EasyChair Preprint

№ 11295

Data Exfiltration Detection

Lasya Kanchimreddy, Bhavya Sri Ananthaneni,
Mounika Rajulapati and R Akshaya

November 15, 2023

Data Exfiltration Detection

Kanchimireddy Lasya
Kalasalingam University
Dept. of Computer Science and Engineering
Srivilliputhur, Krishnankoil, India
9921004312@klu.ac.in

Ananthaneni Bhavya Sri
Kalasalingam University
Dept. of Computer Science and Engineering
Srivilliputhur, Krishnankoil, India
9921004827@klu.ac.in

R. Mounika
Kalasalingam University
Dept. of Computer Science and Engineering
Srivilliputhur, Krishnankoil, India
9921004601@klu.ac.in

R. Akshaya
Kalasalingam University
Dept. of Computer Science and Engineering
Srivilliputhur, Krishnankoil, India
99210041498@klu.ac.in

ABSTRACT:

Despite the fact that DNS was first developed by Pavel Mockapetris in 1983 and hasn't been significantly modified since, it still meets the exact requirements of RFC 882. Because packages span a few hosts, networks, and eventually the Internet, they also want to span a few administrations. Limits and associated operating methods (protocol and statistics format, etc.) combine with the number of sources (including mailboxes), the number of supported locations, and the diversity of these environments to create a consistent way to relate to precise sources that are comparable but scattered over the environment. If you want to motivate a powerful problem, Dan Kaminsky, a well-known DNS protection researcher, describes DNS as a globally deployed community that interconnects each private and non-private Internet. This causes extreme problems. Is DNS secure enough? Are you vulnerable to statistics breaches? The solution is that DNS can be used as a backdoor for hackers looking to steal sensitive statistics.

Keywords – Data exfiltration,

INTRODUCTION

The use of Domain Name Systems (DNS) is becoming increasingly popular as a means of data exfiltration, either through the use of malware-infused devices or the use of malicious insiders. The most recent DNS safety survey found that forty-six percent of respondents had experienced exfiltration, and forty-five percent had experienced DNS tunneling, which involves the tunneling of IP Protocol site visitors through DNS port 53, which is no longer regularly monitored by firewalls or other advanced technology. The types of data that are most likely to be stolen include personally identifiable information (PII), social security numbers, regulated data related to the Payment Card Industry (PCI) and HIPAA compliance, and intellectual assets that provide an agency with an unfair advantage. Other sensitive data, such as credit score card numbers, corporate financials and payroll statistics, as well as emails, can also be encrypted and embedded in DNS. The reasons for doing this can range from cybercrimes like hacking and spying to financial crimes, where you can make a lot of money without having to worry about the hassle of dealing with the underground market.

DNS as a transport protocol:

Most organizations have implemented multiple layers of protection mechanisms, including next-generation firewalls, IDSs, and IPSs. However, hackers can exploit the DNS protocol to bypass these carefully crafted security measures. The DNS protocol, which has been in existence for over 30 years, is both trusted and vulnerable to attacks from hackers and malicious insiders. To fully comprehend this vulnerability, it is crucial to understand the structure of DNS messages.

DNS messages can be categorized into two types: queries and replies, both of which follow the same format. Each message consists of a header and four sections: question, answer, authority, and additional. The "flags" field in the header controls the content of these sections, but the overall structure of all DNS messages remains the same.

Various elements and parameters within the DNS have specific length limits, which are listed

below. While some of these limits can be easily modified, others are more fundamental. This presents an opportunity for hackers to exploit the DNS protocol. They can utilize the base 512 octets available in UDP messages to "encode" data and avoid detection. Additionally, hackers can embed signaling data or use light encoding techniques within the labels or names areas, allowing them to evade detection and carry out their malicious activities. Data exfiltration through DNS can involve inserting a lengthy string in either the names section (up to 255 octets) or the UDP messages section (up to 512 octets), formatted as a question, and then sending it to a malicious DNS server that logs the query. Hackers deploy a call server that has question logging enabled, serving as the "trap server" for the sensitive data being stolen. This call server runs a basic installation of BIND and is accessible from the Internet. It can also be hidden behind a cable modem, as long as port 53 is forwarded to it. Additionally, cybercriminals may employ other clever techniques such as ID tagging and sequence numbering. These techniques are particularly useful for tagging transactions, such as credit card purchases, where the sequence of events can reveal important information like names, numbers, or card verification values (CVV). The FrameWorkPOS malware is especially adept at exploiting this. Despite the potential for a large number of DNS queries being sent out during an exfiltration attempt, it may seem like a simple task to detect and intercept this method of transport. However, thieves are skilled at evading detection. They employ tactics like slow drip, which sends queries at a deliberately slower pace to avoid triggering alerts by keeping the volume of queries low. Another technique they use is source IP spoofing, where the source IP address is altered in the queries to make it appear as if the queries are coming from multiple different clients. While proper network security measures should be able to detect this on the transfer port, it is surprising how often these methods still succeed.

Data Exfiltration Strategies:

When it comes to data exfiltration, the most effective approach is often the simplest. Many organizations are not adequately prepared to counter exfiltration attempts, as their security measures primarily focus on perimeter protection. However, it is crucial to start from the assumption that persistent attackers may gain access and to develop strategies for detecting and disrupting their activities, particularly their efforts to compromise data assets once they have established a presence. The most common methods of exfiltration involve outbound FTP or HTTP/HTTPS connections, accounting for over 50% of the data breach incidents analyzed. These methods blend in with normal network traffic, making it difficult to distinguish them from legitimate user activities. Attackers employ various strategies for exfiltrating data, ranging from indiscriminate file dumps that take the data offline for later analysis or processing, to meticulous filtering to extract only the most relevant and valuable information.

LITERATURE REVIEW

Our research details the attack vectors utilized to exfiltrate data, whereas all previous reviews have focused on the difficulties in preventing or mitigating data exfiltration. When we refer to problems, we mean things like many channels of leakage, controlling access rights, encryption, and steganography. An attack vector is a specific way or technique used to exfiltrate data, such as phishing, SQL injection, and passive monitoring; The current reviews offer some insights on insider assaults and unintended data leaking, but their scope is not well defined. Nevertheless, our analysis offers insight into data exfiltration brought on by malevolent actions of a remote attacker rather than any specifics of that kind. Although insider attack vectors may also be addressed by some of the solutions, our study does not include such attacks. We also take into account the fact that data exfiltration is a wide field of study and that a variety of devices, including PCs, smartphones, web servers, databases, virtual machines, printers, networks, and Internet of Things sensors, might leak data. As a result, it is difficult to incorporate papers from every field. Consequently, this review's purview is restricted to data exfiltration from networks, virtual machines, web servers, databases, and PCs.

METHODOLOGY

Data exfiltration detection is of utmost importance in maintaining data security and preventing data breaches within an organization. The process involves a combination of techniques and strategies to effectively identify and respond to potential data breaches.

To begin with, network and endpoint monitoring is essential. Continuous monitoring of network traffic, system logs, and endpoint devices allows organizations to identify potential data breaches. By scrutinizing data flows for anomalies, such as

unexpected or large data transfers to external locations, organizations can establish baselines of typical network behavior and recognize deviations that may indicate data exfiltration attempts.

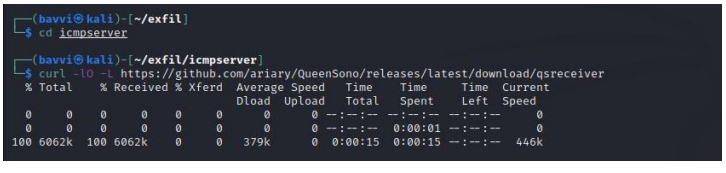
In addition, log analysis plays a crucial role in data exfiltration detection. Security information and event management (SIEM) systems can collect and analyze logs from various sources, including firewalls, intrusion detection systems, and servers. By correlating events and patterns in these logs, organizations can identify unusual activities, such as repeated login failures or suspicious file access.

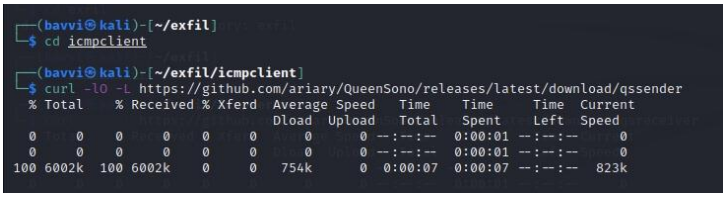
Anomaly detection is another valuable method for identifying data exfiltration. By utilizing machine learning algorithms and behavior analytics, organizations can detect deviations from normal user or system behavior. These techniques can uncover patterns that human analysts might overlook. For instance, if an employee who typically accesses certain files suddenly attempts to access sensitive data they have never interacted with before, it could be an indication of data exfiltration.

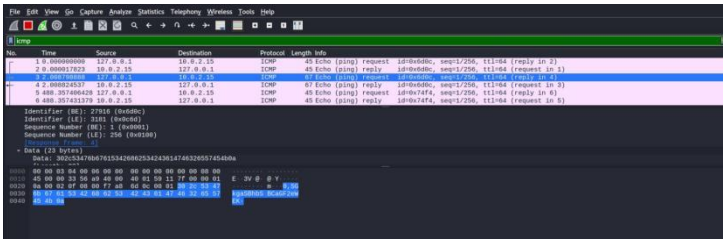
Furthermore, data loss prevention (DLP) solutions play a critical role in data exfiltration detection. These tools enable monitoring, control, and blocking of the transfer of sensitive data, both within and outside the organization. They can effectively identify attempts to send sensitive information through email, messaging apps, or file-sharing platforms.

In conclusion, the detection of data exfiltration requires a comprehensive approach that includes network and endpoint monitoring, log analysis, anomaly detection, and the implementation of data loss prevention solutions. By employing these techniques and strategies, organizations can enhance their data security and mitigate the risk of data breaches.

OUTPUT:







CONCLUSION

A comprehensive cybersecurity strategy necessitates the critical component of data exfiltration detection. This involves a multi-faceted methodology that integrates network monitoring, log analysis, anomaly detection, data loss prevention, endpoint security, user behavior analytics, and continuous monitoring. By employing these techniques and technologies, organizations can identify potential data breaches, thwart data exfiltration attempts, and respond swiftly to mitigate the impact of any successful breaches. User training and awareness also play a crucial role in this methodology, as employees can serve as an extra layer of defense in recognizing and reporting suspicious activities. Ultimately, an effective data exfiltration detection methodology helps safeguard sensitive data, protect an organization's reputation, and maintain data

security in an ever-evolving threat landscape.

References:

[1] Al-Shaer, E., & Haider, Z. (2005). Packet-level traffic analysis for worm detection and characterization. In Proceedings of the 15th international conference on World Wide Web (WWW) (pp. 26-34).

[2] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (NIST special publication 800-145). National Institute of Standards and Technology.

[3] Dain, O., Bilar, D., & Zhang, H. (2011). Towards an understanding of anti-forensics behavior. In Proceedings of the 8th international conference on Autonomic and Trusted Computing (ATC) (pp. 192-203).

[4] Kuhn, M. G. (2007). Exfiltration channels: A field guide to post-insider threat data exfiltration. In Proceedings of the 2nd international conference on Information systems security (pp. 58-70).

[5] Karim, A., Manogaran, G., & Lopez, D. (2018). The role of big data and cloud computing in data and information security. Journal of King Saud University-Computer and Information Sciences.

[6] Gao, L., & He, Q. (2017). A survey of big data architectures and machine learning algorithms in the healthcare sector. Journal of King Saud University-Computer and Information Sciences, 30(4), 431-438.

[7] Vigna, G., Robertson, W., Balzarotti, D., Kruegel, C., & Kirda, E. (2004). Detecting malicious software by behavioral windows. In Proceedings of the 12th ACM conference on Computer and Communications Security (CCS) (pp. 261-270).

[8] Shishika, D., Alzhrani, K., & Erbad, A. (2019). A survey of machine learning and deep learning models for zero-day malware detection. IEEE Access, 7, 164380-164402.

[9] Stolfo, S. J., Fan, W., Lee, W., Prodromidis, A., & Chan, P. K. (2000). Cost-based modeling for fraud and intrusion detection: Results from the JAM project. In Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX) (Vol. 2, pp. 130-144).

[10] Zanero, S., & Toporkov, A. (2005). Honeyd: A virtual honeypot daemon. In Proceedings of the 12th USENIX Security Symposium (pp. 1-14).

[11] Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

[12] Bishop, M. (2003). Computer Security: Art and Science. Addison-Wesley.

[13] Filar, B., & Brodsky, A. (2006). A taxonomy of data leakage. In Proceedings of the 6th Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop (pp. 194-200).

[14] Carvalho, T., Alves, S., Silva, L., & Morais, F. (2015). A survey on insider threats: Concepts, detection techniques, and case studies. Computers & Security, 51, 16-33.

[15] Liu, D., & Jia, C. (2012). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.

[16] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of network-based defense mechanisms countering the DoS and DDoS problems. IEEE Communications Surveys & Tutorials, 15(4), 2046-2069.

[17] Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media.

[18] Sood, A. K., Enbody, R., & Bansal, D. (2013). Malware phylogeny generation using permutations of code. In Proceedings of the 28th Annual ACM Symposium on Applied Computing (SAC) (pp. 1084-1089).

[19] Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2010). Learning and classification of malware behavior. In Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF) (pp. 108-125).

[20] Shabtai, A., Moskovitch, R., & Elovici, Y. (2014). Detection of malicious code by applying machine learning classification algorithms on static features: A state-of-the-art survey. Information Security Technical Report, 16(4), 4-18.