected while running the actual ransomware. Their experiments found that Amoeba had negligible overhead and outperformed in performance and space efficiency over the state-of-the-art SSD, FlashGuard.

## Key Management

Key management refers to recovering the encryption key that was used to encrypt files and using that to decrypt them without paying the ransom. For some ransomware samples, such as samples that hard code the key directly into their executable binary, this may be rather straightforward. For hybrid models, this can be more challenging, as the key is only available in plaintext while the files are actively being encrypted. Some ransomware programs use a symmetric session key for encryption. This key is stored in the victim's computer which then encrypts the user's files. Kolodenker et al. (2017)[8] developed a key backup solution called Paybreak which relies on signatures. PayBreak implements a key escrow approach that stores session keys in a vault, including the symmetric key that the attacker uses. When tested, PayBreak successfully recovered all files encrypted with known encryption signatures.

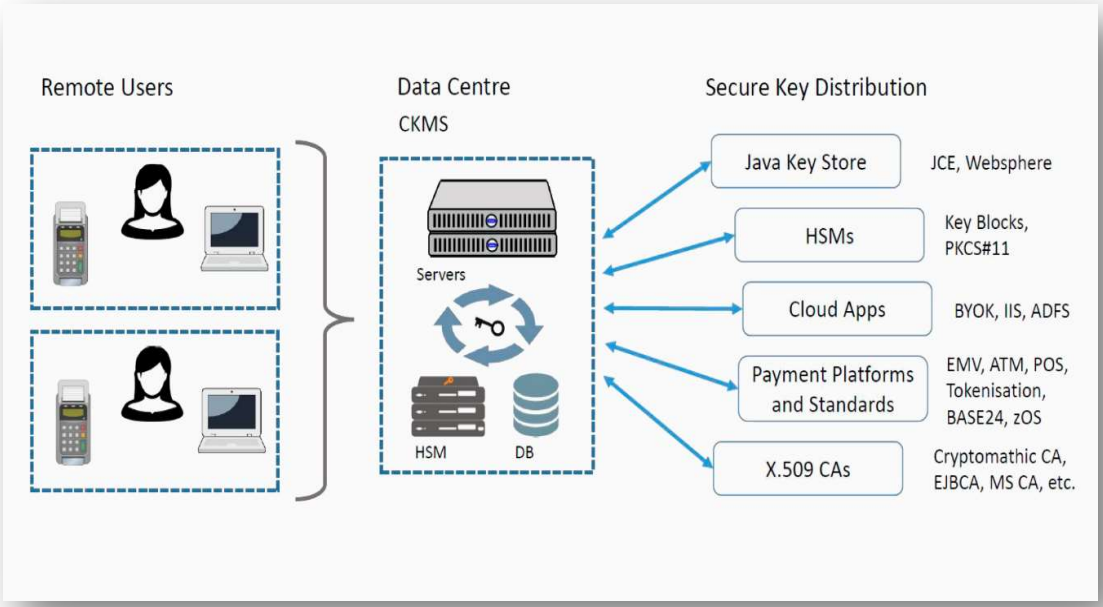


**Fig 2: Key Management Architecture**

**Source:** https://www.cryptomathic.com/news-events/blog/the-benefits-of-an-automated-and-centralized-key-management-system

The security of the symmetric encryption key is vital for ransomware developers. Furthermore, a large subset of current ransomware exclusively deploy AES for data encryption. With this in mind, Bajpai and Enbody (2020)[2] developed a side-channel attack on ransomware's key management to extract exposed ransomware keys from system memory during the encryption process. Their attack leverages the knowledge that the encryption process is a white box on the host system; this approach is successful regardless of which cryptographic API is being used by the malware and regardless of whether a cryptographic API is being used by the malware at all. Their attack was able to identify exposed AES keys in ransomware process memory with a 100% success rate in preliminary experiments, including against NotPetya, WannaCry, LockCrypt, CryptoRoger, and AutoIT samples.

### User Awareness

Chung (2019) [3] looked at preventing ransomware attacks within companies and organizations, arguing that they should help individual employees take precautions against ransomware scams. This is especially important since, as mentioned previously, ransomware attacks are increasingly targeting institutions such as financial or healthcare organizations. The author listed five prevention tips for employees to follow: install antivirus or anti-malware software on every computer and mobile device in use; choose strong and unique passwords for personal and work accounts; regularly back up files to an external hard drive; never open suspicious email attachments; and use mirror shielding technology such as NeuShield as a failsafe data protection measure.

Thomas (2018) also examined how users and employees within organizations can avoid ransomware attacks, but this paper focused on how individuals can avoid falling for phishing attacks, which are a common first step for ransomware. The author surveyed several security professionals and, based on the findings from the survey, proposed several recommendations. The first recommendation was to segment company employees based on factors such as their familiarity with phishing and the impact level of their jobs.

After segmentation, the next recommendation was to develop targeted training for each group; this training should include real-life examples highlighting the seriousness and damage caused by phishing, use real case studies, and include actual incidents within the company. Sharing these actual and personal examples will result in a strong realization of the dangerous impact of spear phishing and will evoke a more personal protection response.

## 3. RESEARCH GAPS/FINDINGS

Based on the related literature, one can make some observations on the current trends and limitations of ransomware security countermeasure solutions. Preventative techniques such as access control and key or data backups can reduce the damage that ransomware can inflict on systems and possibly deter future attacks. However, these prevention-based approaches suffer from several shortcomings as well. Firstly, they can have significant overhead. Access control or key backup schemes can incur significant computational costs (Wang et al., 2015)[15]. Creating data backups can cause the system to take a significant performance hit, especially under high workloads (Alshaikh et al., 2020 [1]).

## 4. IMPLICATIONS FOR PRACTICE, RESEARCH, POLICIES AND CYBER SAFETY IN AFRICA

Cyber Safety is very important because it helps mitigate cyber attacks against the CIA triad, that is Confidentiality, Integrity and Availability. African countries have been victims of cyber crime and attacks. Good Cyber practices will help the economy of the continent by investors having belief that the cyber ecosystem is resilient. Consistent practice, research and policies helps improve safety and resilient of the cyber space and this go along way to be a pacesetter in new technologies in the cybersecurity field.

## 5. CONCLUSION

In this work, ransomware prevention was explored. Prevention techniques mostly focused on access control, data and key backups, and hardware-based solutions. However, it seems that there is a trend in using machine learning based approaches to detect ransomware. In the end, I highlighted the existing research challenges and enumerated some future research directions in the field of ransomware.

## 6. RECOMMENDATION FOR POLICY AND PRACTICES

- Mock exercises should be conducted for uses by simulating ransomware attacks to verify if user awareness control is effective.
- Data backups must be made compulsory and offsite backups must be obligatory.

## 7. DIRECTION FOR FUTURE WORKS

- DeepFake Ransomware: Deepfakes are the manipulated digital representations such as images, videos where an attacker tries to mimic the real person (Güera and Delp, 2018 [5]). In the future, it could be possible for attackers to create ransomware that will automatically generate DeepFake content of a victim performing some incriminatory or intimate action which he/she never did. The victim will be asked to pay the ransom in order to avoid that content being published online. To mitigate such ransomware attacks will be challenging due to the velocity of data and the availability of numerous social media channels to spread the content.
- Remote Working Vulnerabilities: The recent COVID-19 pandemic made it mandatory for several institutions to initiate the work-from-home scenarios or implement bring your own devices (BYOD) policies (Palanisamy et al., 2020). As a result of which, several vulnerabilities (Curran, 2020) were exploited by the attackers that resulted in several ransomware attacks. In one of the reports by SkyBox Security, the ransomware attacks witnessed 72 percent growth compared to the previous years. Hence, it is one of the future research directions to look at mitigating such attacks during remote working scenarios.
- Increase in Ransomware-as-a-service (RaaS) Attacks: Ransomware as a service or RaaS is gaining popularity from the past few years. In RaaS model, an experienced attacker creates ransomware and offers that code to script kiddies or gray-hat hackers for some price (Meland, Bayoumy, Sindre, 2020[9], Puat, Rahman, 2020[12]). The script kiddies or gray-hat hackers then use that code to carry out their own attacks. The Cerber ransomware attack is one example of the RaaS model in action. With emerging technologies and an increasing number of internet users, there is a strong possibility for a surge in these types of attacks. Hence, mitigating such attacks in the future seems to be a potential research direction.

## REFERENCES


1. Alshaikh H., Nagy N.R., Hefny H. Ransomware prevention and mitigation techniques. Int J Comput Appl. 2020;177(40):31–39.
2. Bajpai P., Sood A.K., Enbody R. 2018 APWG Symposium on Electronic Crime Research (eCrime) 2018. A key-management-based taxonomy for ransomware; pp. 1–12.
3. Chung M. Why employees matter in the fight against ransomware. Computer Fraud & Security. 2019;2019(8):8–11.
4. Continella A., Guagnelli A., Zingaro G., Pasquale G.D., Barenghi A., Zanero S., Maggi F. Proceedings of the 32nd Annual Conference on Computer Security Applications. 2016. Shieldfs: a self-healing, ransomware-aware filesystem; pp. 336–347.
5. Güera D., Delp E. *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)* IEEE; 2018. Deepfake video detection using recurrent neural networks; pp. 1–6.
6. Huang J., Xu J., Xing X., Liu P., Qureshi M.K. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017. Flashguard: Leveraging intrinsic flash properties to defend against encryption ransomware; pp. 2231–2244.
7. Kim D., Lee J. Blacklist vs. whitelist-based ransomware solutions. IEEE Consum. Electron. Mag. 2020;9(3):22–28. doi: 10.1109/MCE.2019.2956192.
8. Kolodenker E., Koch W., Stringhini G., Egele M. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. 2017. Paybreak: Defense against cryptographic ransomware; pp. 599–611.
9. Meland P., Bayoumy Y., Sindre G. The ransomware-as-a-service economy within the darknet. *Computers & Security.* 2020:101762.
10. Min D., Park D., Ahn J., Walker R., Lee J., Park S., Kim Y. Amoeba: an autonomous backup and recovery ssd for ransomware attack defense. IEEE Comput. Archit. Lett. 2018;17(2):245–248.
11. Parkinson S. Use of access control to minimise ransomware impact. Network Security. 2017;2017(7):5–8.
12. Puat H., Rahman N. Ransomware as a service and public awareness. *PalArch's Journal of Archaeology of Egypt/Egyptology.* 2020;17(7):5277–5292.
13. Shaukat S., Ribeiro V. 2018 10th International Conference on Communication Systems & Networks (COMSNETS) IEEE; 2018. Ransomwall: A layered defense system against cryptographic ransomware attacks using machine learning; pp. 356–363.
14. Thomas J. Individual cyber security: empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management. 2018;12(3):1–23.
15. Wang Z., Huang D., Zhu Y., Li B., Chung C. Efficient attribute-based comparable data access control. *IEEE Trans. Comput.* 2015;64(12):3430–3443.
16. Buyer's Guide to Choosing a Crypto Key Management System - Part 1: What is a key management system (2018), by Rob Stubbs
17. Buyer's Guide to Choosing a Crypto Key Management System; Part 2: The Requirement for a Key Management System (2018), by Rob Stubbs
18. Buyer's Guide to Choosing a Crypto Key Management System - Part 3: Choosing the Right Key Management System (2018), by Rob Stubbs

19. NIST SP800-57 Part 1 Revision 4: A Recommendation for Key Management (2016) by Elaine Barker
20. Selected articles on Key Management (2012-today) by Ashiq JA, Dawn M. Turner, Guillaume Forget, James H. Reinholm, Peter Landrock, Peter Smirnoff, Rob Stubbs, Stefan Hansen and more
21. CKMS Product Sheet (2016), by Cryptomathic