BOOK CHAPTER | Egungun Be Careful

"Egungun Be Careful Na Express You Dey Go" A Technical Treatise on the Mitigation of Malware for Semi-Technical Users

Asani, Emmanuel O.[1], Odumesi, John O.[2], Oshodi, Akinwale D.[3] & Longe, O. Babatope[4]
[1]Department of Computer Science, Landmark University, Nigeria.
[2]Department of Computer Science, University of Abuja, Nigeria
[3]Centre for Systems and Information Services, Landmark University, Nigeria
[4]Faculty of Computational Sciences & Informatics, Academic City University College, Accra, Ghana
E-mails:[1] asani.emmanuel@lmu.edu.ng; [2]olayemijohn@yahoo.com [3]oshodi.akinwale@lmu.edu.ng [4]olumide.longe@acity.edu.gh
Phones: [1]+2347036103001; [2]+2348185772205; [3]2348055363556; [4]+233595479930

ABSTRACT

We present a semi-technical approach to mitigating the malware menace. Our approach is two-pronged vis-à-vis detection and prevention. We present existing state-of-the-art detection techniques as well as some readily available malware analysis tools for semi-technical users. We concluded by providing suggestions on malware prevention best practices.

Keywords: Semi-Technical Users, Malware, Cybercrime, Mitigation, Treatise, Egungun, Security

1. INTRODUCTION

The colloquial repertoire by the popular Nigerian genre musician, Abass Akande Obesere titled "*Egungun be careful na express you dey go*" is a philosophical rendition, originally addressed to philanderers but recently recontextualized and made popular by social media cliché on the need for caution in undertaking any given endeavor (Inya, 2021). Given the bi-polar tendency of the internet technology to offer limitless potential for profiting to internet users on the one hand, while exposing them to danger on the other hand, the cliché may be adopted as a caution to internet users, majority of whom are non-technical, and are thus easy targets for cybercrimes. Attackers take advantage of the internet's ubiquity and reach to perpetrate far-reaching attacks on users, exploiting vulnerabilities, ignorance and trust. These attacks have devastating consequences on individuals, businesses and national security (Asani *et al.,* 2021). Malware is the principal medium for the propagation of malicious intents in the cyberspace, perpetrated either by taking advantage of existing vulnerabilities, exploiting the naivety of non-technical users or utilization of unique characteristics of emerging technologies (Jang-Jaccard & Nepal, 2014).

Citation: Asani, E.O., Odumesi, O.J., Oshodi, A.D. & Longe, O.B. (2022). "Egungun Be Careful Na Express You Dey Go": A Technical Treatise On The Mitigation Of Malware For Semi-Technical Users. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

Malware is a broad term for malicious lines of code, injected into an information system with the intent of causing harm to that system or other systems, or subverting them for purposes other than those intended by their creators (Aru & Chiaghana, 2018). Viruses, worms, trojan horses, backdoors, keystroke loggers, rootkits, and spyware are all terms used to characterize different forms of malware; malwares can gain remote access to a system and send data from that system to a third party without the user's consent or knowledge, hide the fact that the system has been compromised, disable security measures, damage the system, or otherwise compromise data and system integrity. (Aslan & Samet, 2020).

This paper presents how malwares exploit vulnerabilities, an outline of some state-of-the-art detection techniques and tools which may help semi-technical users avoid falling victims of this menace.

2. HOW MALWARES WORK: VECTORS AND ATTACK DIMENSIONS

Malware is represented by different variants of malicious software, identified by their unique attributes which include their attack vector (method of propagation) and their attack dimension (how they infect systems). Some popular malware variations include viruses, worms, Trojan, adware, spyware, ransomware, botnets, rootkits and so on (Roseline & Geetha, 2021). While these attacks manifest in different dimensions, they all typically pass through four generic phases, namely Infection, Latency, Replication and Propagation, and attack (Sortino, 2021). The Malware life phase is depicted in Figure 1.

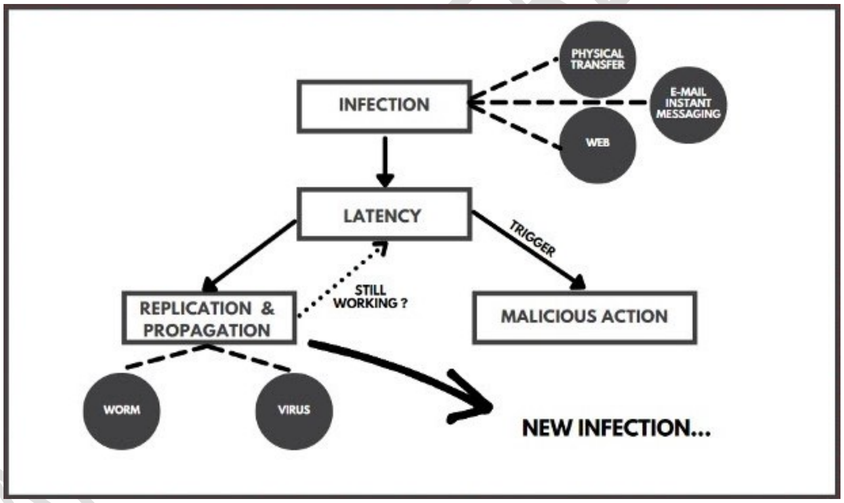

Fig 1. Malware Life Phase (Sortino, 2021)

The Infection phase is the entry stage. The malware gets into or is injected to the target system. The malware may be appended to a legitimate software or the attackers may compromise the target terminal via different attack vectors. Some attack vectors in literature are summarized as follows (Qamar *et al.,* 2019; Krishnan, 2020; Roseline & Geetha, 2021).

Baiting: in order to breach a target terminal, users may be lured into compromising the system. For instance, a branded but malware infected flash drive may be placed conspicuously to attract the unsuspecting user into picking it and inserting it into the company system out of curiosity. Users may equally be baited using ads and games into clicking links or accessing malicious sites. The authors of Stuxnet worm (unofficially believed to be the Isreali government) used baiting to devastating effect in destroying the Iranian Nuclear plant SCADA system.

Social Engineering: an attacker may equally exploit the users' mental and emotional vulnerability through social engineering medium such as phishing email, pharming and so on. Users expose their system to attack by clicking infected urls embedded in a phishing email.

Insider attack: A network may also be breached by physically infiltrating the system through a compromised insider/agent. An insider can physically insert an infected drive or install malware on a network system. Other methods used by attackers to infect target systems include Downloadable free software/plug-ins/games, Networked File sharing program/infected system, P2P file sharing networks. The malware may remain at sleep until it is triggered by a preset condition, which may be time or activity/operation of the host system. Replication and propagation then take place while the attack is being executed on the infected network. Table 1 outlines some popular malware variants, their description and some real-life attacks.

Table 1. Malware variants, description and cases

S/N	Malware Variants	Description	Cases
1.	Virus	- appends itself to a computing resource, multiply spreads across other resources on the network. - Aims to alter data, damage its host and cause denial of service. - (La Polla *et al.,* 2013; Roseline & Geetha, 2021; Sotino, 2021)	Shamoon appends itself to the target system resources via phishing email and encrypts it. Once in the target system, it is triggered by a preset time.
2	Worms	- Malicious self-contained, self-propagating program. - can infect its target by a software flaw or be delivered through phishing or smishing. - Embedded worms can change and remove data, inject more malicious software, and replicate in the target system until it runs out of resources. - (Roseline & Geetha, 2021; Sotino, 2021)	In 2010, Stuxnet infiltrated the Iranian SCADA system through a drive, took control of the centrifuges and ran them to self-destruct. Stuxnet is the first known nation-state weaponized malware For more on stuxnet see: John Byrd's answer to What is the most sophisticated piece of software ever written? - Quora
3	Trojan	- Looks legitimate/useful but loaded with malicious codes. - May be spread using social engineering methods like phishing and bait websites. - (Roseline & Geetha, 2021; Sotino 2021)	The Zeus malware attacks in 2007 spread chiefly through phishing and file downloads from the Internet. Zbots can infect legitimate and trustworthy websites with the trojan allowing unsuspecting internet users to download the infected files.
4.	Keylogger	- Keylogger is a rootkit variant that records keystrokes covertly for the purpose of monitoring and information theft. - (Qamar *et al.,* 2019; Sotino, 2021)	Flexispy, Olympic dreams

S/N	Malware Variants	- Description	Cases
5.	Spyware	- This is a type of malicious software that infects a computer or other device and collects data about a user's online activities without their knowledge or agreement. - (Roseline & Geetha, 2021)	DarkHotel is a spyware suspected to be sponsored by the south-korean government and was used to perpetrate attacks on specific targets, chiefly agents of the US government. It infiltrated its target by infecting a hotel's WiFi network and baited users through software updates. During the update, the malware is able to crawl into the target system and install keylogging codes through which it is able to record data from users' keystrokes, gain persistence to contact the infected machine in the future, collect data from the computer users' hard drives, detect and erase any traces of its presence when the attack is successful.
6.	Adware	- A spyware variant that monitors user's web usage data. - Attackers sell the data to companies who in turn use it to guide their advertisement. - Not harmful but negatively affects user experience. - (Roseline & Geetha, 2021)	Wajam was perpetrated by Wajam Internet Technologies Inc. product. It infects browser and crawl valuable usage data from users
7.	Ransomware	- Malware variant gains access and control of the victims's system through phishing, and by exploiting vulnerabilities, as well as configuration loopholes. - The attackers then encrypt the victims' data until a specified ransom is paid - (Roseline & Geetha, 2021)	WannaCry in 2017: This is the worst ransomware attack in history launched via phishing emails in 2017. The threat exploits a vulnerability in the Windows environment. It is estimated that more than 200,000 people were affected. The losses caused by WannaCry exceeded $4 billion.
8.	Botnets	- Operated by a botmaster - A network of bots which helps an attacker infiltrate target systems and gain unauthorized remote control - Can be used to launch DDoS attacks - (Qamar *et al.,* 2019)	The Mirai botnet was responsible for a huge distributed denial of service (DDoS) in 2016. It targets and infects IoTs which it in turn, turns to a remotely controlled bot, which was used to perpetrate coordinated attacks.

S/N	Malware Variants	Description	Cases
9.	Rootkits	- Helps the attacker remotely infiltrate and gain administrator-level control of its target. - Made up of a dropper, loader and rootkit - usually transmitted via a Trojan. - Runs at startup and difficult to detect - (Qamar *et al.,* 2019; Roseline & Geetha, 2021; Sotino, 2021)	Tornkit and Hummingbad
10.	Fileless Malware	- This variant of malware does not need to install itself before infiltrating the target. - It exploits and modifies native system resources in the system's operating system. - It is thus difficult to detect.	Astaroth
11.	Keylogger	- Keylogger is a rootkit variant that records keystrokes covertly for the purpose of monitoring and information theft. - (Qamar *et al.,* 2019; Sotino, 2021)	Flexispy, Olympic dreams

3. MALWARE MITIGATION

Malware attacks may be mitigated either by adopting a precautionary approach or by deploying existing malware detections tools.

Malware Detection Approaches

Malware have been detected in literature using two major approaches viz static techniques and dynamic techniques. A hybrid of the two approaches has also been proposed and implemented.

Static Malware Detection Techniques

Otherwise referred to as signature-based technique, it investigates the existence of malicious features such as abnormal latency and resource usage, hashes, malicious strings, signature and metadata (Roseline & Geetha, 2021). The investigation is done based on existing knowledge base and makes no provision for zero-day attack. This is the techniques of choice by many antivirus software, and this is why periodic updates is a necessity, for users. Having identified malicious attributes, the malware is the extracted using techniques such as rule-based pattern matching, automatic signature generation method and kernel-based data object mapping method (Shabtai *et al.,* 2011; Rhee *et al.,* 2014; Qamar, *et al.,* 2019).

A manual semi-technical user approach may be to perform a search of the computer's ***task manager*** to check for strange app name, duplicate app presence often due to attackers' tendencies to rename malwares after existing software to avoid detection, and abnormal memory and resource usage. Recent works such as (Shabtai *et al.,* 2011; Rhee *et al.,* 2014; Yerima *et al.,* 2014; Anderson &Roth, 2018; Qi *et al.,* 2021; Ma *et al.,* 2022) were able to detect malware with considerably high accuracy using static technique.

Dynamic Technique

Also known as behavioral techniques, this method is able to identify malicious codes by investigating malware samples at run-time with a view to analyzing and identifying its behavioral features (Saracino *et al.,* 2018). This is often done in safe mode or on a virtual machine and it is resource intensive. A machine learning algorithm may then be trained to automatically apprehend it and its variants (Qamar, *et al.,* 2019; Roseline & Geetha, 2021). Recent works such as (Karim *et al.,* 2016; Saracino *et al.,* 2018; Amer & Zelinka, 2020; García & DeCastro-García, 2021; Jing *et al.,* 2021) were able to detect malware with considerably high accuracy using dynamic technique

4. USEFUL MALWARE ANALYSIS TOOLS

We present some malware analysis tools that can be easily sourced online and can form part of a powerful malware hunting toolkit for semi-technical users.

Process Hacker

Allows users to view the processes being executed on the system and where. It is able to track the activities of a malware, particularly as it tries to obfuscate users by replicating and renaming itself as a harmless software. It can be used to analyse the memory of the software and extract strings such as IP address, creator, that may give insight as to whether it is malicious or not. analyst to see what processes are running on a device.

ProcMon was developed by Microsoft to monitor filesystem, Registry and process/thread activities. The filtering feature allow users to track events such as process creation, its source, its thread stacks/dependencies, and details such as image path, command line, user, session ID and so on. It has been used successfully to track and apprehend the popular banking trojan, known as *emotet*.

Autoruns is a Microsoft utility that highlights programs scheduled to launch at start up, login, or after a trigger such as the launching of an in-built application. It is able to detect and highlight suspect applications with in-built or registry created persistence mechanisms.

Fiddler acts as a web proxy for HTTP/HTTPS traffic, it captures and reports traffic highlighting attempts by malicious codes or file to download harmful payloads.

Cuckoo Sandbox is an automated malware analysis tool. It can analyse suspicious files by simulating its execution and give detailed report on its behavior during execution.
Other useful tools include wireshark for network traffic analysis, x64dbg, Ghidra, Radare2/Cutter, REMnux, Google Rapid Response (GRR) and so on.

5. MALWARE PROTECTION BEST PRACTICES FOR SEMI-TECHNICAL USERS

Here are some best practices to consider when implementing malware protection:

- Adopt a zero-trust security policy: all access requests, whether coming from outside or inside the network, must be verified for trustworthiness before they can gain access to a system. The goal is to secure access by end-user devices, users, Application Programming Interfaces (APIs), microservices, Internet of Things (IoT), and all of which may be compromised by attackers.
- Verify the source of an application before installing: it is best to download digitally signed software from official site only
- Leverage email security: the majority of ransomware infections are spread via malicious downloads or email attachments. Implement a layered security approach, including a secure email solution, a company-sanctioned file-sharing solution, and endpoint protection on user devices.

- Regularly back up data and test restore procedures: backup is a critical practice that can help to protect against data loss. It can help ensure that normal operations can be maintained even if the organization is attacked by network-based ransomware worms or other destructive cyber-attacks.
- Strong passwords and regular software updates: ensure all users create strong, unique passwords, and regularly change passwords. Update your systems as quickly, as security flaws become known and patches are released.

6. CONCLUSION

This article is targeted at semi-technical users, who usually fall victim of malware either as individual or as the weak link within an organization. This paper presents detection and preventions as two-pronged approach towards malware mitigation.

REFERENCES

1. Amer E. & Zelinka I., (2020). A dynamic Windows malware detection and prediction method based on contextual understanding of API call sequence. *Computer & Security, 92.* https://doi.org/10.1016/j.cose.2020.101760
2. Anderson, H., & Roth, P. (2018). EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models. *ArXiv, abs/1804.04637*.
3. Aru O.E. & Chiaghana C.E., (2018). Malware Analysis and Mitigation in Information Preservation. *IOSR Journal of Computer Engineering 20(4)*, 53-62. DOI: 10.9790/0661-2004015362
4. Asani E.O., Omotosho A., Danquah P.A., Ayoola J.A. Ayegba P.O. & Longe O.B. (2021). A maximum entropy classification scheme for phishing detection using parsimonious features. *TELKOMNIKA Telecommunication, Computing, Electronics and Control, 19(5)*, 1707-1714. DOI: 10.12928/TELKOMNIKA.v19i5.15981
5. Aslan Ö. & Samet R., (2020). A Comprehensive Review on Malware Detection Approaches. *IEEE Access 8,* 6249-6271. DOI: 10.1109/ACCESS.2019.2963724
6. García D.E. & DeCastro-García N., (2021). Optimal feature configuration for dynamic malware detection. *Computer & Security, 105.* https://doi.org/10.1016/j.cose.2021.102250
7. Inya O. (2021). "Egungun be careful, na Express you dey go": Socialising a newcomer-celebrity and co-constructing relational connection on Twitter Nigeria. *Journal of Pragmatics, 184,* 140-151. https://doi.org/10.1016/j.pragma.2021.08.005
8. Jang-Jaccard, J & Nepal, S (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80(5)*, 973-993. https://doi.org/10.1016/j.jcss.2014.02.005
9. Jing C., Wu Y. & Cui C. (2021). Ensemble dynamic behavior detection method for adversarial malware. *Future Generation Computer Systems 130*, 193-206
10. Karim A., Salleh R. & Khan M.K. (2016). SMARTbot: A Behavioral Analysis Framework Augmented with Machine Learning to Identify Mobile Botnet Applications. *PLoS ONE, 11(3).* https://doi.org/10.1371/journal.pone.0150077
11. Krishnan, S. (2020). Exploitation of Human Trust, Curiosity and Ignorance by Malware. *ArXiv, abs/2002.11805*.
12. La Polla M., Martinelli F. & Sgandurra D. (2013). A survey on security for mobile devices. *IEEE Commun. Surv. Tutor. 15(1)* 446–471.
13. Ma Y-W., Chen J-L., Kuo W-H. & Chen Y-C., (2022). AI@nti-Malware: An intelligent framework for defending against malware attacks. *Journal of Information Security and Applications 65*. https://doi.org/10.1016/j.jisa.2021.103092
14. Qamar A., Karim A. & Chang V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems 97*, 887-909. https://doi.org/10.1016/j.future.2019.03.007

15. Qi, P., Wang, W., Zhu, L., & Ng, S. (2021). Unsupervised Domain Adaptation for Static Malware Detection based on Gradient Boosting Trees. *Proceedings of the 30th ACM International Conference on Information & Knowledge Management*, 1457–1466. https://doi.org/10.1145/3459637.3482400
16. Rhee J., Riley R., Lin Z., Jiang X. & Xu D. (2014). Data-centric OS kernel malware characterization *IEEE Trans Inf Forensics Secur, 9,* 72-87. 10.1109/TIFS.2013.2291964
17. Roseline S.A. & Geetha S., (2021). A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks. *Computers and Electrical Engineering 92*. https://doi.org/10.1016/j.compeleceng.2021.107143
18. Saracino A., Sgandurra D., Dini D. & Martinelli F. (2018). MADAM: effective and efficient behavior-based android malware detection and prevention. *IEEE Trans Dependable Secur Comput 15(1),* 83–97.
19. Shabtai A., Menahem E. & Elovici Y. (2011). F-sign: automatic, function-based signature generation for malware. *IEEE Trans Syst Man Cybern Part C (Applications and Reviews), 41(4*), pp. 494-508, DOI: 10.1109/TSMCC.2010.2068544.
20. Sortino, (2021). *A Malware's Life*. Retrieved 22/01/2022. https://systemweakness.com/a-malwares-life-8a0c3770e57

APPENDIX: Web resources

21. 11 Best Malware Analysis Tools and Their Features | Varonis Retrieved January 9th, 2022 from https://www.varonis.com/blog/malware-analysis-tools
22. Baker, K (2021). The 11 Most Common Types of Malware. Retrieved January 9th, 2022 from https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/
23. Berr, J (2017). "WannaCry" ransomware attack losses could reach $4 billion. Retrieved January 7th, 2022 from https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/
24. Dossett, J (2021). A timeline of the biggest ransomware attacks. Retrieved January 6th, 2022 from https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/
25. Halliday, J (2010). Stuxnet worm is the 'work of a national government agency'. Retrieved January 7th, 2022 from https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency
26. INTERPOL (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19. Retrieved January 7th, 2022 from https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
27. The 11 Most Common Types of Malware. Retrieved January 9th, 2022 from https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/