A Baseline of Malware Infections and Anti-Malware Deployment in Ghanaian Government Ministries

[1]Paul Danquah, [2]John Amoako Kani & [3]Jojo Desmond Lartey
[1,2&3] Department of Information Technology
Heritage Christian University College
Ghana, West Africa
E-mail: pauldanquah@yahoo.com

ABSTRACT

An established fact is the increasing growth in malware incidents and anti-malware deployment worldwide, it is believed Ghana is no exception given the relatively little research done on the Ghanaian context. This research focused on determining the extent of malware infections and anti-malware deployments in the Ghanaian government with specific emphasis on the government ministries. The approach was sequential exploratory with subsequent simultaneous triangulation of qualitative and quantitative data. The results obtained and analysis of the results show that within the context of malware baselining, viruses are the most common malware infections and that accounted for over fifty percent of downtime experienced by users. Third party mobile devices, laptops and computers tend to be the most infected systems within the Ghanaian government ministries and the most challenging threat that has not been properly countered is the advanced persistent threat even though most threats are identified and addressed within a week of infection. In the anti-malware setting, the rate of effectiveness of the current anti-malware protection is predominantly above average or average at minimum given their primary objective of efficacy as the basis for purchase.

Keywords: Malware, Anti-Malware, Ghana Government Ministries, Baseline

iSTEAMS Multidisciplinary Conference Proceedings Reference Format
Paul Danquah, John Amoako Kani & Jojo Desmond Lartey (2019): A Baseline of Malware Infections and Anti-Malware Deployment in Ghanaian Government Ministries. Proceedings of the 20th iSTEAMS Multidisciplinary Trans-Atlantic Conference, KEAN University, New Jersey, United States of America. 10th – 12th October, 2019. Pp 93-104 www.isteams.net/usa2019 - DOI Affix - https://doi.org/ 10.22624/AIMS/iSTEAMS-2019/V20N1P7

1. INTRODUCTION

As Cyber Security experts battle against malware infections and ransomware extortions, the financial losses for innocent user and corporate keep increasing. The word malware is a short form of malicious software, it is the collective name for a number of malicious software designed to cause damage to a computer, server, client or computer network (Szor, 2005). Antimalware on the other hand is a type of software program designed to prevent, detect and remove malicious software (malware) on IT systems, as well as individual computing devices (Harley, Myers & Willems, 2010). Malwares manifest in many forms including virus, trojan, worms, spyware, adware, rootkits and ransomware. Similarly, antimalware software protects against infections caused by many types of malware, including all types of viruses, as well as rootkits, ransomware, worms and spyware. Kinder, Katzenbeisser, Schallhart and Veith(2010), in their paper indicated that "malware costs more than $10 billion every year and the cost is still increasing.

Classical signature-based and emulation-based methods are becoming insufficient, since malware writers can easily obfuscate existing malware such that new variants cannot be detected by these methods". Malware infections have generally become prominent over the years, the situation in Ghana is no exception. Research statistics of malware attacks by various antimalware vendors have consistently shown growth in numbers. Typical examples are shown figures 1 and two from AV Test and Kaspersky research labs respectively.

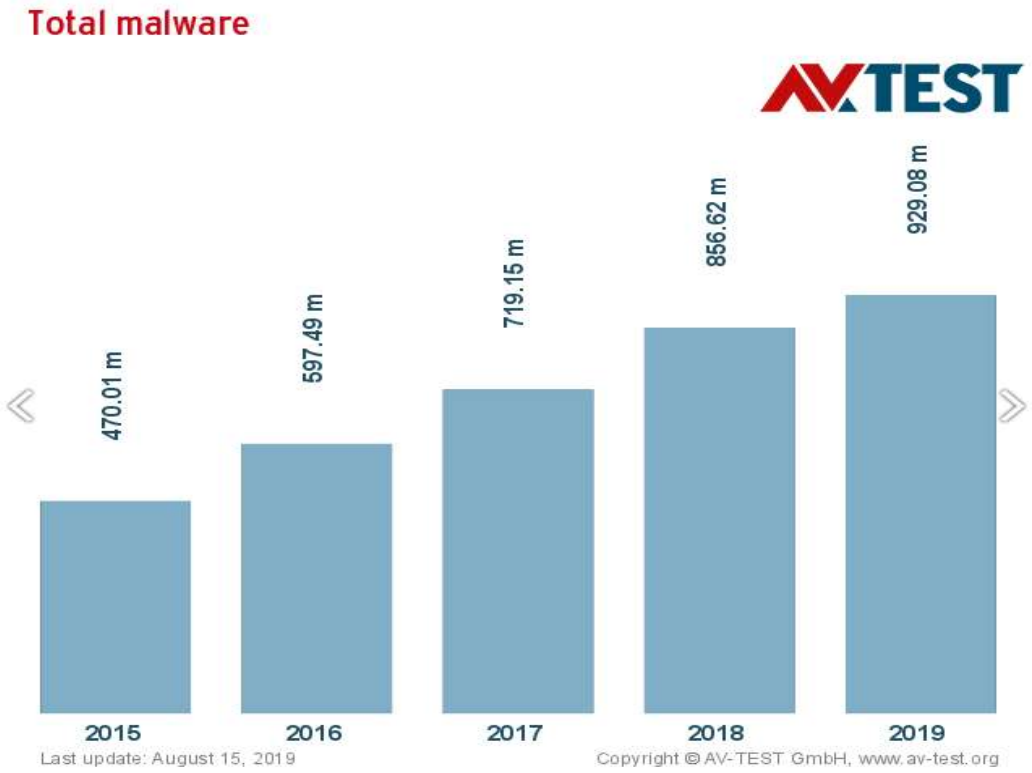

Figure 1: Total Malware over five years (2015 to 2018) period
Source: https://www.av-test.org/en/statistics/malware/

Evidently, total number of malware attacks have been on the increase as time progresses. The Ghanaian government ministries have experienced relative stability in numbers and their operations, however, there is not much published data on the malware infections status and the extent to which ant-malware deployments are made. Despite the unavailability of published information, the Ghanaian government context has seen the drafting and implementation of the National Cyber Security Policy which has 9 Pillars consisting of namely; effective governance, legislative and regulatory framework, cybersecurity and capacity building, research and development towards self-reliance, compliance and enforcement, child online protection, cybersecurity emergency readiness, and international cooperation.The seeming absence of published material on this subject matter served as a motivation for this research to inductively assess the malware and anti-malware baseline of Ghanaian government implementations with the ministries as a case study. This research therefore serves as a unique and novel contribution to the body of information security experiences in Ghana.

2. LITERATURE REVIEW

Types of Malware include; Backdoor, Botnet, Downloader, Information-stealing malware, Launcher Rootkit, Spam-sending malware, Scare-ware, Worm or virus, ransomware. Moshiri, Abdullah, Binti, Mahmood and Muda (2017), in their paper comprehensively provided a framework for analyzing malware, detecting malware, classifying malware and metrics for evaluating and comparing their performance. Different types of malware have gained popularity at different times, specific malware has also gained prominence sporadically. The most commonly used terminology for malware has been virus, however virus is essentially one type of malware. "The malware landscape has grown in parallel with software and emerging technology, adapting new techniques and strategies from industry into their design paradigms and targeting new platforms as they present lucrative opportunity for attackers" (Homeland Security, 2016). It has become necessary that administrators across all industries protect their devices from malware attacks, focusing their efforts on keeping device OSs and security software up to date and hardening their infrastructure against open vectors of attack. According to (Sikorski and Honig, 2012), there are two fundamental approaches to malware analysis: static and dynamic. Static analysis involves examining the malware without running it. Dynamic analysis involves running the malware.

Emphasis has also been laid on the prominence being gained by specifically ransomware, "ransomware continues to be one of the most crucial cyber threats and is actively threatening IT users around the world. In recent years, it has become a phenomenon and traumatic threat to individuals, governments and organizations" (Zakaria, Abdollah, Mohd and Ariffin, 2017). It therefore implies that ransomwares not only disrupts computational operations but it is also used to extort huge amount of money from the victims if the victims want to regain back access to the system and files. Inadvertently, cybercriminals tend to make millions of profits and keep on spreading new variants of ransomware (Zakaria et al, 2017). On the other hand, "zero-day malware is a major problem as long as these specimens are a serious cyber threat. Most of the efforts are focused on designing efficient algorithms and methodologies to detect this type of malware; unfortunately models to simulate its behavior are not well studied" (Rey, Dios, Hernández and Tabernero, 2020).

Given the evidence provided from published work, there are quite obvious that concerns about the different types of malware and challenges being faced by anti-malware vendors in addressing them. Consequently, proposals have also been made to address the issues. (Preda, Christodorescu, Jha and Debray, 2007), in their proposed solution suggested an approach that uses a trace semantics to characterize the behaviors of malware as well as the program being checked for infection, and uses abstract interpretation to "hide" irrelevant aspects of these behavior . Tiwari & Shukla (2018), in their paper also proposed a method to detect android malware using permissions and API by generating two types of feature vector named as common and combined feature vector. The approach for malware detection has generally been extended to using behavioural based approaches as opposed to signature base approaches. A practical example is the proposal by (Huda, Abawajy, Al-Rubaie, Pan and Hassan, 2019) in response to the signature based detection challenges of malware introduced intelligent models and algorithms that can extract behavioural features and inherent attack patterns from the existing malware data, it was design to further integrate the behavioural indicators into the detection system

Various independent vendor neutral organizations have also attempted to assess and rank anti-malware solutions based on varying metrics. These metrics range from management, client performance, efficacy, preventive capability and many other metrics. It is essential to not that these rankings are periodically done hence do not necessarily depict a picture that is perennial.

Baselining represents a snapshot of the capability of a setup at some point in time. The capability of a process is essentially the range of outcomes that can be expected if a process is followed. If baselines are regularly established, trends in the process capability can be more easily obtained. The ISO27001 standards is an evaluation scheme of information security operational system. The ISO27001's Information Security Management System (ISMS) has a Capability Maturity Model (CMM) for assessing an organization's ability to establish, implement, maintain and continually improve information security management system.

Proença & Borbinha (2018) provide the ISO27001's ISMS CMM guide as shown below;
"Level 1: Initial No Criteria
Level 2: Planning
Level 3: Implementation
Level 4: Monitoring
Level 5: Improvement"

The efficient management of malware and deployment of ant-malware is no exception. A basis for placing a whole government ministries on the CMM as a baseline is an evident gap in knowledge, this study therefore might not be able to ultimately place the Ghanaian government ministries sector at a specific stage of the ISMS CMM as a baseline but should be capable of provide indicative existing situations.

3. METHODOLOGY

The approach used in this research was a sequential exploratory design, the focus was on qualitatively collecting data first via preliminary interviews, and this was then followed by the collection and analysis of quantitative data. The reason for this approach was to use the initial findings to develop the survey instrument to administer to a larger sample. Beyond this was the simultaneous triangulation where more qualitative and quantitative data are collected concurrently and analyzed separately and then compared. This method was used to confirm and cross-validate findings. A mixed method approach was used, in this context, the data collection, data analysis and interpretation of the evidence was purposefully done. The essential purpose was to provide a broader view of the research setting, thus viewing the phenomena from different perspectives. The respondents were predominantly heads of the IT department or heads of divisions responsible for IT operations. The principal objective of the mixed approach was to ensure the approach leveraged on complementary strengths of quantitative and qualitative methods without any coinciding weaknesses. To ensure the validity of research though, a combination of the sequential exploratory design and concurrent triangulation design was adopted. Quantitative data is dominant in the final analysis due to the volume comparatively obtained from the subjects.

The total number of ministries are 34, 28 ministries were served with the survey instrument and 25 responded, thus constituting 74% of the population. An initial 5 ministries were served and interviewed at the exploratory stage to deduce the essential malware infections situation and the mode and extent of anti-malware deployment for the Ghanaian government ministries. Further to the interviews, a survey instrument was designed to collect data on the same subject matter. Specifically, the survey instrument was served to 28 of the population size and responses were obtained from 25. A total of 9 were successfully interviewed for in-depth information on the situation.

4. RESULTS AND ANALYSIS

Survey Responses:

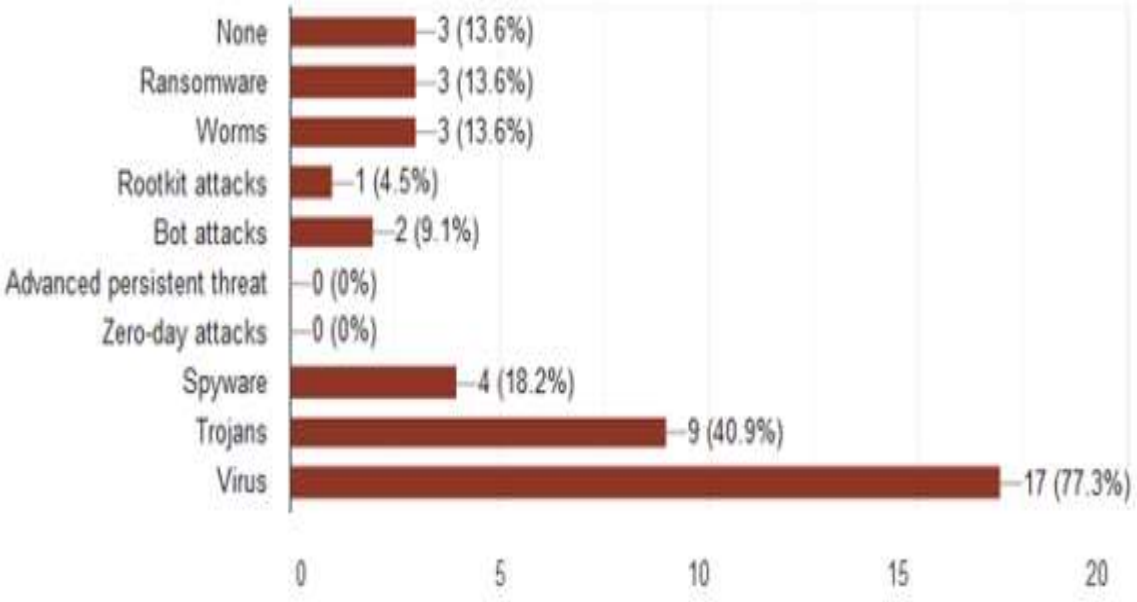

Figure 2: Responses to Question; In the past year, what type of malware incidents has your organization experienced? (select all that apply)

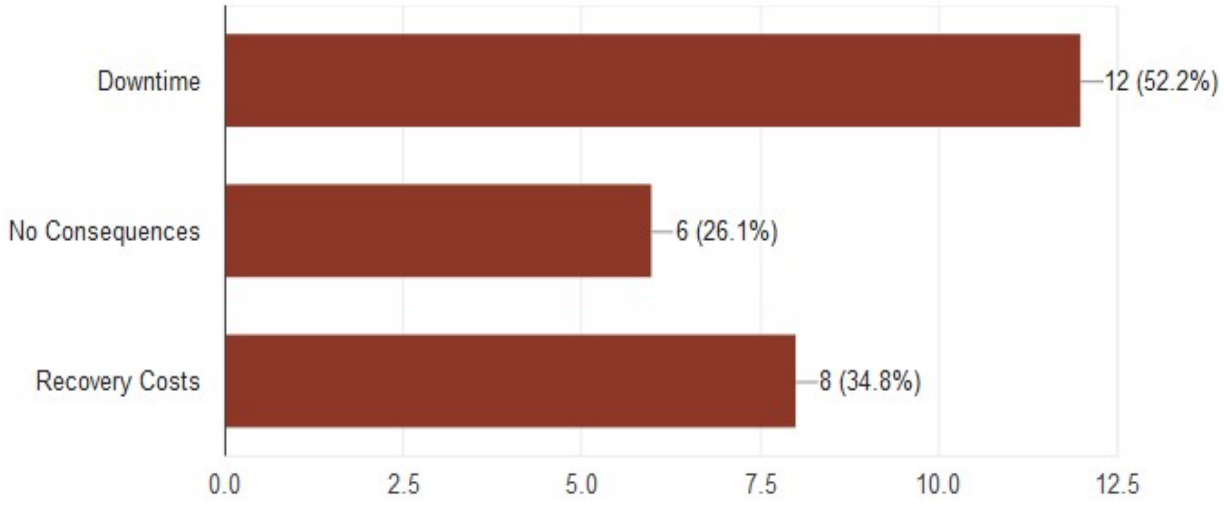

Figure 3: Responses to Question; What consequences did your organization experience as a result of these incidents? (select all that apply)

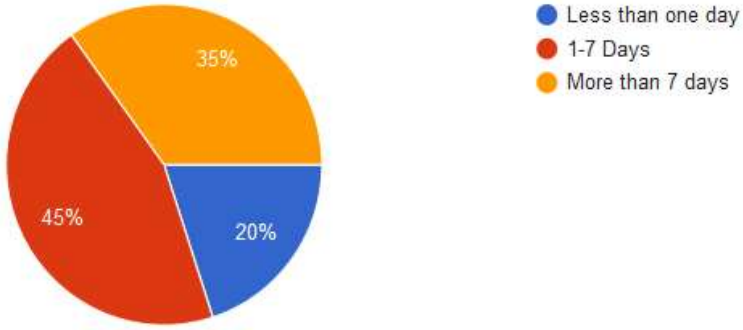

Figure 4: How long malware infections went undetected

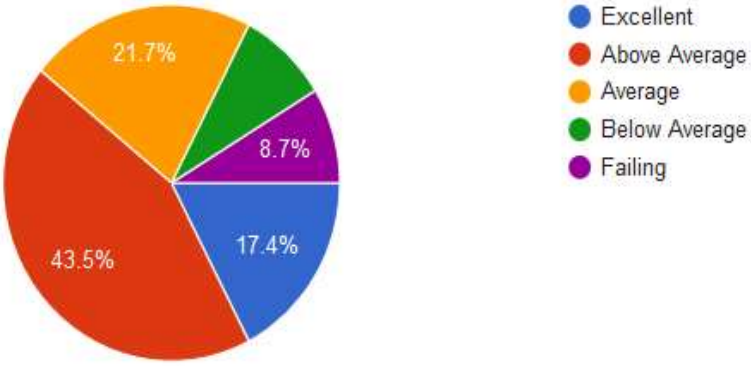

Figure 5: Effectiveness of Anti-Malware in use

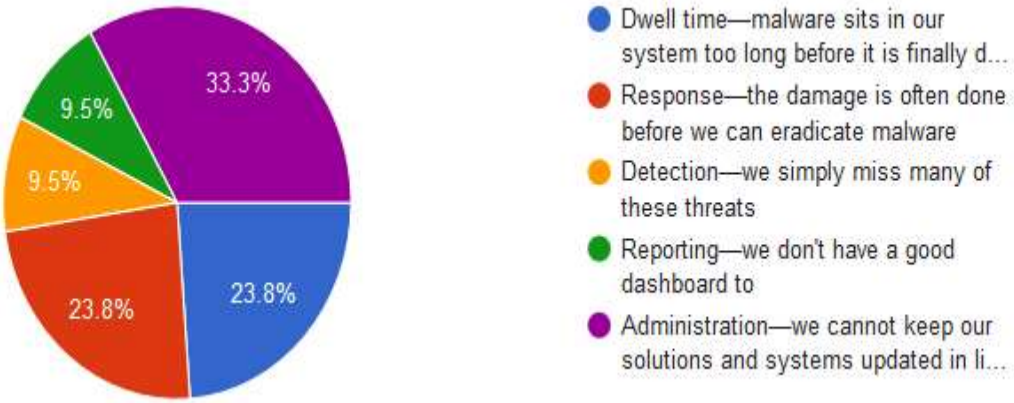

Figure 6: Perceived biggest failing of currently used anti-malware

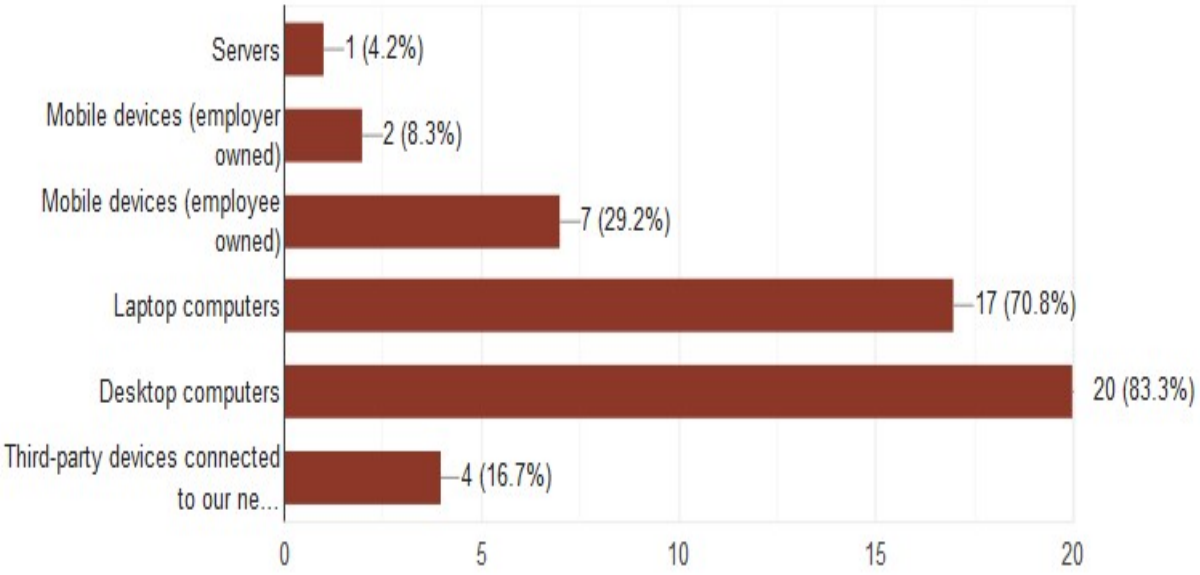

Figure 7: Most vulnerable endpoints in use

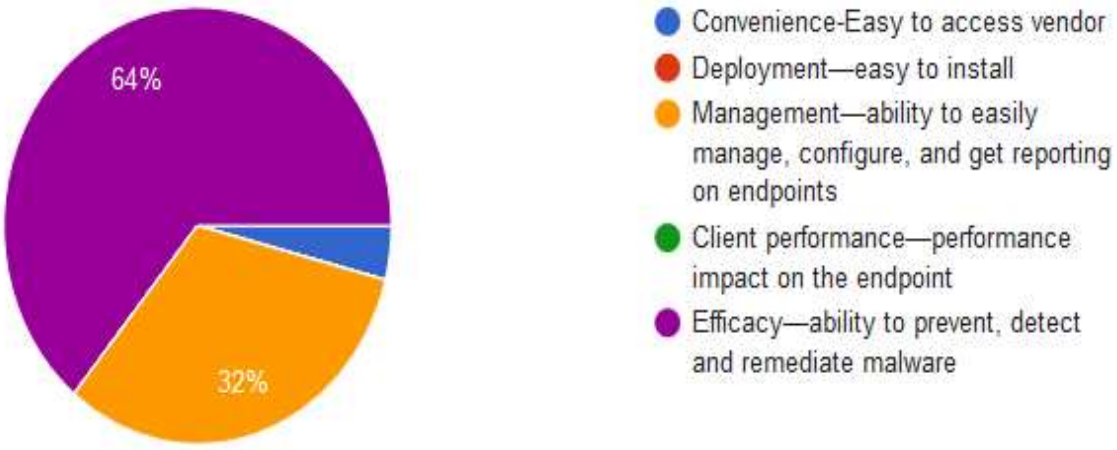

Figure 8: Most important consideration in purchase of anti-malware

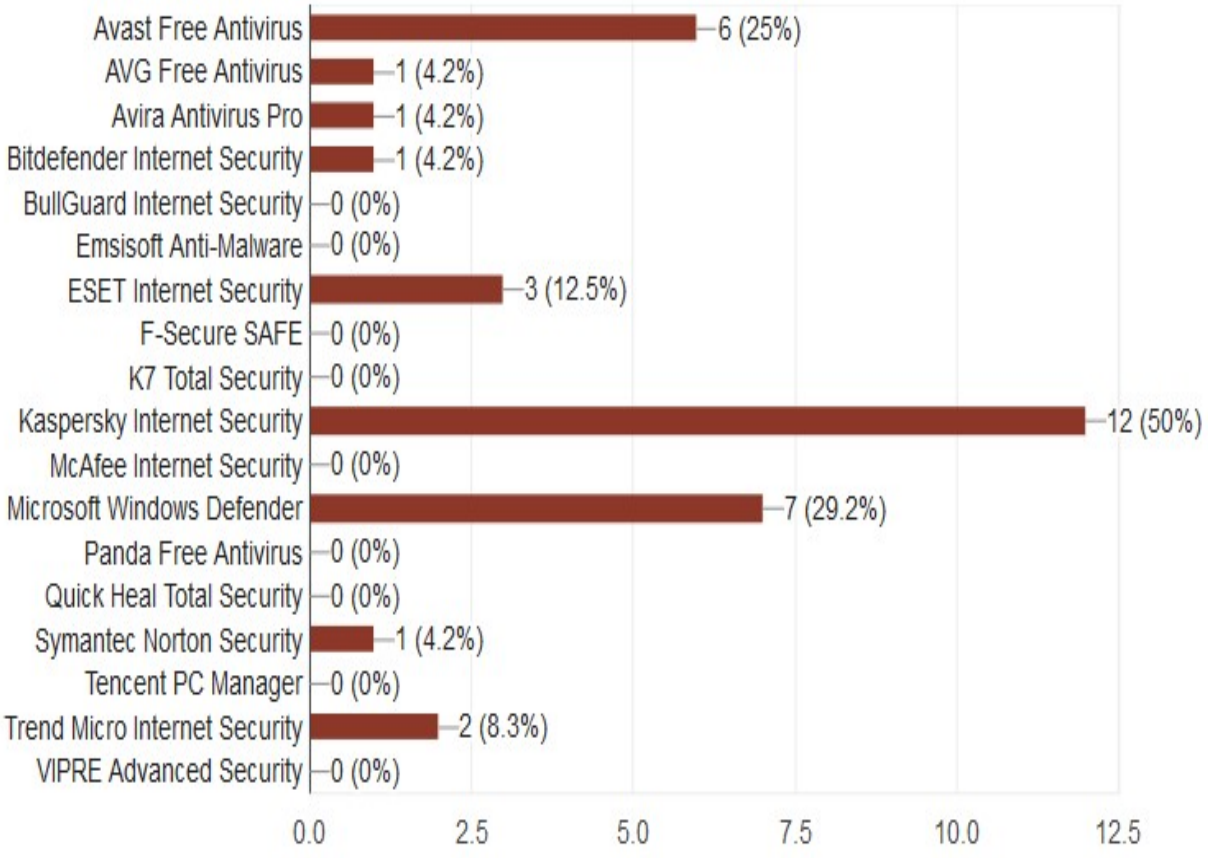

Figure 9: Vendors of endpoints in use

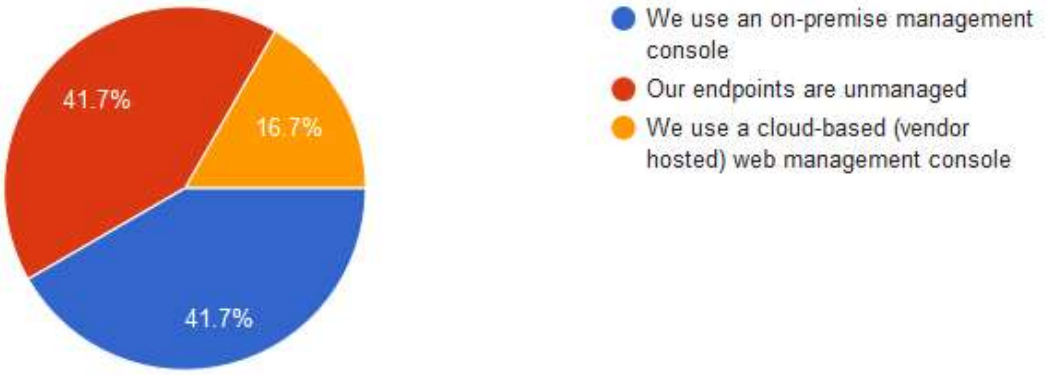

Figure 10: Mode of Deployment

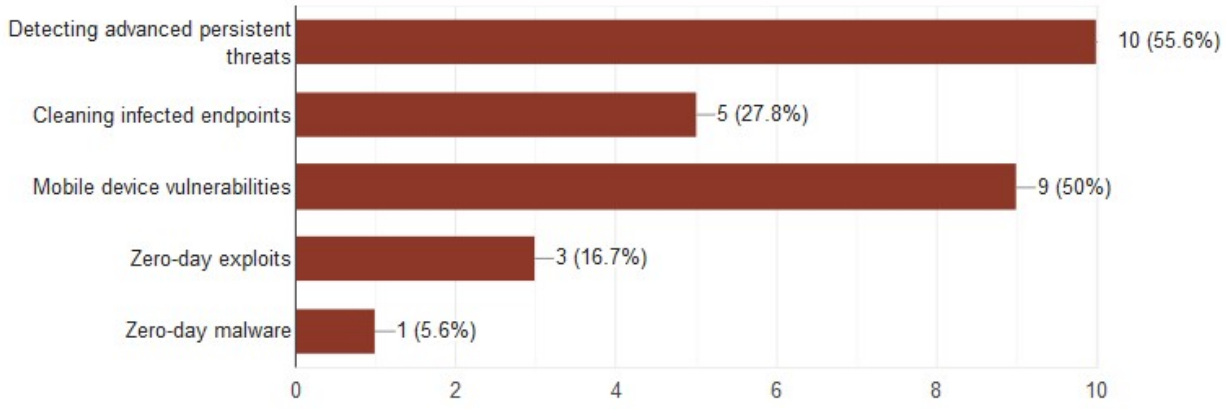

Figure 11: Limitations of currently deployed anti-malware

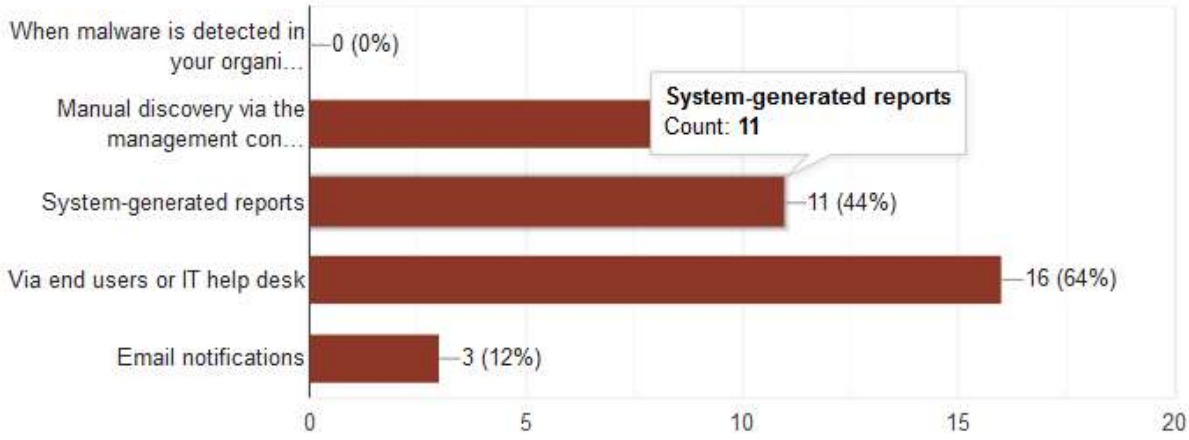

Figure 12: Methods of malware detection

4.1 Analysis of Figures

The responses suggest that viruses are the most prevalent malware challenges being faced by the Ghanaian government ministries by accounting for over seventy seven percent of incidents. Other relatively low records of malware experienced were ransomware, worms, rootkit attacks, bot attacks, spyware and trojans. Evidently, the only malware attack not experienced is the zero day attack. This is shown in figure 2. It is worth noting that over fifty two percent of the malware infections led to downtime as compared to twenty six percentage experiencing no consequences and thirty four percent of recovery costs as shown in figure 3. Furthermore, responses shown in figure 5 show that about forty three percent of the Ghanaian government ministries consider their ant-malware solutions to be performing above average with about twenty one percent considering theirs to be average. Figure 5 shows that, over forty five percent of respondents acknowledge that they usually have infection detected within seven days after they have been infected by a malware.

Twenty four percent successfully detect with twenty four hours and thirty five percent are successful in detecting only after seven days. The respondents perceive the biggest failing of their current anti-malware solutions as failure to detect many of the threats. About four percent of respondents experience the challenge of not being able to keep their solutions and systems updated in line with the latest malware evolutions and variant. Figure 8 shows that the Ghanaian government ministries sector typically consider efficacy, thus the ability to prevent, detect and remediate malware when evaluating or purchasing an endpoint anti-malware solution as the most important factor. Over forty eight percent of respondents constituting the majority attested to this as compared to thirty two percent for management and four percent for convenience.

Figure 9 shows that the most popular ant-malware brand/vendor is Kaspersky followed by with Windows Defender with about fifty and twenty nine percent of government ministries subscribing to its usage respectively. It is worth noting that about twenty five percent of the respondents use a free anti-malware. The most widely used anti-malware management approaches are the on premise management console. This accounts for forty one percent of respondents whereas an equal number is unmanaged with about sixteen percent using a cloud-based (vendor hosted) web management console. Figure 11 shows that detecting advanced persistent threats and mobile device vulnerabilities tend to be problems that are not being solved by their current anti-virus solution. Detecting advanced persistent threats averages over fifty five percent whereas mobile device vulnerabilities averages about fifty percent from respondents. A distribution of methods of currently detecting malware infection show that sixty four percent depend on end users' reports as well as help desk reports. About forty four percent on the other hand tend to be system generated. This is shown in figure 12 above.

4.2 Responses and Analysis from Interviews and Observations

The general purpose of interviewing the respondents was to confirm the responses given in the survey instrument. A unique observation and feedback which warranted further investigation and confirmation was the observation that the usage of free unlicensed anti-malware by government institutions. This was confirmed by the respondents who fell within the category, further to this observation, it was realized that responses in figure 2 recorded no advanced persistent threats yet that is considered the most difficult to detect. This is quite contradictory hence a further probe was carried to be sure if respondents appreciated what “advanced persistent threats” entailed. The confirmation was positive. The interviews and observations carried out during the research however generally confirmed the responses received from the survey instrument with the exception responses to how malware incidents within organizations are currently detected, majority of the respondents indicated their detections/observation were usually done manually and not system generated or via IT help desk.

4.3 Induced Baseline

Malware:

1. Viruses are most common infections constituting 77.3% of infections as against all other malwares types.
2. Malware infections account for downtime with 52.2% of responses indicating they experienced downtime as a result of malware infections.
3. Third party mobile devices, laptops and computers tend to be the most infected systems constituting over 83%of infected devices.
4. Advanced Persistent Threat is the most challenging threat that has not been properly countered as shown by 55.6%

Anti-malware:

1. Effectiveness of the current anti-malware protection is predominantly above average
2. Efficacy is the basis for purchase over management, convenience, deployment and client performance

5. CONCLUSION

This research focused on determining the malware baseline and anti-malware landscape of the Ghanaian government ministries. The approach was a sequential exploratory one where findings from preliminary interviews were used as a basis to develop the survey instrument for a larger sample. Beyond this was the simultaneous triangulation where more qualitative and quantitative data were collected concurrently and analyzed separately and then compared. Given the results obtained and analysis of the results, it may be concluded that within the context of malware baselining, viruses are the most common malware infections yet there are relatively little consequences experienced with the infections. Third party mobile devices, laptops and computers tend to be the most infected systems within the Ghanaian government ministries. In the anti-malware landscape context, they rate the effectiveness of the current anti-malware protection is predominantly above average or average at minimum though a significant number attest to difficulties in dealing with advanced persistent threats. The priority of the respondents in evaluation of anti-malware for purchase was on efficacy of the product and its ability to detect malware as against its convenience in use, client performance and ease of deployment. Possibly, a repetition of this research with an extension of the research to identify the psychology behind some of the practices within other sectors outside the government ministries sector would provide a better perspective of the baseline within the Ghanaian government ministries context.

REFERENCES

1. Harley, D. Myers, L. & Willems, E.(2010) "Test Files and Product Evaluation: the Case for and against Malware Simulation" , AVAR2010 13th Association of Anti-Virus Asia Researchers International Conference.
2. Huda, S., Abawajy, J., Al-Rubaie, B., Pan, L. & Hassan, M.(2019), Automatic extraction and integration of behavioural indicators of malware for protection of cyber–physical networks, Future Generation Computer Systems, Volume 101, Pages 1247-1258
3. Kinder J, Katzenbeisser S, Schallhart C, Veith H (2010) Proactive detection of computer worms using model checking. IEEE Trans Depend Secure Comput 7(4):424–438
4. Moshiri, E., Abdullah, A. B.,Binti, R., Mahmood, R & Muda, Z.(2017), Malware Classification Framework for Dynamic Analysis using Information Theory , Indian Journal of Science and Technology, Vol 10(21), DOI: 10.17485/ijst/2017/v10i21/100023, June 2017, https://pdfs.semanticscholar.org/6528/f669cab80c94633432a71624afb8a9a82b5f.pdf
5. Proença, D. & Borbinha J. (2018), Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001, https://www.researchgate.net/publication/325786419, DOI: 10.1007/978-3-319-93931-5_8
6. Rey, M., Dios, Q., Hernández, G. & Tabernero, B.(2019), Modeling the spread of malware on complex networks, Advances in Intelligent Systems and ComputingVolume 1004, Pages 109-116
7. Sikorski, M. & Honig, A. (2012). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*.
8. Szor, P.(2005), The Art of Computer Virus Research and Defense, Pearson Education. p. 204. ISBN 978-0-672-33390-3

9. Tiwari, S.R. & Shukla, R.U.(2018), An Android Malware Detection Technique Based on Optimized Permissions and API, Proceedings of the International Conference on Inventive Research in Computing Applications, ICIRCA , Article number 8597225, Pages 258-263
10. Zakaria, W.Z.A., Abdollah, M.F., Mohd, O. & Ariffin, A.F.M.(2017), The rise of ransomware, ACM International Conference Proceeding Series 28, Pages 66-70

About the Authors

Dr. Paul Danquah:
Dr. Paul Asante Danquah is an IT professional and a Senior Lecturer at the Heritage Christian College in Accra, Ghana. He holds a BSc HONS in Computing, MSc in Information Security and a PhD in IT (Specialized in Cybercrime) from the University of Greenwich UK, Anglia Ruskin University UK and Open University Malaysia respectively. He has various industry certifications, some of which are ISO27001 Lead Implementer, Certified Ethical Hacker (CEH), Certified EC-Council Instructor, Data Center Infrastructure Expert (DCIE), Cisco Certified Network Professional (CCNP) and Microsoft Certified Systems Engineer (MCSE). Dr. Paul Danquah has worked in various capacities over the last 20 years, these range from Programmer, Network Engineer, IT Manager and Technical Director of various organizations.

Mr. John Kani:
Mr. John Kani is an Assistant Lecturer with Heritage Christian College. Mr. Kani is currently a PhD candidate who holds MSc in Information Systems and Bachelor in Management Studies from University of Cape Coast.

Mr. Jojo Lartey:
Mr. Jojo Desmond Lartey is an Assistant Lecturer at the department of Information Technology, Heritage Christian University College, Ghana. His main areas of interest are computational intelligence and dynamical systems. He has BSc. Mathematics from Kwame Nkrumah University of Science and Technology Ghana, MSc. in Industrial Mathematical Modelling from Loughborough University England, and PGCert. in Advanced Computer Systems Development from University of the West of Scotland, Scotland. He is currently investigating traffic control at UNISA as a PhD candidate and he is a member of Society for Industrial and Applied Mathematics (SIAM).