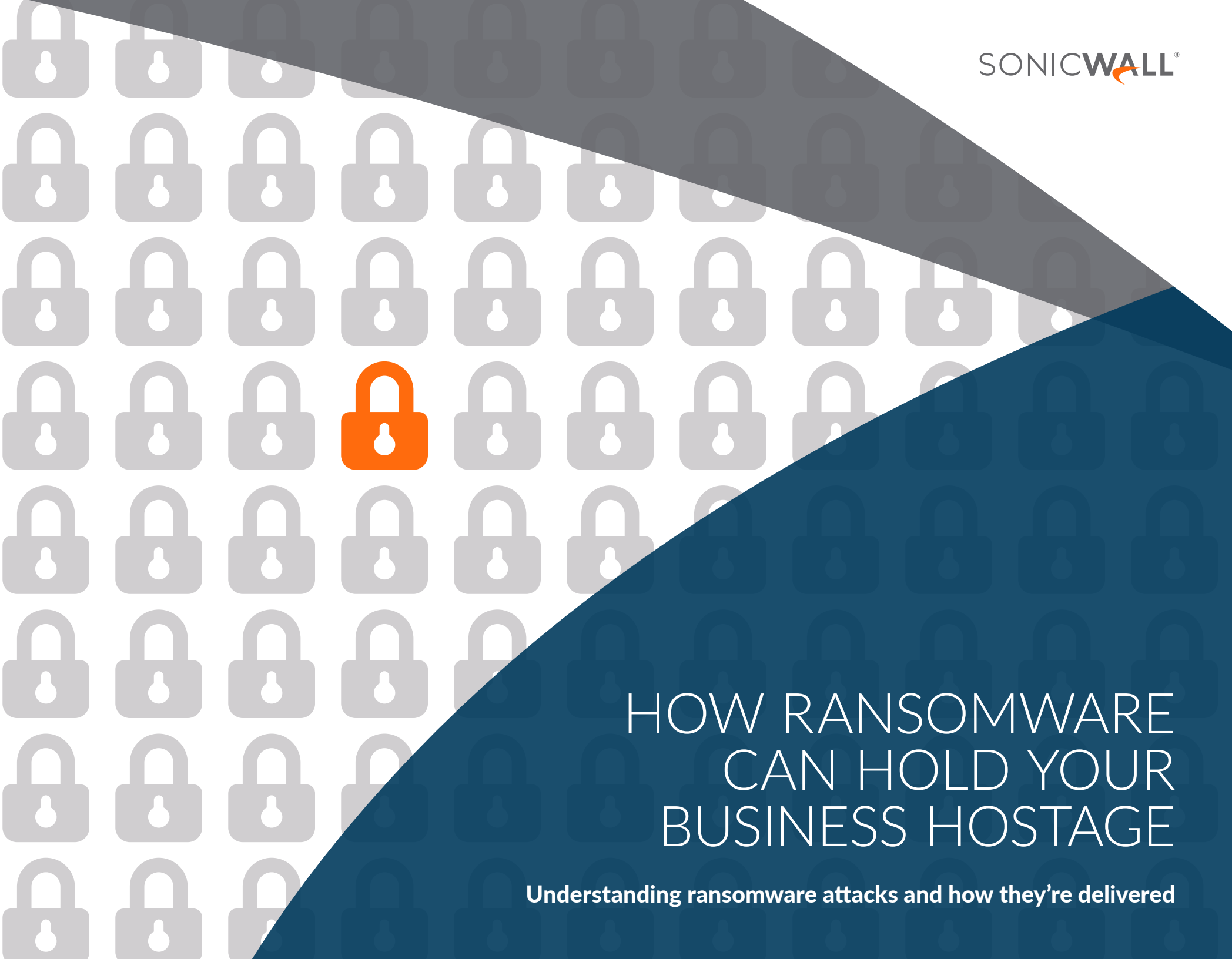


SONICWALL

HOW RANSOMWARE CAN HOLD YOUR BUSINESS HOSTAGE

Understanding ransomware attacks and how they're delivered

Introduction

Ransomware is a form of malware that denies access to data or systems until the victim pays the cybercriminal a ransom fee to remove the restriction. It has been around for many years but has recently become much more popular and profitable. CryptoLocker, CryptoWall and RSA4096 are examples of well-known ransomware.

Although ransomware generates over $25 million in revenue for hackers each year[1], the damage they inflict far outweighs what they make.

[1] *Business Insider*

How ransomware works

Ransomware can make its way onto a system through a variety of means, with the victim ultimately downloading and installing a malicious application. Once on the device, the code will spread throughout the system and encrypt files on the hard drive or simply lock the system itself with a bootlocker. In some cases, it may block access to the system by displaying images or a message across the device's screen to persuade the user to pay the malware operator a ransom for the encryption key to unlock the files or system.

Bitcoin is a popular form of ransomware payment because it is easy to obtain, thereafter hackers launder the money into other currencies like DASH or Monero.

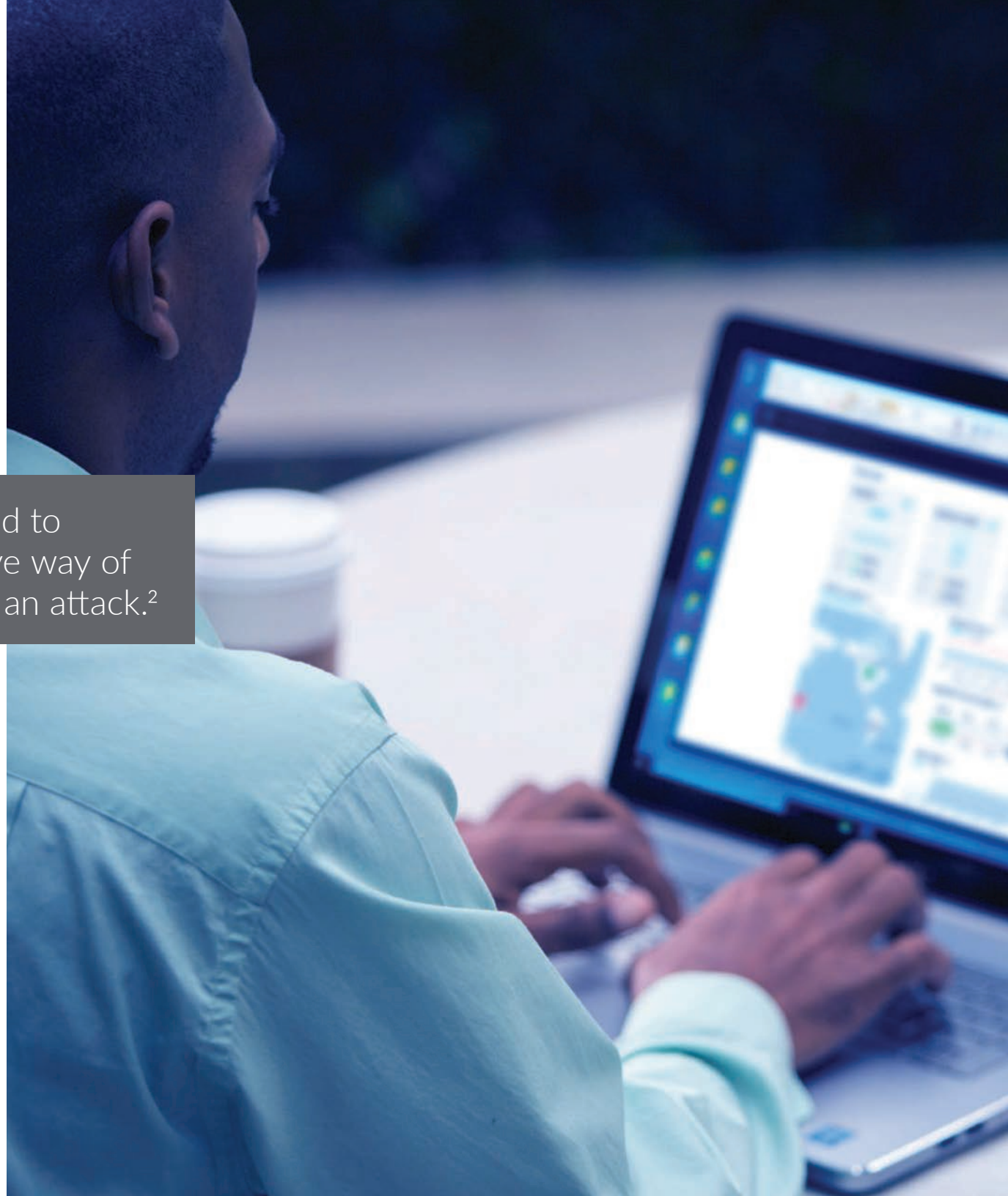
SONICWALL®

Phishing emails

One of the most common distribution methods of ransomware is phishing emails. These types of emails attempt to entice recipients to open an email and click on a website link. The site may ask for sensitive information or contain malware, such as ransomware, that is downloaded onto the victim's system.

Phishing click rates have lowered to 3.4% but still remain an effective way of penetrating defenses to launch an attack.[2]

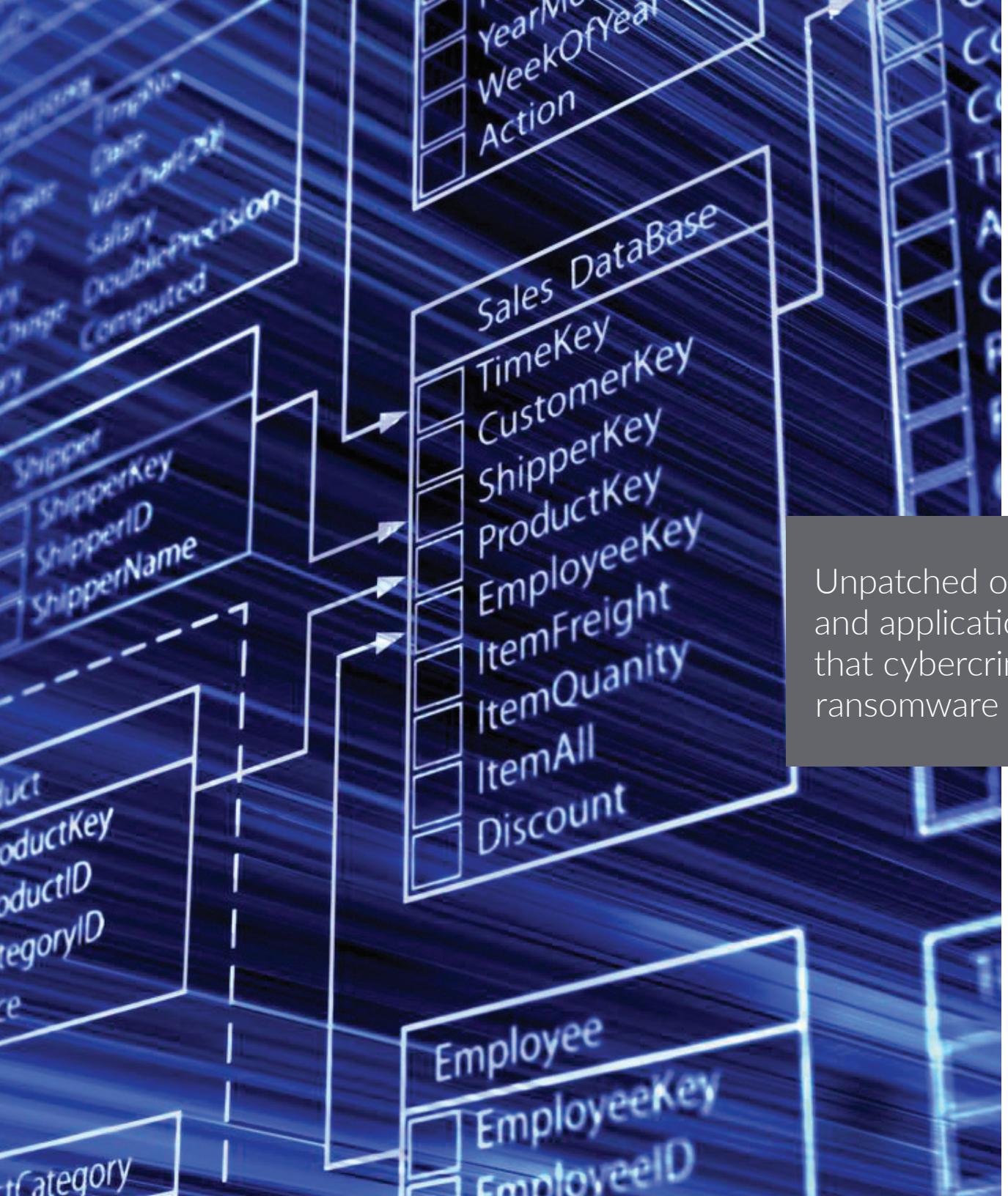
[2] *2020 Verizon Data Breach Investigation Report*



Malvertisements

Another popular form for distributing ransomware is “malvertising,” or malicious advertising, which uses online advertisements to spread ransomware. The attacker infiltrates advertising networks, sometimes posing as a fake advertiser or agency, and inserts malware-laden ads into legitimate websites. Unsuspecting visitors to the sites don’t even need to click on the advertisement for their system to become infected.

In addition to launching ransomware, “malverts” can be used to extract customer credit card numbers, Social Security numbers and other confidential information.

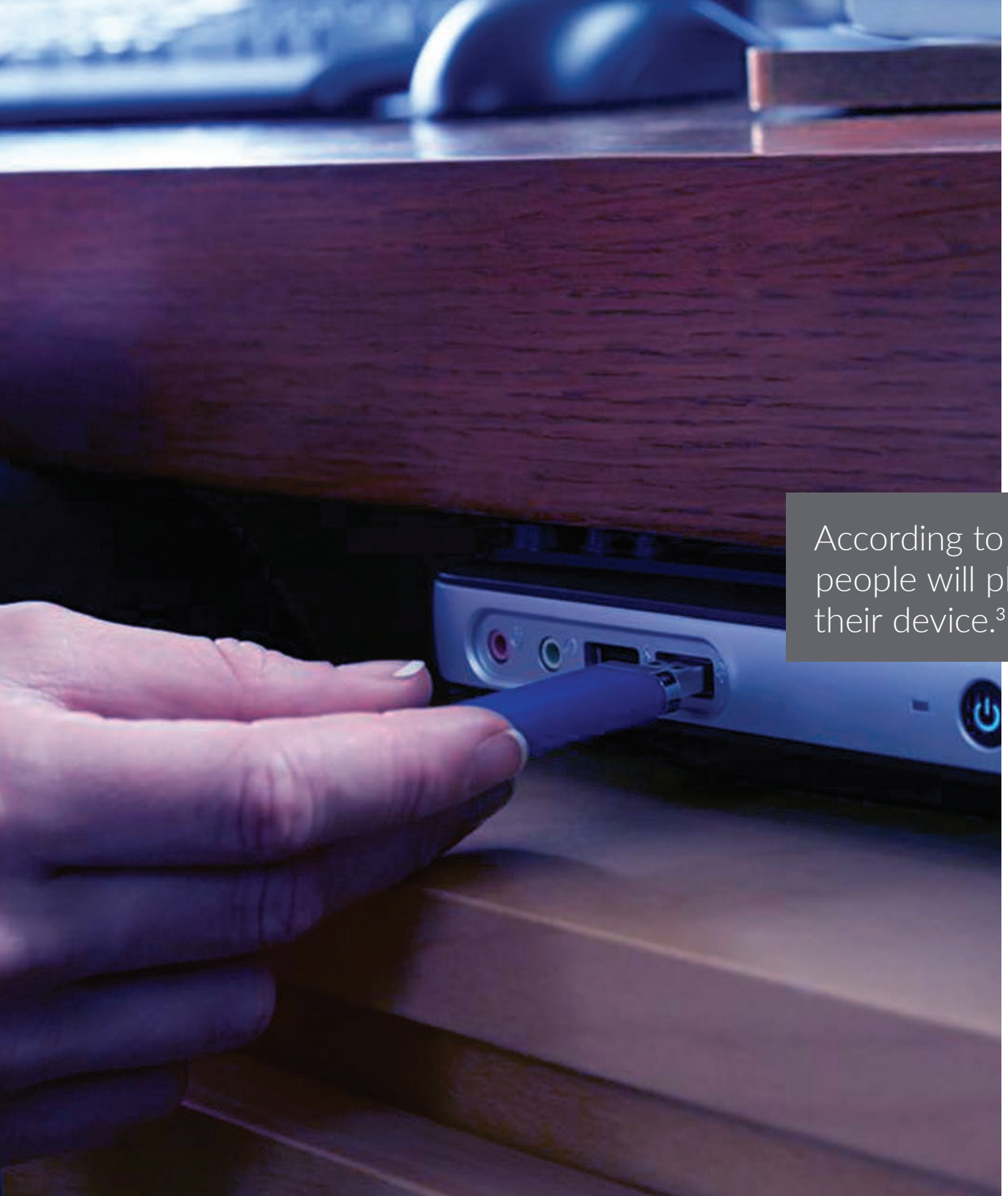


Exploitation of unpatched systems and applications

Many attacks are based on known vulnerabilities in operating systems, browsers and common apps. Cybercriminals are able to exploit these vulnerabilities to launch their ransomware attacks against systems that are not up to date with the latest software patches.

Unpatched operating systems, browsers and applications may contain vulnerabilities that cybercriminals can exploit to launch ransomware attacks.

SONICWALL®



External devices

External devices, such as USB drives, are used to store and transfer files — making them targets for spreading ransomware across multiple systems. Some of these files contain an advanced feature known as macros that can be used by hackers to execute ransomware when the file is opened.

According to the latest study, 48% of people will plug a found USB key into their device.[3]

[3] *Users Really Do Plug in USB Drives They Find*

SONICWALL®

Why traditional methods fail to prevent ransomware attacks

Many of the traditional security controls often fail to detect ransomware if they are only looking for unusual behavior and standard indicators of compromise. Once on the system, ransomware behaves like a security application and it can deny access to other systems/ programs. It usually leaves the underlying files and systems unaffected and only restricts access to the interface.

Ransomware, coupled with social engineering, can create a very effective attack.

Hidden ransomware

Ransomware can also go undetected in firewalls that are unable to decrypt and inspect SSL-encrypted web traffic. Legacy network security solutions typically either don't have the ability to inspect SSL/TLS-encrypted traffic or their performance is so low that they become unusable when conducting the inspection. Increasingly, cybercriminals have learned how to hide malware in encrypted traffic.

The use of Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption continues giving hackers a chance to bypass perimeter security unchecked in many cases.

Conclusion

SonicWall can enhance protection across your organization by inspecting every packet and governing every identity. As a result, this protects your data wherever it goes, and shares intelligence to safeguard against a variety of threats, including ransomware.

Visit the SonicWall ransomware web page.

SONICWALL®

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com