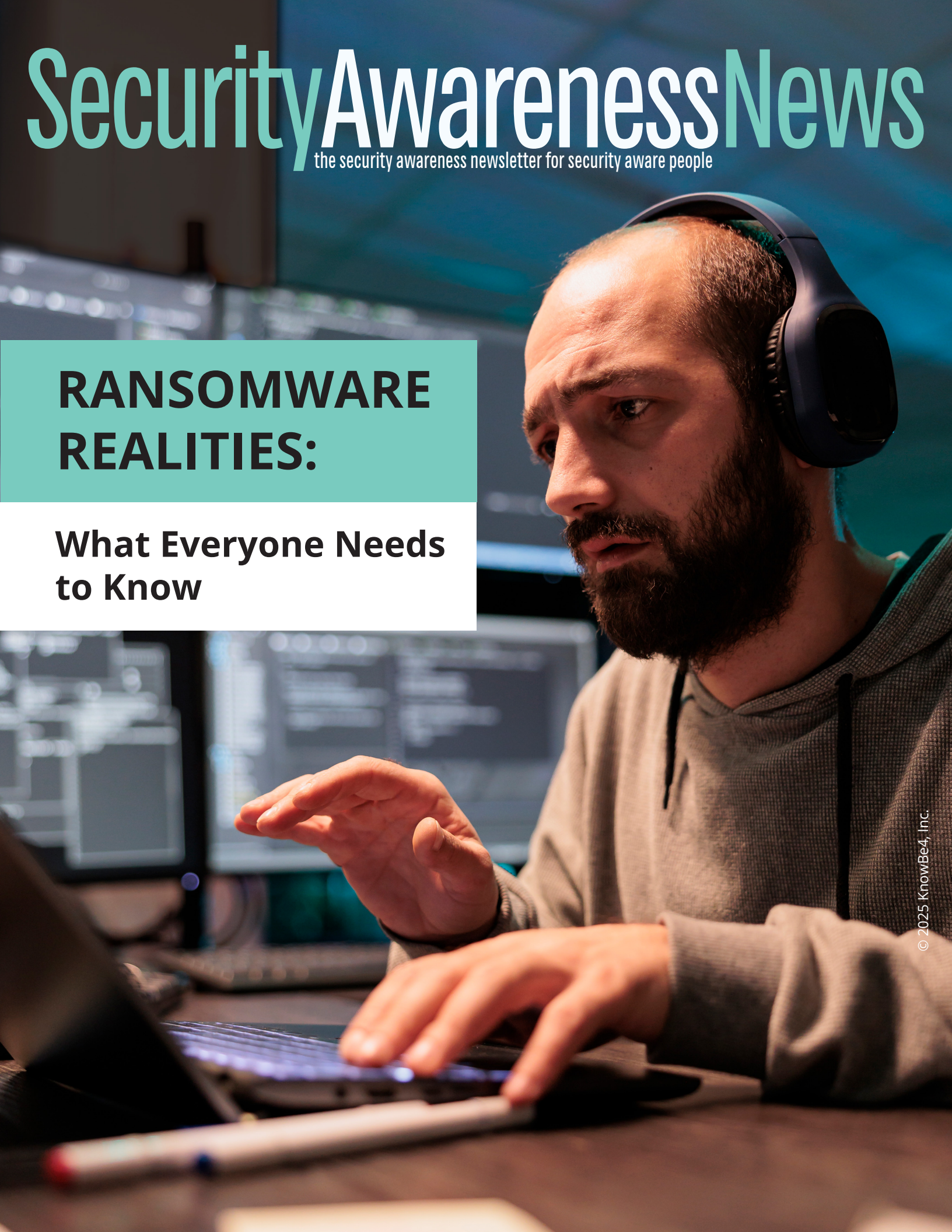
SecurityAwarenessNews

the security awareness newsletter for security aware people



RANSOMWARE REALITIES:

What Everyone Needs to Know

Ransomware In Action

Ransomware is a type of malicious software (malware) designed to **block access to a computer system or files until a large sum of money is paid to the attackers.** Here's how ransomware attacks work:

First comes the exploitation. There are many ways a device can be infected with ransomware, one of the most common being phishing attacks. These attacks use deceptive messaging to convince people to open malicious links or attachments.

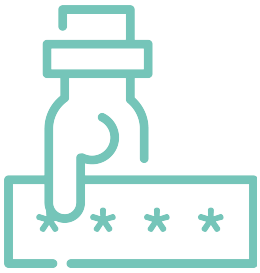
After a device is infected, **the malware seeks out specific files and encrypts them,** often without making its presence known. The encryption process blocks access to crucial assets and resources, bringing operations to a halt. The malware will then display a ransom note on infected devices explaining what happened and how much the target must pay to restore their systems.

All of this adds up to a difficult choice:

1) Pay the ransom, which is often extremely expensive and generally not recommended by law enforcement, or

2) Attempt to recover without paying the ransom, which may take weeks, months, or may not be possible at all.

To make matters worse, some attacks feature a double extortion technique. In this situation, instead of simply encrypting data and asking for payment, the malware first extracts confidential data like passwords and sends it to the attackers. They then threaten to leak it, putting more pressure on the target to pay.



In all cases, what sets ransomware apart from other forms of malware is that it targets one of the most imperative aspects of any organization: availability.

When operations halt, it leads to a loss of revenue and a world of inconvenience. And in the case of healthcare or critical infrastructure like power grids, that inconvenience quickly turns into potentially life-threatening scenarios.

RaaS: The Criminal Enterprise

What follows is an overview of the ransomware business model. It is based on a real-world example of how Ransomware as a Service (RaaS) typically works to show why it's so effective. Let's meet the main players of this criminal enterprise.

Developers

Everything starts with a team of developers who create and maintain strains of ransomware. Part of their job is to constantly update the malware to ensure it's successful and destructive. They also create the decryption keys that unlock data after payment is received.

Customers

Many RaaS organizations don't launch any attacks themselves. It's in their best interest to rent ransomware out to affiliates — the customers that pay a subscription fee to use their services. The affiliates also pay a percentage of each successful ransomware attack.

Access Brokers

Access brokers exist to ensure customer success. These savvy cybercriminals have already compromised several organizations without them knowing. They then sell the access they've acquired to affiliates, who use it to launch attacks without doing much research themselves. After all, why bother spending time trying to hack into an organization when someone has already done all of that work?

Customer Service

Next up is a team of customer service agents. They offer live chat support to help victims send payment and then decrypt their data. Just like any successful organization, RaaS profits rely heavily on strong customer support.

Money Launderers

Another key to long term success is avoiding law enforcement. This is where RaaS organizations turn to money laundering, which is the process of disguising the illegal origin of money. The goal is to take money that was gained illegally through ransomware attacks and make it appear as if it was acquired through legitimate businesses.

By using the RaaS model, ransomware groups can effectively leverage their areas of expertise to ensure a higher rate of success and, by extension, steal more money.

Avoiding Digital Lockdowns

Ransomware infections are disruptive, difficult to recover from, and often expensive. Let's review a few ways you can avoid these digital lockdowns and keep yourself and your organization safe.

Stay Alert for Social Engineering Attacks

Social engineering is the art of manipulating people and tricking them into making mistakes. Phishing scams are one of the most common social engineering attacks you might encounter. They often feature warning signs such as threatening language, urgent requests, and unrealistic promises or scenarios. Stay alert for those signs, and use extreme caution when opening links or attachments.

Keep Software and Firmware Updated

Most organizations have specific policies in place for what gets updated and when. It's essential that you follow these and never install unapproved software or applications. Doing so can lead to unnecessary risk. In your personal life, consider enabling automatic updates on all of your devices.

Use Strong, Unique Passwords

Attackers often leverage automated software that can crack inferior passwords in a matter of seconds. Therefore, it's vital to protect every account with a strong, unique password that is hard to guess and never shared or used for other accounts.

Always Follow Policy

Organizations develop policies to help keep people, data, and assets safe. By always following those policies, you play a key role in avoiding costly security mistakes like ransomware infections.

Report Suspicious Activity Immediately

If you notice anything suspicious, such as a phishing email, report it immediately per your organization's procedures. Timely reporting helps mitigate potential damages and allows organizations to contain dangerous situations.