THE EVOLUTION OF RANSOMWARE TACTICS IN 2024

Introduction

Ransomware continues to be a threat to businesses of all sizes in 2024. Early reports show that attacks are up 130% since 2022.[1] No one is immune to these attacks. In 2024 alone, a major airline, multiple health systems, transportation providers, and educational institutions have been breached and subjected to ransomware. In some cases, business continuity plans were ineffective, further compounding financial and reputational loss. Clearly, there are gaps in protection methodologies that need to be addressed, as threat actor tactics have evolved. Let's discuss some of the newer attack methods and tactics.

Ransomware as a Service

A growing number of organizations are using different forms of outsourced services to increase their flexibility and better match their skills with their main goals. With this strategy, they may concentrate on their main goals and leave the peripheral tasks to skilled outside vendors. But thieves have seen this pattern and are starting to imitate it, especially when it comes to ransomware attacks.

Attackers have discovered that by outsourcing the parts of ransomware operations that they are less competent at carrying out themselves, they can increase their efficiency and efficacy. Because of this, a new ecosystem has emerged inside the cybercriminal underground, wherein producers of ransomware produce advanced tools and infrastructure that are intended to be used in attack launches. These developers then offer their creations to "affiliates" who are responsible for carrying out the actual attacks.

Affiliates find this model especially appealing since it offers them little to no upfront cost access to these robust tools and infrastructure. Rather, the developers usually work on a profit-sharing model, keeping a portion of the ransom money that the affiliates can effectively extract. Because of the low entrance hurdle, more criminals can now engage in ransomware assaults, even if they lack the technical know-how to create the malware themselves.

[1] https://www.blackfog.com/the-state-of-ransomware-2024/

Ransomware creators have started using strategies that are similar to those of reputable companies in order to make it easier to attract affiliates. They actively promote their products and services, highlighting the features and advantages of their tools and services, in forums on the dark web and other unofficial channels. These commercials frequently emphasize the product's ease of use, significant profit margin, and developer-provided support system.

There are a lot of similarities between this concept of outsourced ransomware and ethical corporate operations. Similar to how businesses go to specialist service providers to manage specific parts of their operations, ransomware developers' experience is being used by hackers to execute assaults more effectively. This pattern highlights how the world of cybercrime is still changing and how harmful actors' strategies are becoming more and more sophisticated.

It is critical for enterprises to identify this change in the attackers' tactics as they struggle with the growing threat of ransomware attacks. Organizations should strengthen their defenses against ransomware attacks by realizing that these operations are outsourced. This could entail making investments in more sophisticated cybersecurity tools, giving staff members extensive training, and creating incident response plans that take into account the particular difficulties presented by this new round of ransomware assaults.

Multiple Extortion Schemes

Data backups have long been the main line of defense for business owners against ransomware attacks. They frequently discover that the most effective approach to recover control of their systems and lessen the effects of being held captive is to restore them from secure backups. Attackers have, however, adjusted to this tactic by utilizing triple and double extortion schemes.

Double extortion is when hackers steal confidential material from the victim and encrypt it, threatening to make it public if their ransom demands are not satisfied. This strategy puts more pressure on the victim because disclosing private information could result in financial losses, legal repercussions, and harm to one's reputation.

This is furthered by triple extortion, in which the attackers may release the stolen data even after they have been paid the initial ransom. Distributed Denial of Service (DDoS) assaults are another tactic used by attackers to impede the victim's recovery. These attacks overload the organization's network and impair its response capabilities.

Attackers can target partners and clients in addition to the first victim to worsen reputational harm and sour business connections. Stakeholder trust may be lost as a result, and there may be financial consequences.

Organizations need to improve their cybersecurity posture beyond depending just on data backups as ransomware threats continue to advance. It is imperative to implement a multi-layered strategy that includes strong access controls, frequent software updates, staff training, and incident response preparation. Businesses, cybersecurity professionals, and law enforcement agencies can work together and share information to assist firms stay ahead of the always evolving ransomware landscape.

Use of AI and Machine Learning

In today's economic environment, artificial intelligence has become a revolutionary force that is transforming sectors and businesses. Its effects are extensive, ranging from process optimization and improved decision-making to the creation of fresh chances for development and innovation. But as AI develops and becomes more powerful, hackers are also becoming interested in it. They are using AI's potential to create ever-more-complex and catastrophic ransomware attacks.

Hackers are using AI and machine intelligence to propel their ransomware campaigns to previously unheard-of heights[2]. These technologies are being used to develop malware that can avoid detection by security software, craft phishing emails that are extremely targeted and persuasive, and encrypt files at a startling rate. Furthermore, ransomware powered by AI has the capacity to function independently, picking targets and modifying its tactics without the need for human assistance.

[2] https://talkbusiness.net/2023/08/ai-and-ransomware-a-scary-combination/

The emergence of ransomware driven by artificial intelligence presents a serious risk to enterprises across all industries. It emphasizes how critical it is for companies to strengthen their cybersecurity defenses and take a proactive stance to reduce the dangers brought on by this dynamic threat landscape. Businesses need to spend money on strong, multi-layered security measures, update their systems frequently, and warn staff members about the risks posed by ransomware boosted by artificial intelligence.

Staying ahead of AI-driven threats will need a combination of technology improvements, alertness, and teamwork as the battle between cybercriminals and defenders intensifies. Companies need to collaborate closely with cybersecurity specialists, exchange threat intelligence, and constantly modify their approaches to combat the dynamic methods used by malevolent actors. In this quickly evolving digital ecosystem, enterprises can only hope to defend themselves from the disastrous effects of AI-powered ransomware assaults by remaining aware, prepared, and nimble.

Prevention and Response Strategies

Organizations must use a mix of preventive and reactive strategies in line with industry best practices to effectively counter the growing threat of ransomware attacks. Businesses should proactively put in place a strong cybersecurity architecture that consists of ongoing risk assessments, employee education, and the use of cutting-edge security tools like firewalls, intrusion detection systems, and endpoint security. A strong foundation for an all-encompassing security posture can be established by adhering to best practices such as the CIS Critical Security Controls or the NIST Cybersecurity Framework. Reactively, organizations must develop and regularly test incident response plans that outline clear procedures for detecting, containing, and recovering from ransomware attacks. These plans should incorporate best practices such as isolating infected systems, notifying relevant stakeholders, and engaging with experienced cybersecurity professionals to assist in the recovery process. By aligning both proactive and reactive measures with industry best practices, organizations can enhance their resilience against ransomware threats and minimize the potential impact of successful attacks.

Conclusion

In conclusion, the landscape of ransomware continues to evolve, becoming increasingly sophisticated and targeted as we move through 2024. The shift towards personalized phishing campaigns, the exploitation of new vulnerabilities, and the strategic use of legitimate tools underscore the adaptability and persistence of cybercriminals. To effectively combat these threats, organizations can strengthen their defenses by taking the following steps:

1. Act Now | Don't wait for a breach to occur
    a. Take immediate steps to safeguard your critical data and systems
    b. Prioritize cybersecurity to protect your digital future and maintain the trust of your stakeholders
2. Stay Vigilant
    a. Remain proactive in monitoring for threats by regularly updating your cybersecurity protocols
3. Enhance Defenses
    a. Implement comprehensive risk assessments
    b. Adopt advanced threat detection systems
4. Update Incident Response
    a. Ensure your incident response strategies are current and robust
    b. Train your team regularly on new ransomware tactics and recovery procedures
5. Stay Informed | Keep abreast of the latest developments in ransomware and cybersecurity
6. Join the Community
    a. Engage with cybersecurity forums and networks for the latest defense strategies
    b. Share insights and learn from the experiences of others

Assisting your organization in creating a strong defense against ransomware is something that IntraSystems Advisory Division can help with. Reach out today and let's talk!

MEET MERVYN CHAPMAN | Advisory, Cybersecurity/GRC

Mervyn brings over 20 years of experience in Cybersecurity and Information Technology. Currently a Doctoral Candidate in Cybersecurity Innovation Management, he brings a people and process centric perspective to security operations and management. He has served as a Chief Information Security Officer in the Healthcare and non-profit space and as a Principal Consultant within a large nationwide consultancy. He is passionate about user involvement and education as well as crafting business-relevant security policies and processes.

.

MERVYN CHAPMAN

mchapman@intrasystems.com

706.594.1081