CYBERRISKS&LIABILITIES

Ransomware-as-a-Service Explained

Ransomware attacks—which entail a cybercriminal deploying malicious software to compromise a device (or multiple devices) and demand a large payment be made before restoring the technology for the victim—have become a significant concern for organizations across industry lines. In fact, the latest research provides that these attacks have increased by nearly 140% in the past year alone, with the median ransom payment demand totaling $178,000 and the average overall loss from such an attack exceeding $1 million.

A key contributor to this surge is the recent debut of Ransomware-as-a-Service (RaaS). Put simply, RaaS refers to a dark web business model that permits sophisticated cybercriminals to sell their ransomware software to willing buyers (usually less skilled cybercriminals), who then utilize the software to launch an attack and secure a ransom payment.

The RaaS model poses a serious threat to organizations of all sizes and sectors, as it allows cybercriminals of any skill level to execute ransomware attacks on their targets. Review the following guidance to learn more about the RaaS model, its impact on organizational cybersecurity and best practices for addressing RaaS concerns.

What Is RaaS?

Although its purpose is to sell a harmful product, the RaaS model operates quite similarly to a normal business model. First, knowledgeable ransomware developers generate malicious software to be sold. In order to be attractive to buyers, this software must carry a high likelihood of penetration and a minimal risk of discovery.

Once the software has been created and is ready for distribution, it gets launched as a multi-end user infrastructure. RaaS developers then seek potential customers by using typical business marketing methods throughout the dark web—such as advertisements and online forums. Some developers are more selective in who they offer their software to, requiring customers to demonstrate certain technological skills or cybersecurity knowledge, while others are not as strict.

When RaaS developers secure buyers, these customers are usually provided with access to not only the ransomware software itself, but some form of a product portal as well. This portal may include detailed instructions for software implementation, user reviews, support forums and special discounts or offers for future purchases from the developer. Customers may receive permanent access to the software they buy, or only be given an allotted amount of time to utilize it—similar to a rental agreement.

Depending on the developer, RaaS purchases can be a one-time sale or a monthly subscription service. In some cases, RaaS developers don't actually sell their software, but rather recruit other cybercriminals who are willing to launch attacks using the developers' software in exchange for a percentage of the resulting ransom payment. This commission-based partnership is also known as an affiliate program.

Regardless of whether RaaS developers have customers or affiliates, once these cybercriminals receive the developers' software, they can use it to execute ransomware attacks on their targets—potentially resulting in widespread disruption, damaged or destroyed data, reputational repercussions and significant financial fallout for the affected organizations. Well-known RaaS incidents include WannaCry, Cerber, MacRansom, Philadelphia, Atom, Hostman and FLUX.

The Impact of RaaS

Prior to the emergence of RaaS, cybercriminals needed to possess extensive software knowledge and coding capabilities in order to pull off a ransomware attack. In other words, only the most sophisticated cybercriminals could successfully launch such attacks and obtain ransom payments from their victims.

However, the introduction of RaaS to the dark web has allowed cybercriminals of practically any skill level and very little technical ability to accomplish this feat with a simple purchase—contributing to a rapid increase in the frequency of ransomware attacks as a whole.

In addition to attack frequency, cybercriminals involved in RaaS models have become more confident in the strength of their malicious software—thus motivating them to ramp up their ransom payment demands. This is particularly true in the scope of RaaS affiliate programs. Because affiliates only receive a portion of the overall ransom payment following an attack, an elevated payment demand provides them with a larger profit.

That being said, the RaaS model has played a major role in increasing both the frequency and cost of ransomware events in recent years, compounding the expected consequences that affected organizations will face for an already severely damaging form of attack.

Addressing RaaS Concerns

The best way to minimize the growing threat of RaaS concerns at your organization is to make ransomware prevention and response measures a top priority. Remember that ransomware attacks are commonly deployed via phishing emails, deceptive links, dangerous websites, harmful attachments and malicious programs. With this in mind, here are some best practices for combatting ransomware attacks:

- **Secure your systems**—First, it's important to take steps to protect your organizational IT infrastructure from potential ransomware exposures. This may entail:
    - Using a virtual private network (VPN) for all internet-based activities (e.g., browsing and sending emails)
    - Installing antivirus software on all workplace technology
    - Implementing a firewall to block cybercriminals from accessing your organization's VPN
    - Restricting employees' access to websites that aren't secure
    - Establishing email filters to keep phishing messages from reaching employees' inboxes
    - Encrypting sensitive data on all organizational devices and routinely backing up this information
    - Limiting which employees receive administrative controls to prevent inexperienced staff from mistakenly downloading a malicious program
    - Regularly updating all organizational devices and security programs to ensure effectiveness
    - Developing a cyber incident response plan that adequately considers ransomware scenarios and practicing this plan with staff
- **Educate your employees**—Next, be sure to train your employees on how to prevent and respond to a ransomware attack. Give your staff these tips:
    - Avoid opening or responding to emails from individuals or organizations you don't know. If an email claims to be from a trusted source, be sure to verify their identity by double-checking the address.
    - Never click on suspicious links or pop-ups—whether they're in an email or on a website. Similarly, avoid downloading attachments or software programs from unknown sources or locations.
    - Only browse safe and secure websites on organizational devices. Refrain from using workplace devices for personal browsing.
    - If you suspect a ransomware attack, contact your manager or the IT department immediately for further guidance.

For additional risk management guidance and insurance solutions, contact us today.