MAY 31, 2022 / EDUCATIONAL / INFORMATION TECHNOLOGY

The Rise of Ransomware: A Deep Dive into the Latest Threats

The evolution of cyber threats has been marked by ransomware's rapid growth and sophistication. But, if you think ransomware attacks only happen to big corporations, think again.

Small businesses are just as susceptible to these threats. The rise in remote work and online transactions has made it easier for hackers to target anyone with valuable information.

This article delves into the latest trends and developments surrounding ransomware threats while examining their impact on various industries, as well as steps to overcome future ransomware attacks.

Ransomware In A Nutshell

Ransomware is a form of malware that encrypts the victim's data and demands payment for its release, often within a specified time frame, or risks losing access to it permanently.

The sophistication and prevalence of ransomware attacks have increased significantly over time, with high-profile incidents impacting various sectors, including healthcare, government organisations, and private businesses.

For instance, 62% of Malaysian financial services organisations recovered from ransomware attacks in a week. Across all sectors, that would be an average of 32%2.

The Growing Trend Of Ransomware Attacks

The trend of ransomware attacks has been growing rapidly, and it doesn't seem to be slowing down anytime soon. The State of Ransomware 2022 report indicates that a significant percentage of Malaysian organisations, namely 79%, have experienced ransomware attacks3.

One reason for the growth of ransomware attacks is the ease with which they can be executed. Hackers can use off-the-shelf malware and exploit kits to launch these attacks, making targeting a wide range of systems easier.

Another reason is the potential for high payouts, while at the same time executing such attacks has been becoming less expensive. Hackers can demand significant sums of money in exchange for unlocking the victim's data or systems, and many organisations are willing to pay to avoid disruption and potential harm to their reputation.

The increasing use of cryptocurrency has also fueled ransomware attacks. Hackers often demand payment in cryptocurrency, such as Bitcoin, because it is difficult to trace and provides anonymity. This has made it easier for hackers to collect ransom payments without being caught.

With limited options available post-attack, many victims ultimately pay the demanded ransom out of desperation, encouraging further criminal activity.

Notable Ransomware Attacks In 2022

Cisco Attack

The Cisco attack1 on 24 May 2022 demonstrated the evolving tactics employed by ransomware gangs to infiltrate even the most secure organisations.

Yanluowang, a notorious ransomware group, successfully accessed an employee's credentials via a compromised personal Google account and launched a voice phishing campaign to bypass multi factor authentication settings.

Macmillan Publishers Attack

In the Macmillan Publishers attack4 on 28 June 2022, threat actors infiltrated the company's network, encrypting essential files and disrupting its ability to accept process or ship orders. As a result, employees could not access their emails, and operations came to a standstill.

As one of the leading publishing companies with a global presence across over 70 countries, Macmillan serves as another example demonstrating that even well-established businesses are not immune from ransomware attacks.

Rackspace Technology Attack

The Rackspace Technology ransomware attack5 on 2 December 2022 further underscores the pervasive threat such incidents pose to organisations across industries and sizes.

As a prominent cloud service provider, Rackspace experienced significant outages and disruptions to its Hosted Exchange services following a security incident later confirmed as a ransomware attack.

This event involved an innovative exploit method known as 'OWASSRF,' which bypasses mitigations for ProxyNotShell vulnerabilities in Microsoft Exchange Server, demonstrating the evolving nature of cyber threats.

Tactics Used By Cybercriminals To Distribute Ransomware

Phishing Attacks

Phishing attacks often involve emails, links, or websites that appear to be from a trusted source, convincing individuals to reveal sensitive information such as login credentials and financial data.

Threat actors may employ sophisticated techniques like spear-phishing, where personalised messages are crafted based on publicly available information about the targeted individual or organisation.

In addition, phishing links, often disguised within seemingly innocuous emails or messages, lure unsuspecting users into clicking on them and subsequently downloading malware onto their systems.

Exploit Kits

Exploit kits are toolsets to identify and capitalise on vulnerabilities within a target's software or operating system. Once these weaknesses have been exploited, the door is opened for attackers to deliver and install ransomware onto the compromised systems.

One of the most common ways to distribute exploit kits is through malvertising. Cybercriminals will purchase ad space on legitimate websites and then use the ad to deliver the exploit kit to unsuspecting users.

Encryption Complexities

Attackers often use advanced encryption algorithms, like RSA or AES, to make it more difficult for victims to crack the encryption and regain access to their data. Some attackers use such strong encryption that even law enforcement agencies cannot break it without the proper decryption key.

In some cases, threat actors may also employ multiple layers or combinations of encryption methods to extort victims more effectively.

Cybersecurity Measures In Preventing And Mitigating Ransomware Attacks

Regular Data Backups

Regular data backups are among the most critical cybersecurity measures in preventing and mitigating ransomware attacks. This means making copies of your data and storing them in a separate location, such as an external hard drive or a cloud-based service.

It's important to note that backups should be done regularly and automatically. This ensures that you always have the latest version of your data and reduces the risk of data loss or corruption.

Multi-Factor Authentication

Multi-factor authentication, or MFA, provides an added layer of security by requiring users to verify their identity through multiple methods, such as a combination of passwords, biometrics, or unique verification codes sent via email or text message.

This approach makes it more difficult for cybercriminals to gain unauthorised access to sensitive systems and data since they would need to compromise several different authentication factors simultaneously.

Employee Training & Awareness

Employee training and awareness programs play a critical role in preventing and mitigating ransomware attacks. These educational initiatives seek to equip staff members with knowledge of cybersecurity best practices, threat identification, and incident reporting procedures.

With such initiatives, employees become more vigilant in recognising phishing emails, suspicious attachments, or malicious links, often serving as entry points for ransomware infections.

At Grayscale, we are committed to helping organisations protect their data and operations from ransomware threats by providing comprehensive cyber defence solutions tailored to meet their unique security needs. This also includes training and awareness programs for employees to ensure they are well-equipped to recognise and respond to potential cyber threats.

Contact us by email at **enquiries@grayscale.my** for more information on how we can help your organisation stay secure.

APRIL 26, 2022 / EDUCATIONAL / INFORMATION TECHNOLOGY

Cybersecurity : A Necessity for Organisations

SEPTEMBER 26, 2022 / BUSINESS / EDUCATIONAL / MARKETING

Grayscale Hosts Cybersecurity Workshop for Government Agencies

MAR 31, 2022 / EDUCATIONAL / INFORMATION TECHNOLOGY / UNCATEGORIZED

Internet of Things (IoT) Security: A Critical Need for the Future

Leave a Reply

Your email address will not be published. Required fields are marked *

Your Comment *

Your Name *

Your Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

A subsidiary under TechnoDex Group of Companies.

Unit E-07-03, Menara Suezcap 2, KL Gateway, No. 2, Jalan Kerinchi, 59200 Kuala Lumpur, Federal Territory of Kuala Lumpur

T: +603 7932 0111

E: enquiries@grayscale.my