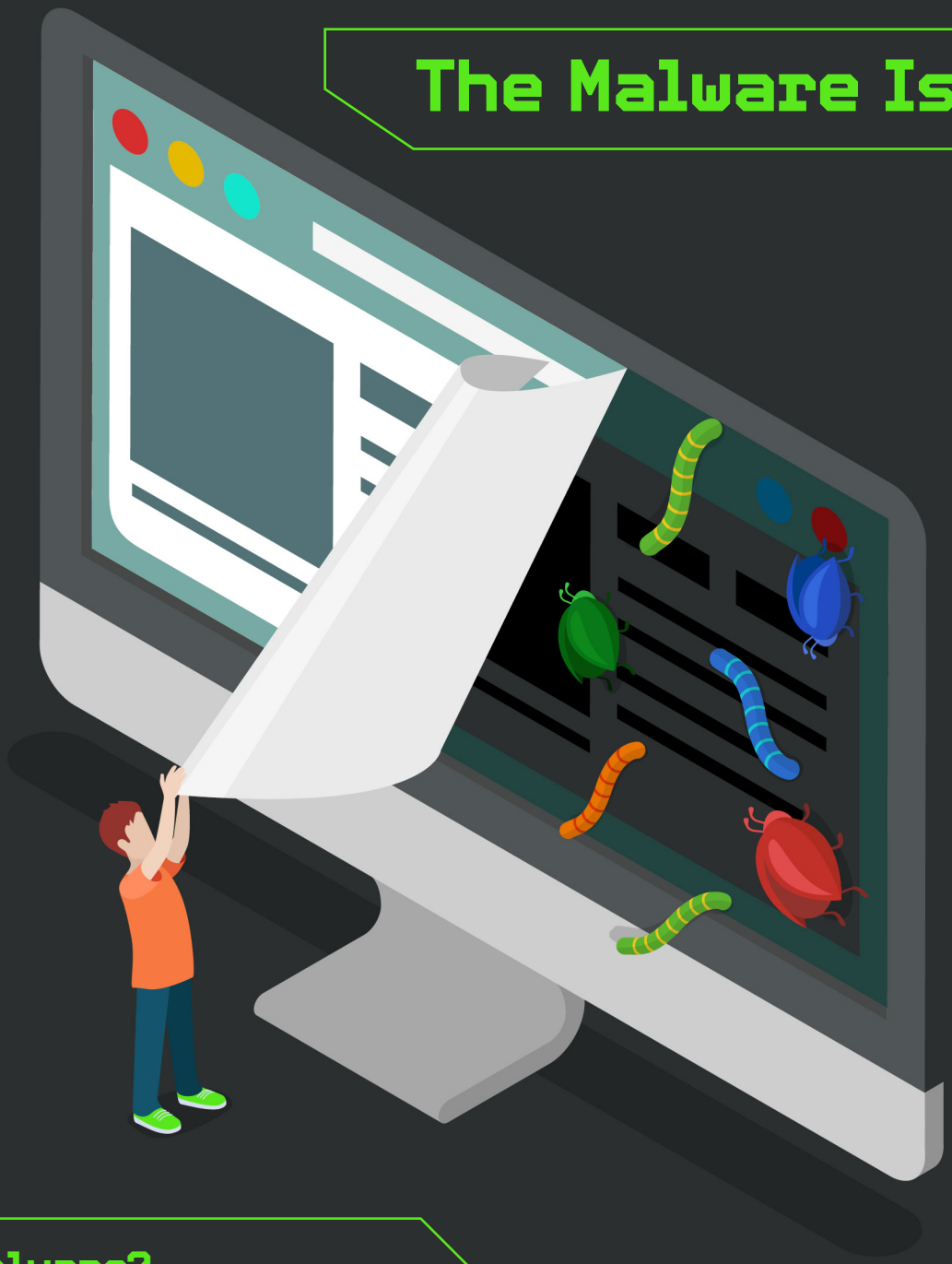
SecurityAwarenessNews

the security awareness newsletter for security aware people

The Malware Issue



What is Malware?

Preventing Malware Infections

What Everyone Needs to Know About Ransomware

What is Malware?

Short for malicious software, malware is an umbrella term covering various types of harmful computer programs and viruses used by cybercriminals for nefarious purposes. Experimental versions date back to the 1970s, and by the late 1990s, malware was infecting home computers.

What is malware capable of?

While the intentions of cybercriminals vary, here are just a few examples of malware's capabilities:

Stealing confidential data

- Some forms of malware are designed to infiltrate networks and give attackers access to confidential data like credit card numbers, customer databases, and business strategies. In other cases, malware may log keystrokes to steal passwords (known as a keylogger) or monitor an individual's computer and internet use (known as spyware).

Encrypting data

- By now, you've probably heard of ransomware, a dangerous infection that encrypts data or systems, locking out the victims until a ransom is paid. Ransomware has exploded over the last few years, becoming one of the most common (and lucrative) variants in existence.

Disrupting services

- The prevalence of unsecure smart devices allows attackers to create botnets—a collection of compromised internet-connected devices. Botnets are often used to perform distributed denial-of-service (DDoS) attacks. These attacks flood internet servers with more traffic than they can handle, causing widespread internet outages that knock services offline.

Can malware be stopped?

We'll cover the specifics of preventing malware infections shortly. For now, the key takeaways are:

- » As long as the internet exists, there will always be malware.
- » Smartphones and other devices can be as easily infected as traditional computers.
- » Malware targets individuals, not just large organizations.
- » All it takes is one careless click to compromise systems and devices.

Preventing Malware Infections

Avoiding malware infections is easy, both at work and at home. Here are five ways to keep a healthy system:

Don't get phished

As always, phishing deserves immediate and ongoing attention. Most malware infections are spread through malicious links and attachments. Be sure to carefully inspect messages for warning signs like bad grammar, threatening language, a sense of urgency, and unexpected attachments.

Beware of removable media

USB flash drives represent an easy attack vector. Cybercriminals hope to leverage someone's curiosity by planting malicious flash drives around organizations and public areas. When the drive is plugged in, it can launch and install malware on the victim's computer.

Utilize security tools

All devices should have antivirus and anti-malware services running in the background. These services reference a database of known vulnerabilities and can block potentially dangerous files or websites. For personal use, do some research and find an option that works for you.

Protect your Internet of Things (IoT)

We live in a connected world of smart homes, smart electronics, and smart cars. This is known as the Internet of Things, and it ushers in major security and privacy concerns. Protect your IoT with strong passwords, and thoroughly research products before adding them to your network. Disable the internet connection of any devices that you don't regularly use.

Stay updated

At work, follow organizational policies for software and firmware updates. In your personal life, consider enabling automatic updates for computers and smart devices so you never miss a critical security patch. Failure to do so could allow cybercriminals to leverage known vulnerabilities.

Did you know?

Some malware strains can cause physical damage to equipment or machines. Stuxnet might be the most notorious example. It is believed that the Stuxnet virus caused significant damage to Iran's nuclear program by causing fast-spinning centrifuges to tear themselves apart! This goes to show that malware presents a threat greater than just data theft or system corruption.

What Everyone Needs to Know About Ransomware

Big business

Government agencies reported that from 2019 to 2020, ransomware attacks cost organizations a billion dollars (USD). The lucrative nature of the ransomware business model is why it has continued to skyrocket as one of the most dangerous attacks to date.

Time is expensive

Beyond paying large sums of money for decryption keys (the code that reverses encryption after payout), downtime for any organization can be prohibitively expensive. Furthermore, most attacks give the victim a specific date by which the ransom must be paid. Miss that deadline and the data will be destroyed, leaked online, or the price of the ransom will be significantly increased.

More than money

Forget about financials for a second. Ransomware becomes life-threatening when it hits hospitals and creates emergency situations, and can also create emergency circumstances within critical infrastructure like fuel supplies and electrical grids. Such attacks highlight the dangerous impact ransomware has on society as a whole and not just organizations.

At your service

It's scary to think about the sophistication of some ransomware variants. But what's even scarier is that you don't need to be a highly experienced coder to launch these attacks. Some ransomware authors sell their software—including instructions on how to use it—to other cybercriminals. This is called Ransomware-as-a-Service or RaaS. It's essentially a subscription-based model that offers an easy payday for novice criminal hackers.

Paying is risky

Paying a ransom creates a series of problems:

- There's no guarantee the criminals will provide decryption keys.
- Even when the keys are provided, unencrypting locked data can be an extremely slow process.
- Paying the ransom makes the victim an even bigger target because the attackers know they're likely to get paid for future attacks.

Data backups can't solve everything

Restoring systems from data backups can be incredibly time-consuming, sometimes even slower than decryption keys. Worse yet, if the data backups haven't been isolated from a network, sophisticated ransomware campaigns may attack the data backups first and then move onto the main network.

We can avoid these problems by staying alert, thinking before clicking, and always following organizational policies. Need more information? Please ask!