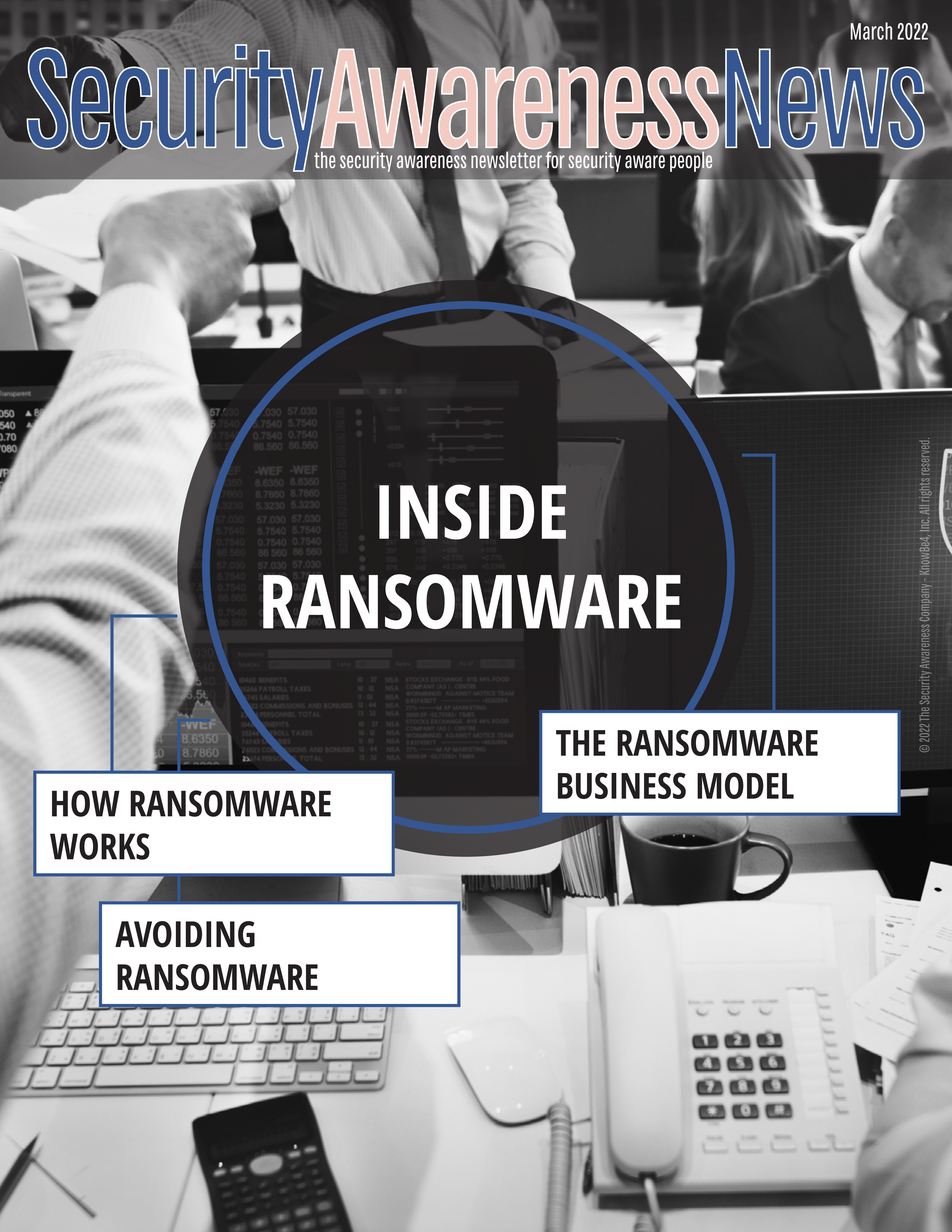
March 2022

SecurityAwarenessNews

the security awareness newsletter for security aware people



INSIDE RANSOMWARE

THE RANSOMWARE BUSINESS MODEL

HOW RANSOMWARE WORKS

AVOIDING RANSOMWARE

HOW RANSOMWARE WORKS

Imagine if someone replaced the locks on your home, preventing you from entering until you paid them a hefty fee. That's the essential concept behind ransomware—a form of malicious software (malware) that encrypts files or systems and denies access to them until a ransom is paid. Here's how it works:

1 INFECTION

Ransomware most commonly finds its way onto computers by someone clicking a malicious link or downloading an infected attachment via phishing emails. Attackers also use stolen login credentials to launch the malware via remote desktop technology, where they gain control of someone's computer remotely.

2 ENCRYPTION

Ransomware encrypts data in a manner that doesn't impact a system's stability. Some variants can spread to other computers on the network and even seek out data backups to destroy them.

3 DEMAND

A typical ransom note explains what has happened and includes instructions for how to pay the ransom, as well as the consequences of not paying by a specific deadline. In some cases, the attackers will offer to decrypt one file for free to prove that the decryption keys work.

4 DOUBLE EXTORTION

As if losing access wasn't enough, advanced ransomware thieves further leverage their position by first extracting confidential data before encrypting it, then threatening to publicize it or sell it if the victim refuses to pay. This process of double extortion pressures organizations into paying.

5 TO PAY OR NOT TO PAY

If a ransomware victim doesn't pay, they risk the chance of losing data forever and, in the case of double extortion, having that data exposed.

If they do pay, there is no guarantee that the attackers will provide the necessary decryption keys and, in the case of double extortion, the victim still has no way of preventing the attacker from selling or leaking the data.

In short, ransomware is always a losing situation. You can help avoid it by staying alert, thinking before clicking, and always following policies.

The Ransomware Business Model

Modern ransomware attacks now feature an almost corporate structure of partners who team up to create a model called "ransomware as a service," or RaaS. Let's explore an example of what the modern ransomware business model looks like:

DEVELOPERS

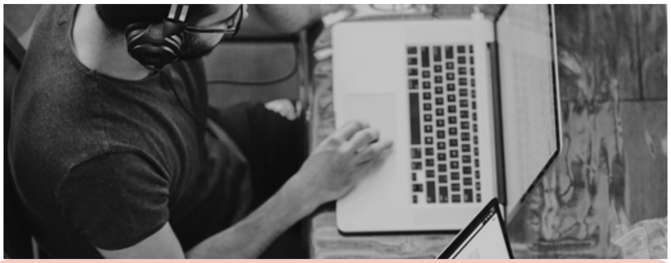
These are the people who develop the ransomware and sell it to others in what has become known as an affiliate program—a subscription-based service for renting the malware.

AFFILIATES

Affiliates are the customers in this situation. They pay a subscription fee and earn a percentage of the profits from successful attacks. They are also the ones who launch ransomware attacks.

ACCESS BROKERS

Why spend time trying to hack into organizations when you can hire someone who has already done that work? Access brokers sell the access they've acquired from successful attacks to other cyber criminals.



CUSTOMER SERVICE

No business can be successful without great customer service. Ransomware groups have been known to offer live chat support to help victims send payment and decrypt their data.

PUBLIC RELATIONS

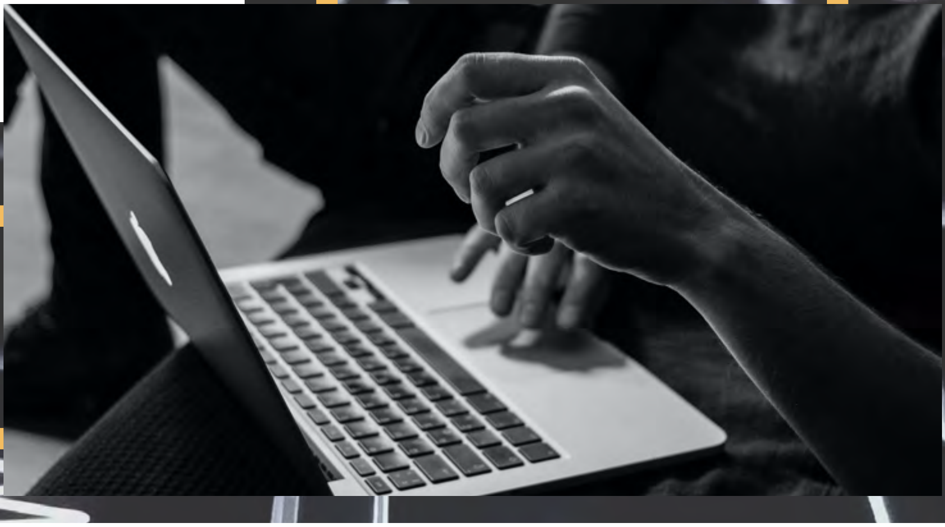
Some ransomware groups openly communicate with the press. They've even issued public apologies for attacks that harm society, such as the Colonial Pipeline attack in 2021 that resulted in widespread fuel shortages.

MONEY LAUNDERERS

Money launderers help the entire ransomware operation avoid law enforcement by "cleaning" the money, so it looks like it was acquired legally.

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

AVOIDING RANSOMWARE



The rise of ransomware was closely followed by a rise in security technologies that are designed to prevent infections. But it takes a human touch to truly avoid becoming a victim.

IDENTIFY PHISHING ATTACKS

Phishing emails are one of the most common attack methods. Always carefully inspect messages for warning signs like a sense of urgency, threatening language, and poor grammar. Remember that even if an email appears to come from someone you know, it could still be a scam.

AVOID REMOVABLE MEDIA

USB flash drives and charging cables offer an easy path towards infecting devices. Only use the charging cables that belong to you. Avoid public charging stations, such as those found at airports and cafes. If you find a random USB drive, don't plug it in.

USE ANTIVIRUS SOFTWARE

Antivirus software is a security tool that can help identify and remove infections. In your personal life, consider installing antivirus software on all devices. Here at work, be sure to follow policy and never bypass any security controls.

DON'T ACCESS PIRATED CONTENT

Not only is it illegal to download pirated content (which means it has been stolen from the content creator), sites that offer illegal downloading services are often the target of criminal hackers. Downloading pirated content is an especially easy way to infect your computer with malware.

MIND YOUR MOBILE DEVICES

Cyber criminals often develop mobile applications that can spread malware. You can avoid them by only visiting reputable online stores and researching the developers. For work devices, always ask before installing any software unless it has been explicitly approved.