Journal of Data Analytics, Information, and Computer Science (JDAICS)
Volume 1, No 2 – April 2024
e-ISSN : 3032-4696

IMPLEMENTATION OF DYNAMIC METHOD FOR MALWARE DETECTION IN EMAIL PHISHING ATTACKS ON LET'S DEFEND

Sanjay[1], Rahayu Ningsih[2], Ahmad Jurnaidi Wahidin[3]*
[1,2,3] Bina Sarana Informatika University, Jakarta, Indonesia
[1] sanjaytopandas1@gmail.com, [2] rahayu.ryh@bsi.ac.id, [3*] ahmad.ajn@bsi.ac.id

Received: 10-04-2024	Revised: 20-04-2024	Approved: 30-04-2024

ABSTRACT
In the rapidly evolving landscape of cybersecurity threats, the need for robust defenses against phishing attacks has become paramount. This study explores the efficacy of malware detection in phishing email attacks using dynamic analysis on the Letsdefend.io platform. Leveraging the insights provided by the Deloitte Center for Controllership regarding the escalating frequency of cyber adversaries targeting organizational data, this research investigates the effectiveness of the Letsdefend.io platform, particularly utilizing the SOC 146 rule, in identifying and mitigating phishing threats. Through a comprehensive analysis process encompassing dynamic malware analysis techniques, such as those employed by VirusTotal and URLHaus, alongside detailed examination of suspicious email attachments using the Mailbox feature, this study aims to provide insights into the evolving tactics of phishing attackers, specifically those utilizing Excel 4.0 Macros. The research methodology involves collecting malware samples for analysis, configuring sandbox environments with tools like Process Monitor and Regshot, and utilizing sophisticated analysis tools like ProcDot to visualize malware behavior. Additionally, the study examines the effectiveness of the Letsdefend.io platform in detecting phishing URLs and malicious domains reported by AnyRun and URLHaus databases. The findings reveal promising results in the detection and identification of phishing threats, shedding light on the potential of dynamic analysis methods in bolstering cybersecurity defenses against evolving phishing techniques. This research contributes to the ongoing efforts to enhance cybersecurity measures and protect organizational assets from the pervasive threat of phishing attacks.
Keywords: Cybersecurity,Dynamic analysis,Malware detection, Phishing

INTRODUCTION

According to the Deloitte Center for Controllership, over the past 12 months, 34.5% of surveyed executives reported that their organization's accounting and financial data have been targeted by cyber adversaries (Chuck Brooks, 2023). Hence, cybersecurity has become increasingly crucial as many organizations and individuals utilize technology and the internet for data storage, access, and processing. Cyber security has become a very critical concern (Admass et al., 2024), Cyber threats that have the potential to become threats are cyber terrorism, cyber crime and cyber war (Ramadhan, 2019), security and privacy issues still have to be handled carefully (Sookhak et al., 2018), so Cyber security needs to be developed with the integration of the latest technology (Putri, 2021) for example the application of IoT (Ilhami, 2022) (Belgaum et al., 2018). Can be used to protect infrastructure (Silalahi, 2022) which is widely used in smart cities (Habibzadeh et al., 2019) (Qamar & Bawany, 2020)

(Vitunskaite et al., 2019) (Ma, 2021), security in transportation (Gunes et al., 2021), health services (Javaid et al., 2023) and others. Cyber threats have grown more complex with the emergence of new technologies such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain. Additionally, cyber attacks are evolving through techniques like phishing, ransomware, and Distributed Denial of Service (DDoS) attacks (Dwiyani Permatasari, 2021).

In the current scenario, human life heavily relies on devices, smartphones, data packages, or internet connections, creating a vulnerability exploited by malicious actors who capitalize on dense network traffic. This can lead to various crimes targeting numerous individuals via website (Safi & Singh, 2023), email (Bountakas & Xenakis, 2023), short message service (SMS) (Barrera et al., 2024), online banking (Syah, 2023), including phishing (Candraditya Pamungkas & Trimuti Saputra, 2020). Phishing can be defined as deception where accounts are used to extract sensitive information from victims. There are numerous types of phishing, including email phishing, whaling, voice phishing, SMS phishing, among others. Phishing messages often contain malware-infected files. Malware is software designed to infiltrate information systems, networks, or servers, sometimes causing damage without the owner's knowledge (Putra, 2023). Researchers or developers of anti-phishing applications are often individuals who have experienced phishing attacks and seek retribution by creating such applications phishing . It is imperative for the public to utilize these tools effectively to mitigate the risk of falling victim to phishing attacks (Hidayat et al., 2023). Supportive tools include VirusTotal and URLHaus.

Fraud involving malware aims to execute on users' computers. Malware has emerged as a cyber security threat (Gorment et al., 2023) and is increasing very rapidly (Venkatasubramanian et al., 2023), malware is one of the most dangerous threats to the digital world (M. & Sethuraman, 2023) (Chen et al., 2023), malware is typically attached to emails sent to users by phishers. Once the victim clicks on the link, the malware starts functioning. Sometimes, the malware is included in downloadable files (Caniago & Sutabri, 2023). Malware detection approaches can be classified into two classes, including static analysis and dynamic analysis (Shaukat et al., 2023). Each method employs different techniques and yields different types of data. The circumstances often dictate which method to employ (Fahriza, 2022). However, utilizing both methods provides a comprehensive overview. This study primarily focuses on dynamic analysis.

In this research, I analyze the Mailbox, VirusTotal, and AbuseIPDB sections of the Let's Defend platform. Mailbox analysis involves examining and analyzing received emails, checking sender addresses, email content, and suspicious attachments to identify phishing emails utilizing Excel 4.0 Macros. Subsequently, VirusTotal is used to scan suspected email attachments, comparing them with existing threat databases to identify related malware. Analyzing data from Mailbox, VirusTotal, and URLHaus seeks patterns and specifics indicating the presence of phishing emails utilizing Excel 4.0 Macros.

RESEARCH METHODS

The method employed in this research is dynamic analysis using the Let's Defend platform. This method was chosen because it can provide a deep understanding of email phishing attacks using Excel 4.0 Macros, and it can identify related malware with high accuracy. The analysis process begins by collecting malware samples for analysis.

The purpose of this process is to validate and gain a deeper understanding of the received emails, whether they are phishing emails, so that useful information can be obtained from the analysis results. Dynamic analysis and malware detection methods are no longer able to keep up with the rapid evolution of malicious code, which includes masking techniques such as polymorphism, packing, and encryption.

Furthermore, basic information about the system configuration is captured before executing the malware using the snapshot feature of the VMware desktop application. Before running the malware, the following four tools will be activated and configured in the sandbox environment: Process Monitor, Process Hacker, CaptureBAT, and Regshot. These tools will record and reproduce the system status at specific points in time. Subsequently, the same tools will be run again after executing the malware, and used to compare the infected system status with the snapshot or previous baseline. Additionally, the ProcDot analysis tool will be used to generate detailed visual representations of all activities that occur after the malware execution. There are four additional tools that will be used to analyze phishing emails, namely, The first step is to search for the source email address in the mailbox, using the email subject "meeting notes" in the mailbox search function on the Lets Defend platform.

Figure 1. Mailbox (Let's Defend)

The second step is to analyze the extracted file. Here, we use Virustotal to check whether the file is malicious or not, and then retrieve data such as URL domain, IP address, and MD5.

Figure 2. File excel Virustotal

The third step is to analyze using Anyrun. In this step, the MD5 obtained from Virustotal is checked to see if there is any malicious activity.

Journal of Data Analytics, Information, and Computer Science (JDAICS)
Volume 1, No 2 – April 2024
e-ISSN : 3032-4696

Figure 3. Malicious Activity(AnyRun)

The fourth step is to search using the browse database by inputting the URL domain obtained from Virustotal to check if anyone has reported whether the URL is malicious or not.

Figure 4. browse database royalpalm.sparkblue.lk

RESULTS AND DISCUSSION

VirusTotal

At VirusTotal, analysis is performed on the excel file from the attachment that has been extracted, named research-1646684671.xls. The analysis results show that out of 60 antivirus engines tested, 36 antivirus engines indicate that the excel file is potentially harmful.

Figure 5 Excel file

Figure 6. iroto1.dll file

Furthermore, in the image above, analysis is conducted on the iroto.dll file, where 8 out of 70 antivirus engines classify the iroto.dll file as harmful.

Figure 7. iroto1.dll file

Subsequently, on the iroto1.dll file, it is found that 10 out of 70 antivirus engines state that the dll file is potentially harmful. In addition to assessing the detection results whether the files are harmful or not, it is also important to gather additional information related to these files as references for further analysis. The information collected includes hashes of the three files using the MD5 type, URLs, and IP domain addresses from the URLs found.

URLHaus

Through this research, we used the search function in the database by entering the domains obtained from AnyRun. The results showed that both domains, namely nws.visionconsulting.ro and royalpalm.sparkblue.lk, are registered as Malware URLs reported by @lazyactivist192 on May 28, 2021, at 14:55:06.

Figure 8. Browse database royalpalm.sparkblue.lk

The importance of educating users in phishing prevention efforts cannot be underestimated. Educated users have the ability to recognize phishing attacks and know the steps to avoid them, making them more likely to avoid the threat than less educated users. User education is the key to protecting oneself from phishing attacks. Users can avoid these threats by recognizing security indicators, identifying phishing websites, and not being tempted by attractive offers in phishing emails. However, education requires significant time and cost investment, especially as phishing attacks continue to evolve. Therefore, Mohammad suggests that to prevent phishing attacks, technical and legal solutions are needed. Various techniques, solutions, and tools have been developed to prevent or at least reduce the success of phishing attacks. Some techniques attempt to block phishing emails or websites, while others aim to inform or warn users. Additionally, there are efforts to increase user awareness of phishing scams. However, to date, there is no solution that can fully prevent phishing attacks, and phishers continue to develop their techniques. Current anti-phishing technology is unable to detect or stop phishing attacks (Abroshan et al., 2018).

From the results of our research, we successfully detected the presence of attachments in an email suspected of cybercrime. We concluded that from the data obtained through malware detection analysis in phishing email attacks, it was revealed that the attackers used phishing techniques distributed via email. They embed malicious scripts into a document disguised as an official document to trick victims into accessing it. This is done with the aim of obtaining important information such as personal data, account data, and financial data from individuals or organizations targeted by phishing (Burita et al., 2021). The obtained information is then stored in servers or databases owned by the attackers.

CONCLUSION

Based on the study conducted in this research entitled "Malware Detection Analysis on Phishing Email Attacks using dynamic method on Letsdefend.io platform with EventID: 93, where this alert is triggered by SOC 146 rule Phishing Mail Detected Excel 4.0 Macros", it can be concluded that malware detection against phishing emails using the Letsdefend.io platform with the utilization of SOC 146 rule has proven effective in identifying attacks and protecting systems from these threats. Further research can be conducted to delve deeper into phishing techniques that utilize Excel 4.0 Macros and identify typical behavioral patterns of such attacks.

DAFTAR PUSTAKA

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2018). Phishing attacks root causes. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 10694 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-319-76687-4_13

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/https://doi.org/10.1016/j.csa.2023.100031

Barrera, D., Naranjo, V., Fuertes, W., & Macas, M. (2024). *Literature Review of SMS Phishing Attacks: Lessons, Addresses, and Future Challenges BT - Advanced Research in Technologies, Information, Innovation and Sustainability* (T. Guarda, F. Portela, & J. M. Diaz-Nafria (eds.); pp. 191–204). Springer Nature Switzerland.

Belgaum, M. R., Alansari, Z., Jain, R., & Alshaer, J. (2018). A framework for evaluation of cyber security challenges in smart cities. *Smart Cities Symposium 2018*, 1–6.

Bountakas, P., & Xenakis, C. (2023). HELPHED: Hybrid Ensemble Learning PHishing Email Detection. *Journal of Network and Computer Applications*, *210*, 103545. https://doi.org/https://doi.org/10.1016/j.jnca.2022.103545

Burita, L., Matoulek, P., Halouzka, K., & Kozak, P. (2021). Analysis of phishing emails. *AIMS Electronics and Electrical Engineering*, *5*(1), 93–116. https://doi.org/10.3934/ELECTRENG.2021006

Candraditya Pamungkas, W., & Trimuti Saputra, F. (2020). Analisa Mobile Phishing Dengan Incident Response Plan dan Incident Handling. *Jurnal Riset Komputer)*, *7*(4), 2407–389. https://doi.org/10.30865/jurikom.v7i4.2304

Caniago, K., & Sutabri, T. (2023). Tindak Kejahatan Phising Di Sektor Pelayanan Di Universitas Bina Insan Lubuklinggau. *Jurnal Riset Sistem Informasi Dan Teknik Informasi*, *8*(1), 117–125.

Chen, Y., Ding, Z., & Wagner, D. (2023). Continuous learning for android malware detection. *32nd USENIX Security Symposium (USENIX Security 23)*, 1127–1144.

Chuck Brooks. (2023). *Tren & Statistik Keamanan Siber Untuk 2023*. Website Forbes.

Dwiyani Permatasari. (2021). *Tantangan Cyber Security di Era Revolusi Industri 4.0*. Kementrian Keuangan Republik Indonesia.

Fahriza, C. F. (2022). *Analisis Ransomware Secara Statis dan Dinamis Untuk Pemetaan Evolusi Ransomware Analisis Ransomware Secara Statis dan Dinamis Untuk Pemetaan Evolusi Ra nsomware*.

Gorment, N. Z., Selamat, A., Cheng, L. K., & Krejcar, O. (2023). Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges, and Future Directions. *IEEE Access*, *11*, 141045–141089. https://doi.org/10.1109/ACCESS.2023.3256979

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security*, *103*, 102196.

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, *50*, 101660.

Hidayat, W., Ramli, H., Ikhram, P. M. B., & ... (2023). Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar. *Vokatek: Jurnal …*, *01*, 28–33.

Ilhami, D. A. S. (2022). Data privasi dan keamanan siber pada smart-city: Tinjauan literatur. *Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi*, *2*(1), 51–60.

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016. https://doi.org/https://doi.org/10.1016/j.csa.2023.100016

M., G., & Sethuraman, S. C. (2023). A comprehensive survey on deep learning based malware detection techniques. *Computer Science Review*, *47*, 100529. https://doi.org/https://doi.org/10.1016/j.cosrev.2022.100529

Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*, *7*, 7999–8012.

Putra, R. C. (2023). *Analisis email phising dan karakteristik malware di kementrian komunikasi dan informatika*.

Putri, Y. H. Z. M. N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT: Information Communication & Technology*, *Vol. 21 No. 1 (2021): JICT-IKMI*, *Juli 2021*, 42–52.

Qamar, T., & Bawany, N. Z. (2020). A cyber security ontology for smart city. *International Journal on Information Technologies & Security*, *12*(3), 63–74.

Ramadhan, I. (2019). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara. *Jurnal Asia Pacific Studies*, *3*(2), 181–192.

Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*, *35*(2), 590–611. https://doi.org/https://doi.org/10.1016/j.jksuci.2023.01.004

Shaukat, K., Luo, S., & Varadharajan, V. (2023). A novel deep learning-based approach for malware detection. *Engineering Applications of Artificial Intelligence*, *122*, 106030. https://doi.org/https://doi.org/10.1016/j.engappai.2023.106030

Silalahi, F. D. (2022). Keamanan Cyber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1–285.

Sookhak, M., Tang, H., He, Y., & Yu, F. R. (2018). Security and privacy of smart cities: a survey, research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(2), 1718–1743.

Syah, R. (2023). Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber. *Jurnal Impresi Indonesia*, *2*(9), 864–870.

Venkatasubramanian, M., Lashkari, A. H., & Hakak, S. (2023). IoT Malware Analysis Using Federated Learning: A Comprehensive Survey. *IEEE Access*, *11*, 5004–5018. https://doi.org/10.1109/ACCESS.2023.3235389

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, *83*, 313–331.