IoT Malware: State-of-the-art Exploitation and Defense

Kristofor Bolton
University of Wolverhampton,
Wolverhampton Cyber Research
Institute (WCRI)

***Abstract*— The predicted increase in the number of IoT devices within the near future presents an opportunity for threat actors and foreshadows an increased threat to digital networks and networked devices. As IoT devices become more prevalent, malware is observed implementing advanced anti-detection techniques by researchers. This paper provides a research survey and research gap analysis of the state-of-the-art in malware exploitation and defence countermeasures methods regarding the IoT.**

Keywords—IoT, malware, evasion, exploitation, detection, defense, survey, gap analysis

I. Introduction

The number of IoT devices is set to grow substantially, expanding from approximately 26 billion in 2019 to 75 billion devices by 2025 [1]. This enormous growth coupled with lax security, or absence of security, within IoT devices creates a perfect storm for the global internet ecosystem [2, 3]. Botnets will have a larger pool to draw bots from, increasing the power of existing attacks such as DDoS, as seen in 2016 with the Miari IoT botnet which affected global internet connectivity [4]. As well as the threat to the internet, attackers will be presented with access to devices within the home creating privacy concerns [2].

This paper focuses on 'state-of-the-art' of exploitation and defence of IoT malware, as such we must define the phrase. Cambridge Dictionary defines 'State-of-the-art' as "... using the most recent ideas and methods" [5]. The sections ahead examine cutting edge methods used by malware authors for exploitation and malware analysists for their countermeasures.

This paper is organised into distinct sections. The next section describes the methodology followed to create this document. Section III introduces a taxonomy created to frame sections IV and V, the survey and gap analysis respectively, aiming to provide additional structure to complement the methodology. Finally, section VI and VII provide a reflection on possible future work and limitations of this work, and a conclusion.

II. Methodology

This paper aims to present an unbiased survey and gap analysis of state-of-the art IoT malware exploitation and defense following research guidelines outlined within Machi and McEvoy research methods [18]. The methodology below describes the protocol followed to create the survey and analysis.

A. Research Questions

What is the 'state-of-the-art' in IoT malware exploitation and defence? What are the gaps within the research studied? What are the challenges researchers face within IoT malware exploitation and defence?

B. Inclusion and Exclusion Criteria

Research articles with the following criteria appear in this paper:

- Published within the last 5 years (unless fundamental or noteworthy).
- Present a novel approach to IoT malware exploitation or defense.

Research articles with the following criteria will be excluded from this paper:

- Non-peer reviewed articles.
- Biased articles, such as white papers.
- Focus on non-novel approaches to IoT malware.
- Not written in English.

C. Source and Search Methodology

Data sources specific to computer science and technology research were used: IEEE Xplore, ACM Digital Library, Science Direct and Cornell University's arXiv.org. Logical operators such as 'OR' and 'AND', and other search manipulation operators, such as double quotes, were used to force specific phrase searches, e.g. "IoT Malware". Additionally, advanced search features were utilised to limit results to research articles from the last five years. An initial search without limitations was conducted to find possible fundamental papers.

III. A Malware Exploitation-Countermeasure Taxonomy

To facilitate a research survey and gap analysis this paper presents a taxonomy created by mapping malware exploitation techniques from Marpaung, et al [8] survey work to Veerappan, et al [6] to survey on countermeasures. This provides a method to visualize related areas of exploitation techniques and their defense. This allowed a more structured approach for gap analysis of the area. Due to the size of the area, the scope of this paper will be limited to one of the three root areas within the taxonomy – Disassembly and its child Code Obfuscation. Within this area we focus on Encryption and Polymorphic Code and Metamorphic Code. This child area and these exploit areas were chosen because they offer the potential to be considered state-of-the-art [9, 10, 13, 14].

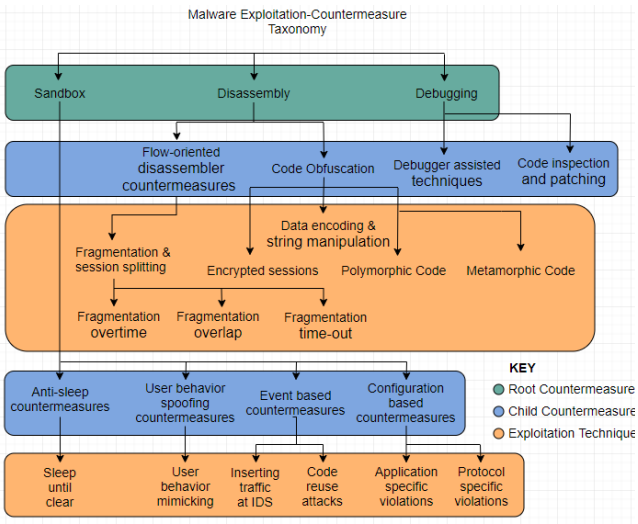

Figure 1.0 Malware exploitation-countermeasure taxonomy

IV. Survey

A. Polymorphic and Metamorphic Code

Polymorphic and metamorphic malware is of concern to researchers [6, 9, 10, 12] despite first appearing in 1990 and 1998 respectively [20] these methods continue to evolve to circumvent countermeasures into the present [19]. These types of malware change their underlying code to avoid creating a consistent signature which can be matched against a known malware list and avoid dynamic analysis techniques, such as sandboxing by appearing to be a non-malicious program by downloading multiple normal-looking packages and then combining them [10]. IoT devices typically lack computational power, memory and energy due to their reduced size and application [7]. This adds complexity to the challenge of securing such devices, particularly when dealing with state-of-the-art exploitation techniques.

For example, Osorio, et al [9, 12] propose and test novel defence solution to detect polymorphic malware by "semantic equivalence determination", a process by which a detection algorithm based on a finite state machine attempts to determine if a malware sample has mechanisms which are present in malware by comparing two software binaries. Typically, malware includes an infection vector, the ability to propagate, self defence mechanisms and a goal-based action (payload), this 'signature' can be detected.

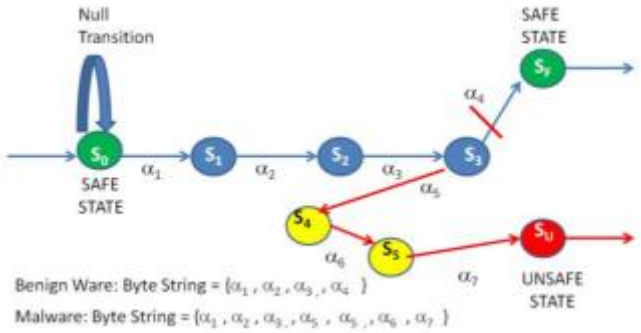

Figure 2.0 Malware input string passing through a finite state machine

Osorio, et al approach presents a promising advancement for the detection of advanced malware in normal computer systems; however, the approach does not translate well to IoT. Their process requires storage for binaries comparison, IoT devices may have limited storage capacity depending on their application, as described by Soliman et al [15]. Additionally, physical memory limitations present an issue when multiple binaries are analysed at once. Most importantly, their detection method, a finite state machine, steps through each byte string within the malware for comparison, a computationally heavy process [9, 12] which beyond hardware limitation issues leaves the IoT device open to further denial of service (DoS) attacks by sending multiple malicious files – even if the malware is unsuccessful in its infection it would still affect the devices responsiveness.

Amouri, et al [16] present a network level intrusion detection method based on IoT node behaviour and packet matching. A decision tree, a supervised machine learning technique, is used to classify packets, a method Amouri, et al justify due to the low computational complexity of the technique which is ideal for IoT. Their work builds on their previous efforts for malware detection [21], their updated work omits computationally heavy feature selection and the number of features is reduced to six to optimise for low-powered and memory-limited architecture. Compared to Osorio et al technique which do not adequately take the limited hardware of IoT devices into account, Amouri et al approach solves several problems. However, supervised machine learning methods required large amounts of data to be trained affectively, as described by Kumar [22]. Due to the nature of IoT networks and the large number of applications, a machine learning approach designed to detect behaviour could be considered inferior as the training needs to be application specific, otherwise error rates will be high [22, 26]. This results in a user or service provider needing to train or retrain the network for the application or if the application changed. In contrast, Osorio et al [9, 12] technique which is not behaviour specific do not suffer this problem.

B. Ecryptied Sessions

The use of encrypted sessions by malware to obfuscate their code and hide data exfiltration is a well-known technique [11, 20, 30]. The use of encryption within malware is generally not considered state-of-the-art, although some implementations can be impressive. Advanced Persistent Threats (APT) are known to utilise encryption heavily within their malware for obfuscation and hiding communications with command and control services [13, 14, 28]. This subsection will focus on the state-of-the-art in countermeasures and detection methods of encrypted sessions which malware creates to exfiltrate data.

He, et al [23] present a novel method to detect encrypted traffic within a cloud network using a combination of deep packet inspection (DPI) and entropy checking. Their method is comprised of two steps. First, network traffic is analysed using DPI to determine which traffic is encrypted by popular protocols (SSL, TLS, HTTPS), other proprietary encryption protocols are detected using entropy checking. The second step determines whether this is the result of user behaviour using behaviour profiling. If the encrypted traffic is inconsistent with the profile it is considered as data being exfiltrated. Although He et al research is not directly on IoT devices, their methods are applicable to IoT networks.

However, more research is required to test the application to IoT regarding the improvement of the lack-lustre detection time He reported which is likely unsuitable for IoT. This is discussed further within the next section, V.

Alornyo, et al [24] work builds in the work of Ma [31] with the concept of identity-based encryption with equality test (IBEET), designed to detect encrypted malware and analyse the integrity of encrypted data within a cloud environment. Metadata from network packets (such as sequence of packet lengths, times, byte distribution, source and destination ports, among others) is collected and analysed by a malware analytic provider (MAP), a trapdoor function which compares the created signatures against a database of signatures created from typical handshake protocols within the cloud network.

He [23] explore methods which arguably have more promise than Alornyo et al. Signature analysis of any type requires the creation and storage of a large number of signatures. If Alornyo et al method was used within an IoT environment it would likely require increased signatures for each type of interaction and protocol between devices, a significant weakness among heterogeneous devices [7]. Additionally, their stated method uses a central server to retain and analyse the signatures, within an IoT environment the devices themselves need to conduct this analysis.

V. Gap Analysis

When searching for gaps within research, the possible academic, economic and societal impacts should be considered. These are considered below for each.

A. Gaps within Polymorphic and Metamorphic Research

The survey suggests machine learning techniques which have been applied to IoT, such as Amouri, et al [16], could be restrained and unable to reach their potential due to the often-limited resources within the IoT environment [22, 26, 27]. However, as described by Kumar there are many machine learning techniques [22] and much research has been conducted on creating and tuning methods for limited devices, such as research conducted by IBM [26] for deep learning with limited numerical precision. Multiple opportunities involving these advances exist for IoT. The impact of these methods could be considered medium-high, due to the typical success rate of machine learning based classifiers [22] and the disruptive affect such successful malware detection would have.

B. Gaps within Ecryptied Sessions Research

Research conducted by He, et al [23] who presented a new approach combining deep packet inspection and behavioural profiling presents an opportunity to apply and improve their methods to IoT. The survey suggests similar research has not been applied to IoT. Specific and actionable gaps exist within their work; improving encryption detection time and fine-tuning the behavioural profile. He states their methods for encrypted traffic detection takes on average 45 seconds. This is far too slow for some IoT applications, such as near-real-time and real-time embedded devices within industrial settings as described by Shahpasand [25].

The impact of improving encryption detection research within IoT, is judged to be useful based on discussions by He, Alornyo and Ma within their papers.

C. Other Gaps within the Research Survey

Limitations in the speed of intrusion detection opens opportunities to research what constitutes “too slow” in terms of detection time. Virology and immunology paradigms could be applied to IoT networked systems to research the affect of slow detection times on malware propagation and perhaps create valuable and impactful insights such as minimum recommended detection times for vendors to aim for. The application of immunology to cyber security is an emerging area [29] and no current research discusses IoT specifically.

Advanced Persistent Threats (APT) use of malware may present a final opportunity discovered by this paper for security researchers. Despite the number of infections and number of targets by APTs reaching into the thousands [13, 14, 28] and their effects becoming global [28, 30], little peer-reviewed research has been conducted into threats and countermeasures of IoT malware used by APTs. Research into this area would be impactful in a number of ways, including; bolstering the knowledge economy, changing organisational culture and practices and may increase public engagement with issues around state-sponsored cyber operations.

VI. Further work and Limitations

The taxonomy created by combining the discussions of Marpaung, et al [8] and Veerappan, et al [6] used to guide the initial survey and topics discussed in this paper is incomplete. This was due to the time limitations, the required time to produce a full systematic survey of the broader field would be significant. The area of focus for this paper within the taxonomy – obfuscation techniques – could be bolstered by further research and additions, including the work of You, et al [11] who is referenced within this paper.

VII. Conclusion

The aim of this paper was to answer three questions posed in section II. State-of-the-art IoT malware is present and continues to evolve in the wild, as does do the defenses and countermeasures created by researchers. The research survey and subsequent analysis has identified a lack of research specific to malware operating within the IoT environment, despite its prevalence, expected enormous growth and typically insufficient security.

Researchers venturing into IoT malware research face difficulties securing IoT and applying methods which may work in other environments, most notably hardware limitations and network architectures of IoT devices. The survey found machine learning techniques which may achieve high success rates in other environments may need to be optimized for limited IoT devices and not simply applied to such devices for example.

Ultimately, the purpose of this paper was to discover possible research gaps within the domain of IoT malware. Promising areas with varying levels of impact have been identified within section V.

REFERENCES

[1] Statista (2019). *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)*. Accessed on: Mar. 15, 2019. [online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] Schneier, B. (2017). *Security and the Internet of Things*. Accessed on: Mar. 15, 2019. [online]. Available: https://www.schneier.com/blog/archives/2017/02/security_and_th.html

[3] Krebs, B. (2018). *Naming & Shaming Web Polluters: Xiongami*. Accessed on: Mar 15, 2019. [online]. Available: https://krebsonsecurity.com/2018/10/naming-shaming-web-polluters-xiongmai/

[4] Cloudflare (2016). *What is the Mirai Botnet?* Accessed on: Mar. 16, 2019. [online]. Available: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[5] Cambridge Dictionary (2019). *Meaning of 'state-of-the-art' in English*. Accessed on: Mar. 17, 2019. [online]. Available: https://dictionary.cambridge.org/dictionary/english/state-of-the-art

[6] Veerappan, C., Keong, P., Tang, Z., and Tan F. (2018). Taxonomy on malware evasion countermeasures techniques. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. 5-8 Feb. 2018. Singapore, Singapore. [online]. Available: https://ieeexplore.ieee.org/document/8355202

[7] Hossain, M., Fotouhi., M, and Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In *2015 IEEE World Congress on Services*. 27 June – 2 July 2015. New York, NY, USA. [online]. Available: https://ieeexplore.ieee.org/document/7196499

[8] Marpaung, J., Sain, M., and Lee, H. (2012) Survey on malware evasion techniques: state of the art and challenges. In *2012 14th International Conference on Advanced Communication Technology (ICACT)*. 19-22 Feb 2012. PyeongChang, South Korea. [online]. Available: https://ieeexplore.ieee.org/document/6174775

[9] Osorio, F., Qiu, H., and Arrott, A. (2015). Segmented sandboxing – A novel approach to Malware polymorphism detection. In *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)*. 20-22 Oct 2015. Fajardo, Puerto Rico, USA. [online]. Available: https://ieeexplore.ieee.org/document/7413685

[10] Selamat, N., Ali, F., and Othman, N. (2016). Polymorphic Malware Detection. In *2016 6th International Conference on IT Convergence and Security (ICITCS)*. 26 Sept. 206. Prague, Czech Republic. [online]. Available: https://ieeexplore.ieee.org/document/7740362

[11] You, I., and Yim, K. (2010). Malware Obfuscation Techniques: A brief Survey. In *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*. 4-6 Nov. 2010. Fukuoka, Japan. [online]. Available: https://ieeexplore.ieee.org/document/5633410

[12] Osorio, F., and Qui, H. (2013). Static Malware Detection with Segmented Sandboxing. In *2013 8th International Conference on Malicious an Unwanted Software (MALWARE*). 22-24 Oct. 2013. Fajardo, Puerto Rico, USA. [online]. Available: https://ieeexplore.ieee.org/document/6703695

[13] Kaspersky (2015a). *Equation Group: The Crown Creator of Cyber-Espionage*. Kaspersky Press Release. [online]. Available: https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage

[14] Kaspersky (2015b). *Equation Group: Questions and Answers*. Version 1.5. Archived by archive.org. [online]. Available: https://archive.org/details/B-001-004-374

[15] Soliman, S., Sobh, M., and Bahaa-Eldin, A. (2017). Taxonomy of malware analysis in the IoT. In *2017 12th International Conference on Computer Engineering and Systems (ICCES)*. 19-20 Dec 2017. Cairo, Egypt. [online]. Available: https://ieeexplore.ieee.org/document/8275362

[16] Amouri, A., Alaparthy, V., and Morgera, S. (2018). Cross layer-based intrusion detection based on network behaviour for IoT. In *2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON)*. 9-10 April 2018. Sandy Key, FL, USA. [online]. Available: https://ieeexplore.ieee.org/document/8363921

[17] Sikorski, M., and Honig, A. (2012) *Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software*. No Starch Press, San Francisco, CA, USA.

[18] Machi. L. A., and McEvoy. B. T. (2009) *The Literature Review*. Crown Press, Thousand Oaks, CA, USA.

[19] Moubarak, J., Chamoun, M., and Filiol, E. (2018) Developing a K-ary malware using Blockchain. In IEEE *NOMS 2018 Network Operations and Management Symposium*. 23-27 April 2018. Taipei, Taiwan. [online]. Available: https://ieeexplore.ieee.org/document/8406331

[20] Rad, B., Masrom, M., and Ibrahim, S. (2012). Camouflage in Malware: from Encryption to Metamorphism. *IJCSNS International Journal of Computer Science and Network Security*. VOL. 12, No. 8. August 2012. [online]. Available: https://s3.amazonaws.com/academia.edu.documents/46300512/Camouflage_In_Malware_From_Encryption_To20160607-13910-1num97l.pdf

[21] Amouri, A., Morgera, S., Bencherif, M., and Manthena, R. (2018). A Cross-Layer, Anomaly-based IDS for WSN and MANET. In *Sensors*. Vol.18, No.2. Feburary 2018. [online]. Available: https://www.mdpi.com/1424-8220/18/2/651/htm

[22] Kumar, A. (2016). *Learning Predictive Analytics with Python*. Packt Publishing, Livery Street, Birmingham, UK.

[23] He, Gaogeng., Zhang, Tao., Ma, Yuanyuan., and Xu, Bingfeng. (2014). A Novem Method to Detect Encrypted Data Exfiltration. In *2014 Second Internaitonal Conference on Advanced Cloud and Big Data*. 20-22 November 2014. Huangshan, China. [online]. Available: https://ieeexplore.ieee.org/document/7176100

[24] Alornyo, S., Asante, M., Hu, X., and Mireku, K. (2018). Encrypted Traffic Analysis using Identiy Based Encryption with Equality Test for Cloud Computing. In *2018 IEEE 7th International Conference on Adaptive Science & Technology (ICAST)*. 22-24 August 2018. Accra, Ghana. [online]. Avaialble: https://ieeexplore.ieee.org/document/8507063

[25] Shahpasand, R., Sedaghat, Y., and Paydar, S. (2016). Improving the Stateful Robustness Testing of Embeddded Real-Time Operating Systems. In *IEEE 6th Intenational Conference on Computer and Knowledge Engineering (ICCKE)*. 20-21 October 2016. Mashhad, Iran. [online]. Available: https://ieeexplore.ieee.org/document/7802133

[26] Gupta, S., Agrawal, A., and Gopalakrishnan. (2015). Deep Learning with Limited Numerical Precision. In *Proceeding of the 32nd Internaitonal conferenceon Machine Learning*. 2015. Lille, France. [online]. Available: http://proceedings.mlr.press/v37/gupta15.pdf

[27] Anguita, A., Ghio, A., and Pischiutta, S. (2007) A learning machine for resoure-limted adaptive hardware. In *2nd NASA/ESA Conference on Adaptive Hardware and Systems.* 5-8 August 2007. Edinburgh, UK. [online]. Available: https://ieeexplore.ieee.org/document/4291969

[28] FireEye, Mandiant (2013). *APT 1: Exposing One of China's Cyber Espionage Units*. [online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

[29] Brown, J., Anwar, A., and Dozier, G. (2017). An artificial immunity approach to malware detection in a mobile platform. *In EURASIP Journal on Information Security* 2017. Springer. [online]. Available: https://doi.org/10.1186/s13635-017-0059-2

[30] FireEye (2018). *Annual Threat Report: M-Trends 2019*. [online]. Available: https://www.fireeye.com/current-threats/annual-threat-report.html

[31] Ma, S. (2016). Identity-based encryption with outsourced equality test in cloud computing. In Information Sciences. 2016. Pp. 389-402. Elsevier. [online]. Available: https://www.sciencedirect.com/science/article/pii/S0020025515006520