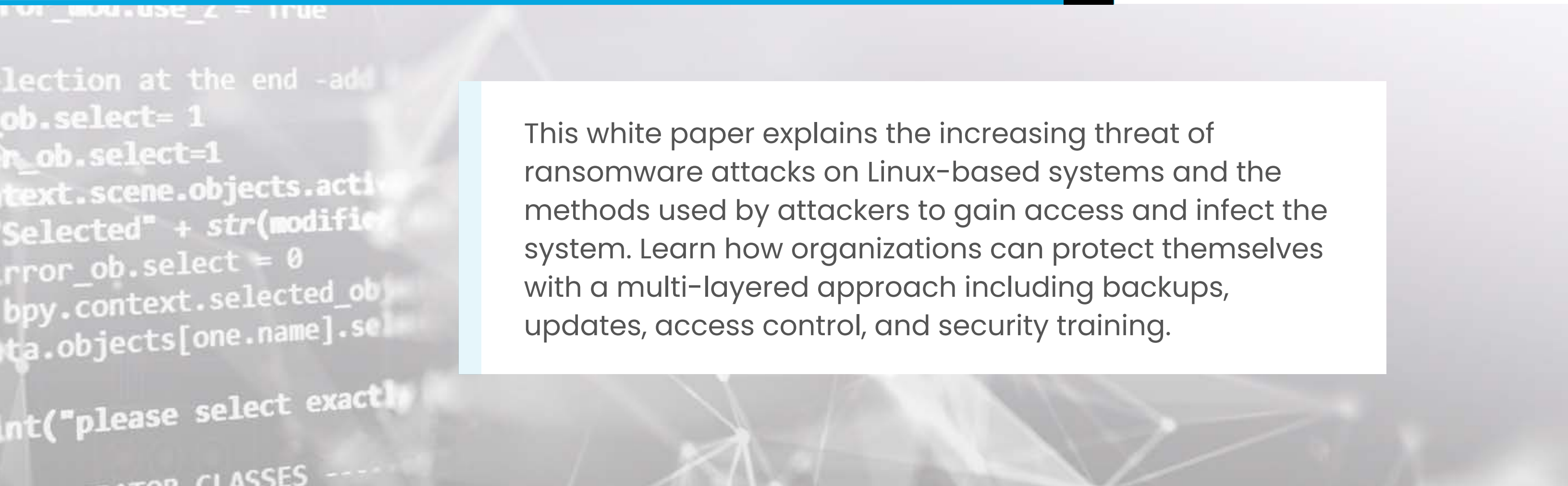
www.VectorUSA.com

VECTORUSA

WHITE PAPER

THE GROWING THREAT OF RANSOMWARE ON LINUX-BASED SYSTEMS



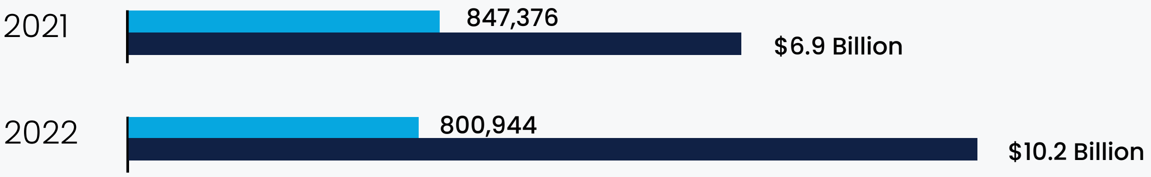
This white paper explains the increasing threat of ransomware attacks on Linux-based systems and the methods used by attackers to gain access and infect the system. Learn how organizations can protect themselves with a multi-layered approach including backups, updates, access control, and security training.

Introduction:

In recent years, ransomware attacks have become a major threat to businesses of all sizes. Traditionally, these attacks have targeted Windows-based systems, but as Linux-based systems have become more common, cybercriminals have turned their attention to these platforms. While Linux has long been considered more secure than Windows, recent ransomware attacks on Linux-based systems have demonstrated that no system is immune to cyber-attacks. This white paper will explore the growing threat of ransomware on Linux-based systems, and what organizations can do to protect themselves against these attacks.

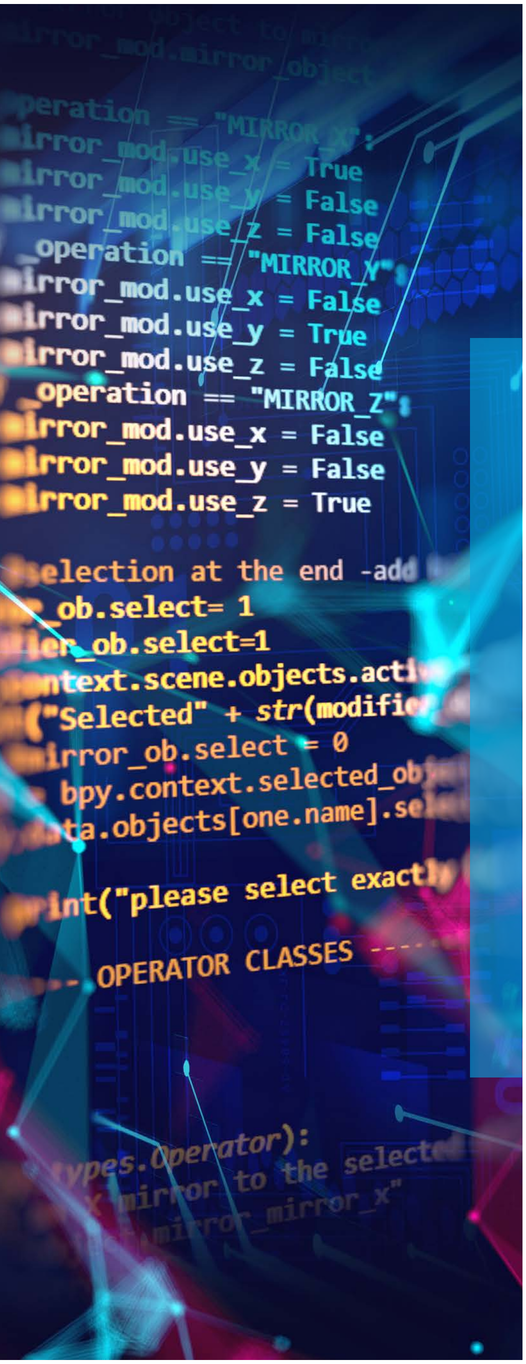
Background:

Ransomware[1] is a type of malicious software that encrypts files on a victim's computer, rendering them inaccessible. The attacker then demands payment, typically in the form of cryptocurrency, in exchange for the decryption key. Ransomware attacks have become increasingly sophisticated in recent years, with attackers using a variety of techniques to evade detection and infect systems. According to the 2022 report by IC3[2], there was a 5% reduction in cyber incident complaints received, with 800,944 complaints reported compared to the previous year. Nonetheless, the report indicates a substantial increase in the potential total loss, rising from $6.9 billion in 2021 to over $10.2 billion in 2022.



Linux-based[3] systems have long been considered more secure than Windows-based[4] systems, due in part to their open-source nature and the ability for users to control and modify the code. However, as Linux has become more popular and its use has expanded beyond servers and data centers, cybercriminals have begun to target these systems with ransomware attacks.

Ransomware Attacks on Linux-Based Systems:



Ransomware attacks on Linux-based systems have been increasing in frequency and sophistication in recent years. In some cases, attackers have exploited vulnerabilities in the software, while in others they have gained access to the system through social engineering attacks[5] or weak passwords. Once the attacker gains access to the system, they can use a variety of techniques to infect the system with ransomware.

Attackers often disguise ransomware as legitimate updates or patches, particularly on Linux-based systems that require frequent updates. An example of this is the Microsoft ransomware[6] disguised as a patch which exploited the "PrintNightmare" vulnerability, allowing remote code execution on Windows systems. This highlights the importance of organizations staying vigilant, implementing multi-layered security, and applying the latest patches to protect against ransomware attacks.

Another method used by attackers is to exploit vulnerabilities in third-party software that is running on the system. This can include web servers, databases, and other applications that are commonly used on Linux-based systems. By exploiting these vulnerabilities, attackers can gain access to the system and install ransomware. The SolarWinds supply chain breach[7] compromised US government agencies & private companies via supply chain compromise. Attackers inserted malicious code into software updates to gain access to networks & exfiltrate data. This is just one example of a third-party attack that can impact developers, partners, customers or acquisitions.

Protecting Against Ransomware on Linux-Based Systems:

To protect against ransomware on Linux-based systems, organizations should take a multi-layered approach to security. This should include:

☑ **Regular backups:** Regular backups of critical data and systems can help mitigate the impact of a ransomware attack. Backups should be stored offline or in a separate, secure location to prevent them from being encrypted along with the rest of the system.

☑ **Patching and updates:** Keeping software up-to-date with the latest security patches and updates is critical to preventing attacks that exploit known vulnerabilities.

☑ **Access control:** Limiting access to sensitive systems and data can help prevent attacks that rely on weak passwords or social engineering techniques.

☑ **Antivirus and anti-malware software:** Installing antivirus and anti-malware software on Linux-based systems can help detect and block known ransomware threats.

☑ **Security awareness training:** It is noteworthy that a significant proportion of data breaches involve human elements and phishing[8], which is one of the most prevalent forms of social engineering attacks. To prevent social engineering incidents, educating individuals about the risks of ransomware and equipping them with the necessary skills to identify and respond to potential threats is critical.

Conclusion:

As the use of Linux-based systems continues to grow, it is important for organizations to recognize the evolving threat landscape and take steps to protect themselves against ransomware attacks. This includes implementing a strong security posture, regularly updating and patching software, and educating employees about the risks of social engineering attacks. Another important step that organizations should take to enhance their security posture is to implement multi-factor authentication (MFA) to add an extra layer of protection against unauthorized access.

By implementing a multi-layered approach that includes regular backups, patching and updates, access control, antivirus and anti-malware software, and security awareness training, organizations can help mitigate the risk of a ransomware attack. Additionally, organizations should consider working with a trusted cybersecurity partner to develop a comprehensive ransomware response plan that can help them quickly detect and respond to attacks. A cybersecurity partner, can also guide organizations through the process of rolling out MFA and help ensure that it is implemented correctly to maximize its effectiveness in preventing cyber-attacks. By staying vigilant and proactive, organizations can help protect their critical systems and data from the devastating effects of a ransomware attack. While no system is completely immune to cyber-attacks, taking these steps can help ensure that an organization can improve its overall cybersecurity posture and better defend itself against potential threats.

Endnotes

1 https://www.cisa.gov/stopransomware/resources
2 https://www.ic3.gov/
3 https://www.linux.com/what-is-linux/
4 https://computerstudypoint.com/windows-operating-system/
5 https://www.techradar.com/features/social-engineering-attacks-explained
6 https://www.theverge.com/2021/7/6/22565868/microsoft-printnightmare-windows-print-spooler-service-emergency-patch-hotfix
7 https://www.helpnetsecurity.com/2021/01/15/third-party-hacks-solarwinds-breach/#:~:text=That%20said%2C%20a%20compromise%20of%20a%20supplier%20is,Developers%2C%20partners%2C%20customers%2C%20or%20potential%20acquisitions%20are%20examples.
8 https://www.helpnetsecurity.com/2021/01/15/third-party-hacks-solarwinds-breach

About Us:

CELEBRATING 35 YEARS VECTORUSA
PIONEERING INNOVATIVE SOLUTIONS FOR 35 YEARS

At VectorUSA, we are dedicated to delivering top-notch cybersecurity solutions tailored to your organization's unique needs. Our team of experts work closely with you to provide comprehensive protection for your technology infrastructure, offering a sense of security and peace of mind. Our customized security planning and implementation eliminate risks and exposure to cyber threats during your digital transformation. Count on us to safeguard your organization from malicious attacks, so you can focus on your core business operations. To learn more, visit us at VectorUSA.com.

General Information: **800.929.4516**

Customer Service: **877.569.8800**