Survey of Computer Worms

Mackenzie Chase

Abstract—**Computer worms represent only a small portion of the malware that affects end users. As the cyberspace grows with more and more devices connected to the internet and each other, particularly with the rise of Internet of Things (IoT) and Cloud technologies, there is an increasing need for security measures to prevent, detect and recover from the threat of worms. While the protection of systems is crucial, a vulnerability which is far less technical is human error. It is essential to prioritize training and awareness to recognize possible threats, in particular phishing. With new technologies such as machine learning, threat agents can accelerate the creation and deployment of malicious software, as well as increase its sophistication. However these tools can also be used to help combat these threats.**

I. INTRODUCTION

Computer worms have evolved from simple malicious programs to sophisticated threats capable of causing widespread disruption and financial loss. Unlike viruses, worms can replicate and spread independently, exploiting vulnerabilities in networked systems. The digital landscape has become increasingly complex, with interconnected systems facilitating the rapid exchange of information. While this connectivity has numerous benefits, it has also given rise to new cyber threats.

II. DESCRIPTION OF THREAT

Computer worms are a type of malware with the unique trait of being able to propagate throughout a network without the need of a host or user interaction. They exploit vulnerabilities in software and network protocols. Once they infiltrate a system, they can execute payloads that may include but are not limited to, data theft, system damage, or even creating backdoors for future malicious activities. There are fours phases of a computer worm: target discovery, propagation, activation, and infection. This cycle then repeats with each successful infection. Boukerche and Zhang [1] summarized the classifications of Weaver et al. [2] of each phase.

In the target discovery phase, the worm can have a predefined list of hosts to target termed a “hit-list” which can reside within the worm body or externally. The worm can probe the network for vulnerable hosts. It can also be passive needing a vulnerable host to visit the infected machine which requires user intervention.

The propagation phase is classified into three main types: self-carried, second channel, and embedded. Self-carrier worms are capable of propagating the whole worm body. Second channel triggers a download from a third party to propagate itself. Embedded are worms integrated into host files or programs. The activation phase is characterized by human activation, second order activation meaning a user executes a certain program or file which then triggers the worm, a scheduler, or self activation.

Finally, the payload phase can be non existent, an Internal Remote Control (IRC), a spam-relay, a Denial of Service (DoS), data collection, data damage, physical damage, and worm maintenance. A key aspect of worms is the speed at which they can spread; a worm can infect thousands of machines within minutes, leading to extensive damage and disruption.

Notable examples of computer worms include the Morris worm, the first ever worm released in 1988, the ”WannaCry” ransomware, which utilized worm-like behavior to encrypt files across vulnerable systems [3]. The Stuxnet worm, arguably the first cyber-weapon, was able to cause physical damage to Iran’s nuclear program in 2010 [4]. It utilized multiple zero-day vulnerabilities, a vulnerability who’s existence has been known for zero days, to spread and take control of the the programmable logical controllers. Such incidents highlight the financial and operational risks posed by these types of malware.

Attackers have already shifted from monolithic malware to blended malware, meaning instead of using a worm, virus or trojan to spread a payload, they are utilizing some combination of them to maximize its spread with multiple payloads. Polymorphic worms are capable of changing their structure in each new host it infects making them one of the most difficult to detect [5]. This changing of structure means the signature or byte content of the worm changes. Anti-virus software, which should really be called anti-malware software, and intrusion detection systems (IDS) typically try to detect malware statically by comparing file signatures of known malware [6]. This proves problematic if a polymorphic worm has infected a system. As threat agents become increasingly more capable and make use of sophisticated methods, the malware they create becomes more dangerous. The world will need to adapt to these next generation malwares.

III. RELATED WORKS

Sulieman and Fadlalla [5] looked into the detection of zero-day polymorphic worms. They discuss the strengths and limitations of different systems geared towards detecting polymorphic worms. In particular, some of the proposed systems are rooted in generating signatures of worms in honeypot networks. A honeypot is a vulnerable decoy that appears to be apart of a system for the purpose of gathering information on threats. This gives the worm a controlled environment to spread and morph while being monitored. The main types of solutions were byte string signatures, content-based signatures, and automatic signature generation (ASG). One of the main weaknesses of these systems is they can generate false positives if normal traffic enters the honeypot.

Zhou et al. [7] investigated utilizing neural networks to facilitate the detection of worms. They took two different approaches: convolutional neural networks (CNN) and deep neural networks (DNN). Using synthetic worm payload datasets, they trained the models with some portion of the datasets mixed with regular internet traffic that they collected. They then tested the models with the remaining worm dataset and analyzed the results. The main concern is to maximize accuracy which they defined as a function of true positive, true negative, and false positive and false negative results. They did utilize a private company dataset of worm payloads when using DNN but could not provide the generated signatures due to privacy which may make their findings lose some validity. Roseline and Geetha [8] explored traditional and contemporary detection methods for malware. Their finds suggested some incorporation of machine learning with either dynamic analysis or static analysis proved beneficial in improving accuracy of correct malware detection for both computers and mobile devices. Moreover, Aslan and Samet [6] argue as the complexity of malware increases, the successful detection rate decreases. This intuitively makes sense, however they found Behavior-based malware detection outperformed all other types including deep learning based.

Obimbo et al. [9] argue human error is the weakest link in preventing internet worms. Not all malware is detected and removed by IDS and anti-virus software. Phishing emails are a prominent method to get into a system. They highlight the importance that cyber-security is not only an IT department problem but a company wide problem. Training for all employees and even personally for individuals is a necessity for the future.

A rather peculiar defence system of fighting worms, is with benevolent worms. Chowdhury et. al [10] discuss the possibility of using benevolent worms to defend systems. Using the same mechanics of malicious worms, these worms can scan networks for various goals including searching for idle machines, machines that need patches, or even infected machines. Theses benevolent worms can then propagate throughout a network executing desired tasks such as system maintenance, encrypting uninfected files if there is a breach in a system, or even preventing the further spread of a malicious worm.

As we use more of our mobile devices for all aspects of our lives, attackers have set their target on mobile devices. Researchers analyzed the proliferation of malware targeting mobile devices [8].

IoT has boomed in recent years, making it another profitable target for attackers. Vehicles are becoming increasingly complex incorporating IoT like components. More specifically, Vehicle Ad Hoc Networks (VANETs) are another possible target for attackers [1]. Worms would be able to propagate through these vehicle networks with the possibility of causing havoc on the roads by exploiting the on board units through non-safety applications. Several factors would affect a worms propagation namely, vehicle density in an area, communication range, and more. There are some proposed countermeasures but none without limitations. It is an open issue that needs further investigation.

IV. Thoughts & Remarks

The real danger of malware is most are an amalgamation of different types utilizing their most deadly components. A lot of the details regarding machine learning, and anti-virus techniques are out of scope from the course. [9] make reference that as long as users have access to email, there will always be a threat of phishing which leads to the spread of malware. Through awareness programs, and training, we can improve the human aspect in this problem. In terms of technical solutions, anti-virus software, firewalls at both the user and domain level, as well as intrusion detection systems are components of the best practices currently are available. There is a need for future-proofing when worms and other malware evolve beyond the means we currently have to defend against them. It would be a monumental task to rebuild the internet from scratch with proper security measures implemented and further migrate our current structures to that new platform, however like with all things, it likely will not be without flaws and would be susceptible to different threats.

References

[1] A. Boukerche and Q. Zhang, “Countermeasures against worm spreading: A new challenge for vehicular networks,” *ACM Comput. Surv.*, vol. 52, no. 2, May 2019. [Online]. Available: https://doi-org.proxy.hil.unb.ca/10.1145/3284748

[2] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, “A taxonomy of computer worms,” in *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, ser. WORM ’03. New York, NY, USA: Association for Computing Machinery, 2003, p. 11–18. [Online]. Available: https://doi-org.proxy.hil.unb.ca/10.1145/948187.948190

[3] S. William, *Computer security: Principles and practice*. Pearson Education, 2018.

[4] B. Bakić, M. Milić, I. Antović, D. Savić, and T. Stojanović, "10 years since stuxnet: What have we learned from this mysterious computer software worm?" in *2021 25th International Conference on Information Technology (IT)*, 2021, pp. 1–4.

[5] S. M. A. Sulieman and Y. A. Fadlalla, "Detecting zero-day polymorphic worm: A review," in *2018 21st Saudi Computer Society National Computer Conference (NCC)*, 2018, pp. 1–7.

[6] A. Aslan and R. Samet, "A comprehensive review on malware detection approaches," *IEEE Access*, vol. 8, pp. 6249–6271, 2020.

[7] H. Zhou, Y. Hu, X. Yang, H. Pan, W. Guo, and C. C. Zou, "A worm detection system based on deep learning," *IEEE Access*, vol. 8, pp. 205 444–205 454, 2020.

[8] S. Abijah Roseline and S. Geetha, "A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks," *Computers Electrical Engineering*, vol. 92, p. 107143, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790621001464

[9] C. Obimbo, A. Speller, K. Myers, A. Burke, and M. Blatz, "Internet worms and the weakest link: Human error," in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2018, pp. 120–123.

[10] M. M. Chowdhury, J. M. D. Toro, and K. Kambhampaty, "Active cyber defense by benevolent worms," in *2022 IEEE International Conference on Electro Information Technology (eIT)*, 2022, pp. 580–585.