**Moving Target Defense: A Powerful Solution to Ransomware Attacks**

**Mark Kardash**

**Briefing Paper**

**WRTG393**

**Executive Summary:**

One of the biggest issues in information technology today is the struggle to keep data safe. For every defense against cyberattacks, there seems to be some virus or malware designed to circumvent it. This leads to a constant race between hackers and developers, with each group always having to think one step ahead of the other. And while software security may be a concern as old as computers themselves, every year brings a new, powerful threat. And today, a dangerous culprit known as ransomware is growing in popularity. This technique has the purpose of demanding finances from companies as ransom, in exchange for which they will supposedly provide the “antidote” to the attack, be it code or an encryption key. However, understandably, this does not always happen, and the criminals often vanish undetected. In the sections below, I address the rapidly growing problem of ransomware, breaking down its nature, listing its consequences to businesses, and proposing off-network data storage as a potential solution.

**The Problem**

**Graphical user interface, text, application

Description automatically generated**

As defined by DeVry University, ransomware is “a type of malware ("malicious software") used by cybercriminals to… restrict the victim's data by encrypting it and then demanding a ransom payment in exchange for access to the data again.” (Para. 5). While the practice itself is not particularly new, it has recently begun growing in popularity because of more employees working remotely after the COVID-19 pandemic. The widespread use of cryptocurrency has also fueled its rise. In fact, ransomware attacks have seen a whopping 62% rise between January and July 2021, as reported by the United States Cybersecurity and Infrastructure Security Agency (CISA) (cisa.gov). The process of such an attack is a very simple one: Through an infected website, email or application, the criminal launches an assault on the company’s system, after quickly making their demands known to the victim (often through a digital note), including the amount and method of payment (Hull et al, 2019). The company then has a certain amount of time to meet these demands, to regain access to its data. But even doing everything the criminals have told them to does not guarantee a safe resolution, as, after the sum is handed over, the hackers have no reason to keep their word. Just in the January-July 2021 period cited previously, ransomware attacks cost companies over $16.8 million (Cisa.gov). Such losses have employers and developers constantly on guard, utilizing many tools and techniques to prevent them. Most of these solutions focus on recovering the data impacted by the hackers. Some businesses, for example, utilize what is known as Solid State Drive (SSD), which erases data from its original source after copying it to another (McIntosh et al, 2022). While independent from the original operating system, and able to stop ransomware from progressing even in the most advanced stages, SSD is not the most effective defense measure. This is mostly due to its inaccuracy when distinguishing between latest “clean” and infected files, as well as inability to provide enough information on the nature of the attack (McIntosh et al, 2022). Another solution involves copying not the data itself, but the keys needed to decrypt it should a hacker strike, in the hopes of extracting them later. Once again, this may be effective in some cases, but has plenty of shortcomings, being easily circumvented by most ransomware, depending on specific platforms, and potentially becoming a threat themselves, by introducing an infected key. Furthermore, the frequent use of the technique by various applications may require companies to thoroughly pick which of them to use, taking up valuable time (McIntosh et al, 2022). To spare Lawn & Order of such problems, I shall present below a more effective way of protecting our company’s database.

**Potential Solution**

**Text

Description automatically generated**

After reading multiple articles, and comparing various methods of protection, I have concluded that the best way for Lawn & Order to address ransomware attacks would be to implement a tactic known as Moving Target Defense (MTD). Its advantage over unreliable data backing practices is that MTD essentially randomly mixes files in a system (Which is known as shuffling) to “confuse” the malware attacking it, and increase the criminals’ expenses (Lee et al, 2019). For a hacker trying to strike their target and get away with it as fast as possible, this is a major problem, and will very likely force them to quit their attempt. MTD is not only a component in many software security methods today but has also proven to be quite powerful. The reason for this is that this protection “assumes strong adversaries who continuously try to search and encrypt the target extension files. However, currently, most ransomware only searches and encrypts the target extension file at one brush and asks for money.” (Lee et al, 2019, 4.3., para.2). The people who developed MTD were therefore thinking one step ahead of potential perpetrators, something that is so needed today.

When it comes specifically to Lawn & Order’s database, we could protect it by using Moving Target Defense to automatically change the extensions of computer files, thus concealing valuable files from hackers.The new extensions the files receive do not even have to be existing ones. In fact, it is much safer if fictional extensions are used. For instance, MTD may “convert” a .pdf file into a “.dwo” file. Since no such extension actually exists, the malware attacking the system will fail to properly encrypt it, while our operating systems will match each of the files with the corresponding program needed to open it (Lee et al, 2019). In this way, the attackers will once again have wasted time and resources, while our data will remain saved and protected. The strategy of confusion described above makes MTD a very reliable protection for companies like ours. When used alongside other techniques, such as data backup, it can significantly lower the chances of a cyberattack, and, even if one does happen, can prevent significant financial losses. Along with that, it can prevent things like identity theft and customer dissatisfaction, that may come with such a system breach.

**Summary**

Although not that recent, ransomware is a dangerous and rapidly expanding cybersecurity threat. Its main goal is to extort monetary payment from businesses after infecting their databases. It causes significant losses, both financial and data-related to companies and customers every year. Payment of the ransom does not guarantee data decryption, motivating developers to constantly work on new ways to counteract the scheme. Although backing up data and keys on a separate device is a popular preventive measure, it has a variety of issues, especially when the device is system dependent. Moving Target Defense (MTD) is a protection that changes the extensions of important files in the database to non-existent ones, in order to confuse the malware attacking it, leaving it to operate “in the dark”. This wastes the expenses and time of the attackers, forcing them to abandon their criminal operation. I believe Lawn & Order Services could benefit from such a solution because it leaves the critical elements unnoticed by perpetrators. This not only prevents monetary and data loss, but also decreases the possibility of criminals striking again in the future, thus increasing customer trust in the company.

References:

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: Views from a predictive model and human responses. Crime Science, 8(1). <https://doi.org/10.1186/s40163-019-0097-9>

Lee, S., Kim, H. K., & Kim, K. (2019). Ransomware protection using the moving target defense perspective. Computers & Electrical Engineering, 78, 288-299. <https://doi.org/10.1016/j.compeleceng.2019.07.014>

McIntosh, T., Kayes, A. S., Chen, Y. P., Ng, A., & Watters, P. (2022). Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. ACM Computing Surveys, 54(9), 1-36. <https://doi.org/10.1145/3479393>

Ransomware awareness for holidays and weekends. (2021, August 31). CISA. Retrieved December 13, 2022, from <https://www.cisa.gov/uscert/ncas/alerts/aa21-243a>

What is ransomware? (2022, November 15). devry.edu. <https://www.devry.edu/blog/what-is-ransomware.html>