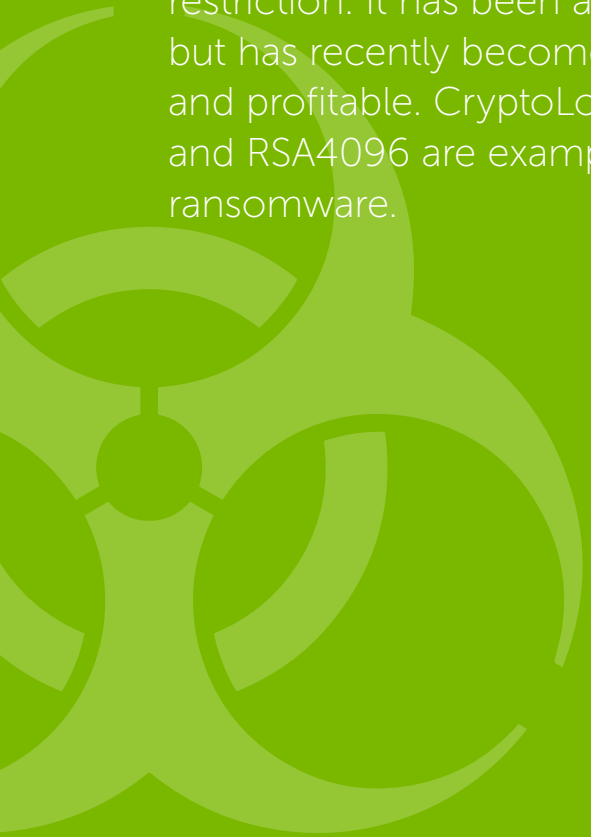
How ransomware can hold your business hostage

Understanding ransomware attacks and how they're delivered

DELL Security

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.



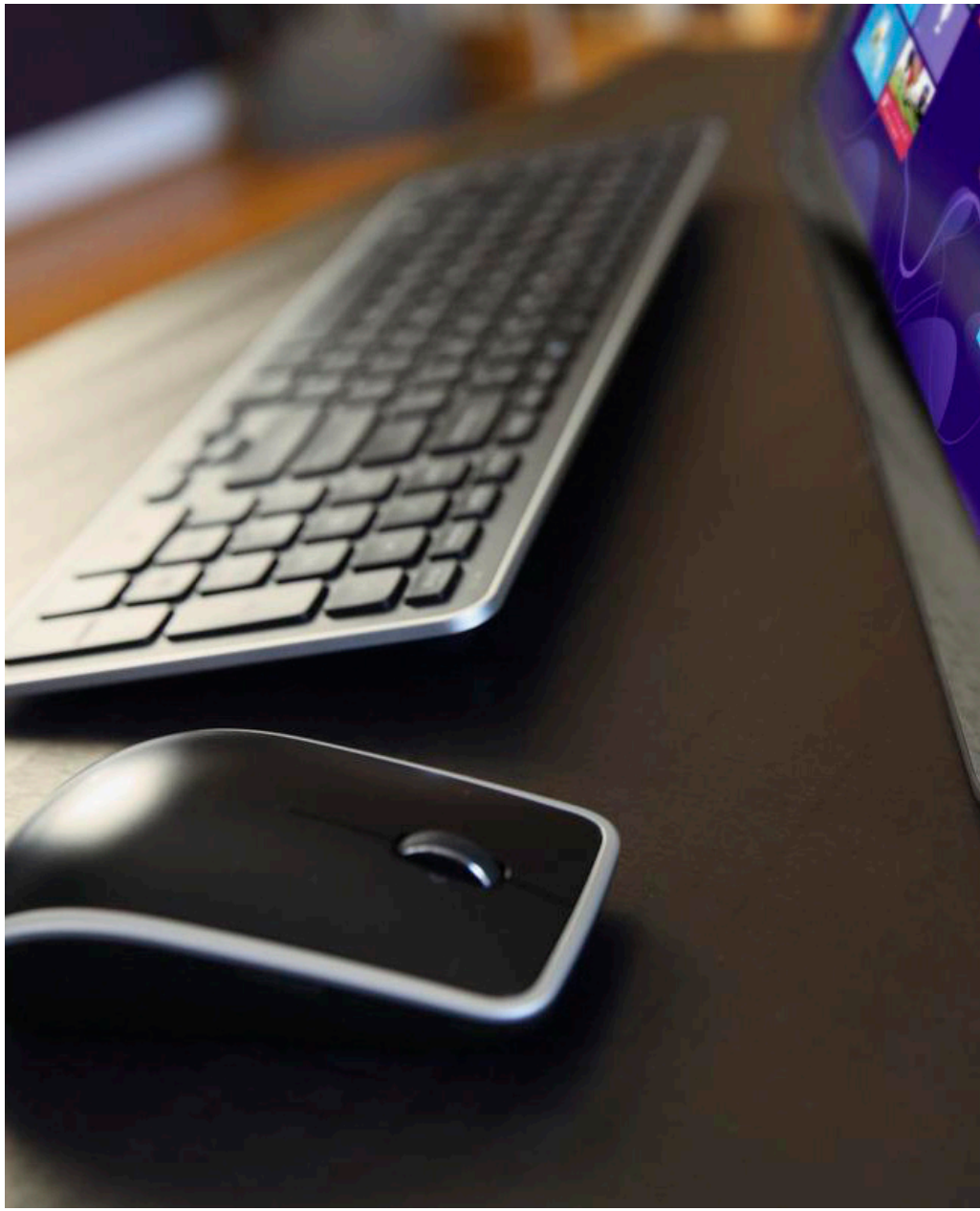
According to the FBI, more than $209 million has already been paid in the first three months of 2016[1] in the United States, compared to $25 million in ransom all of the previous year.

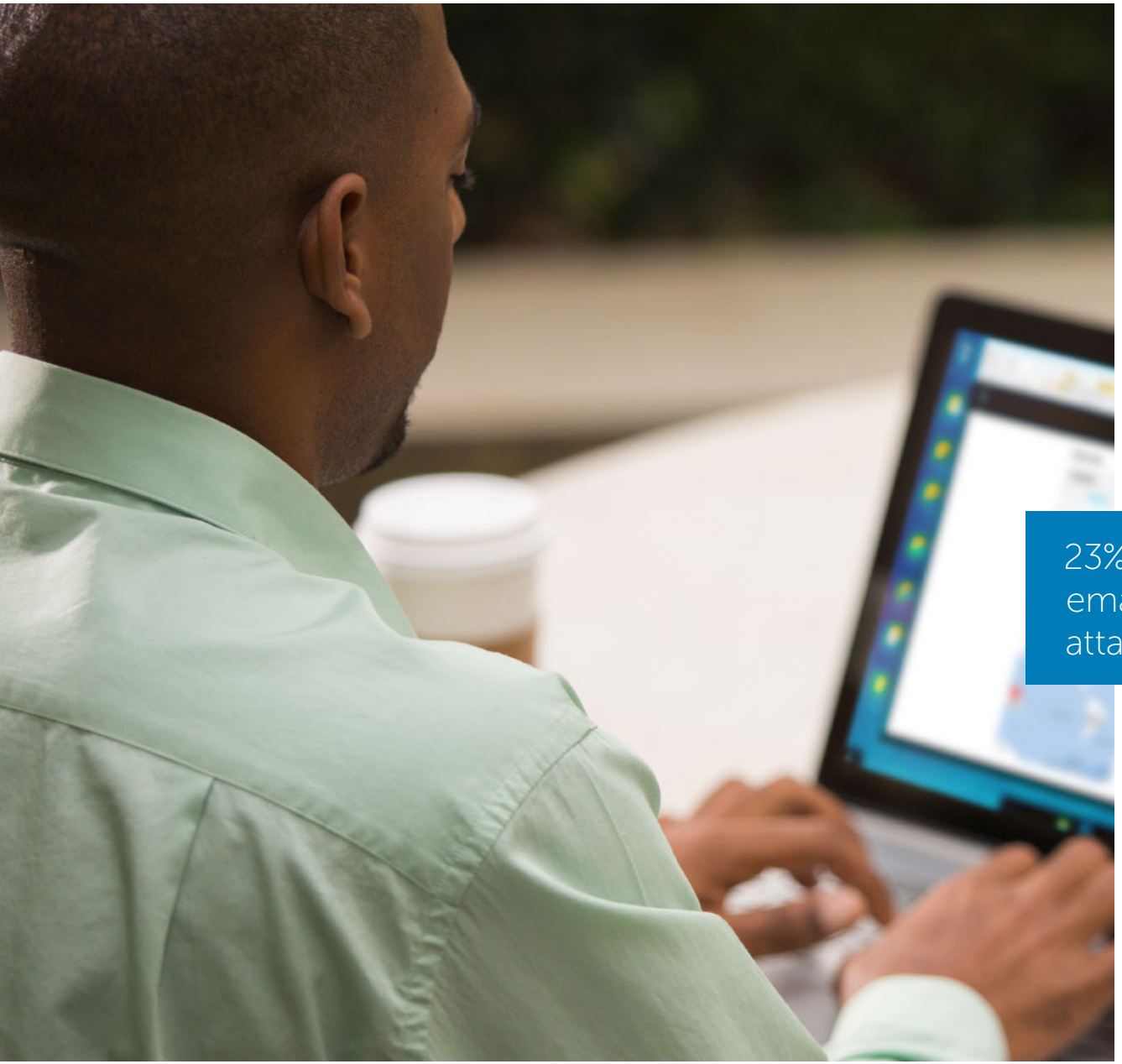
[1] http://sd18.senate.ca.gov/news/4122016-bill-outlawing-ransomware-passes-senate-committee

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 app will spread throughout the system and encrypt files on the hard drive or simply lock the system itself. 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.

Bitcoins are a popular form of ransomware payment because the digital currency is difficult to trace.





Phishing emails

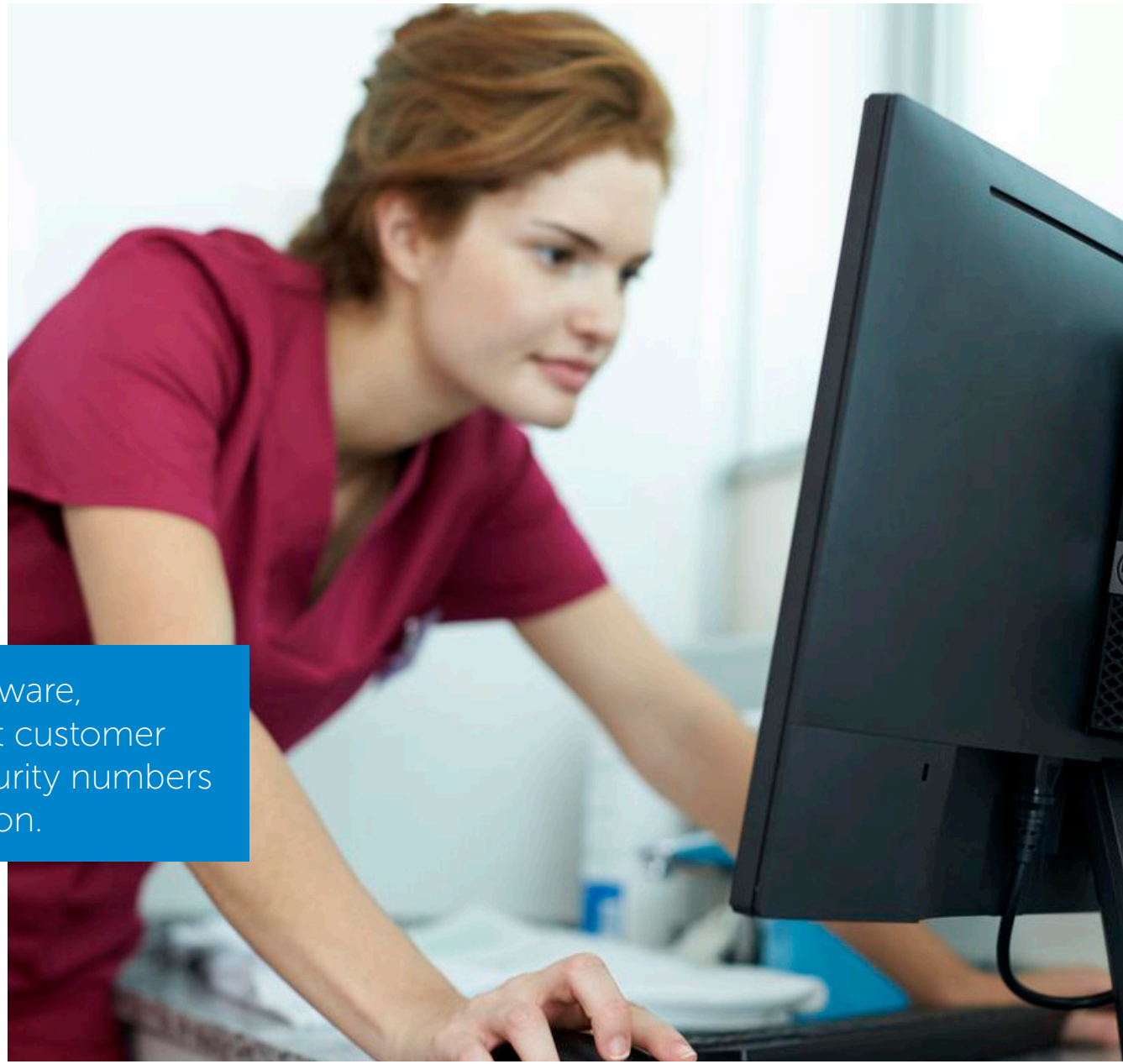
One of the most common distribution methods of ransomware is phishing emails. These types of emails attempt to entice recipients to open an email and click on a website link. The site may ask for sensitive information or contain malware, such as ransomware, that is downloaded onto the victim's system.

23% of recipients open phishing emails and 11% actually click on the attachments[1].

[1] 2015 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.

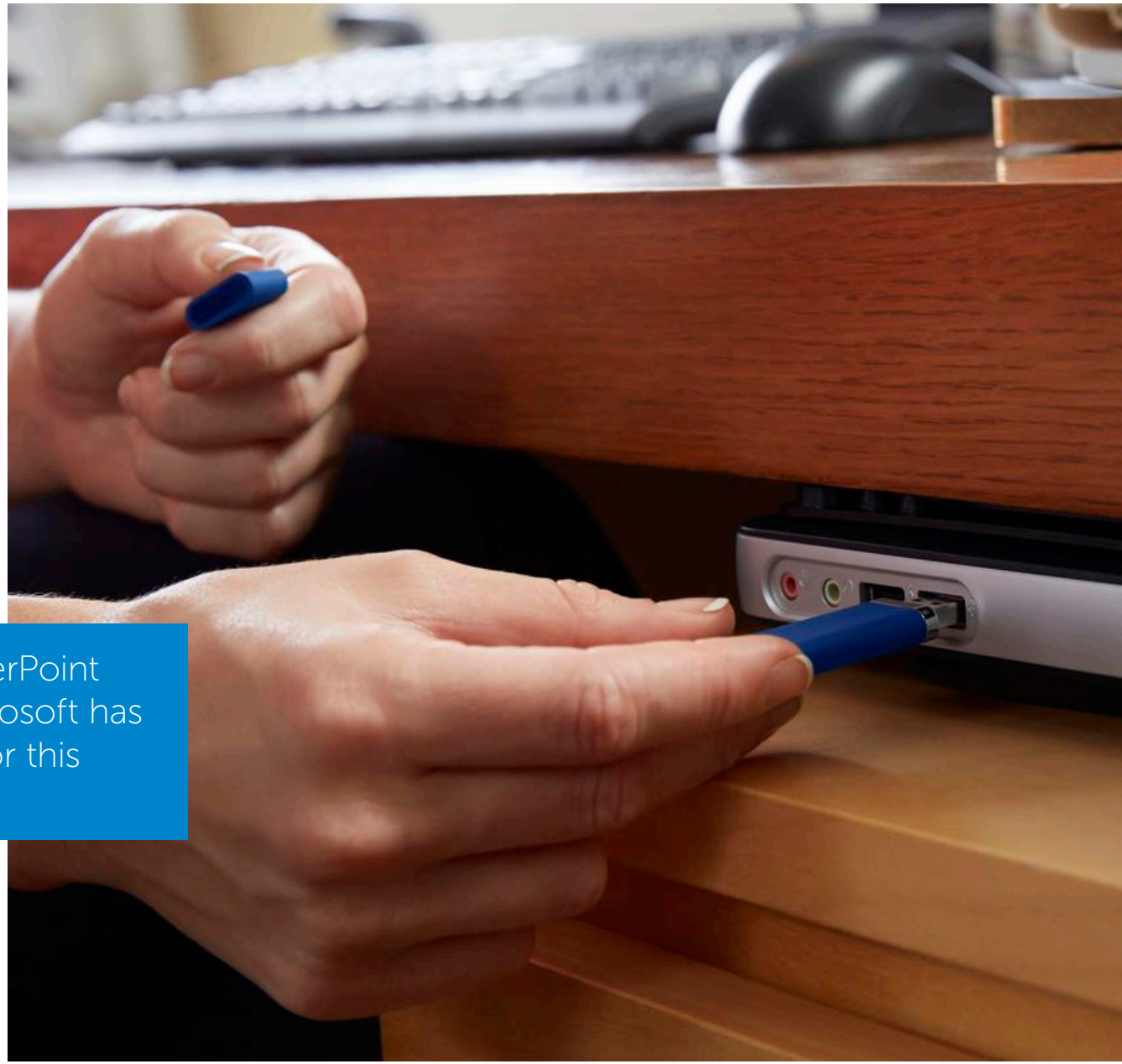
Exploitation of unpatched systems and applications

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.

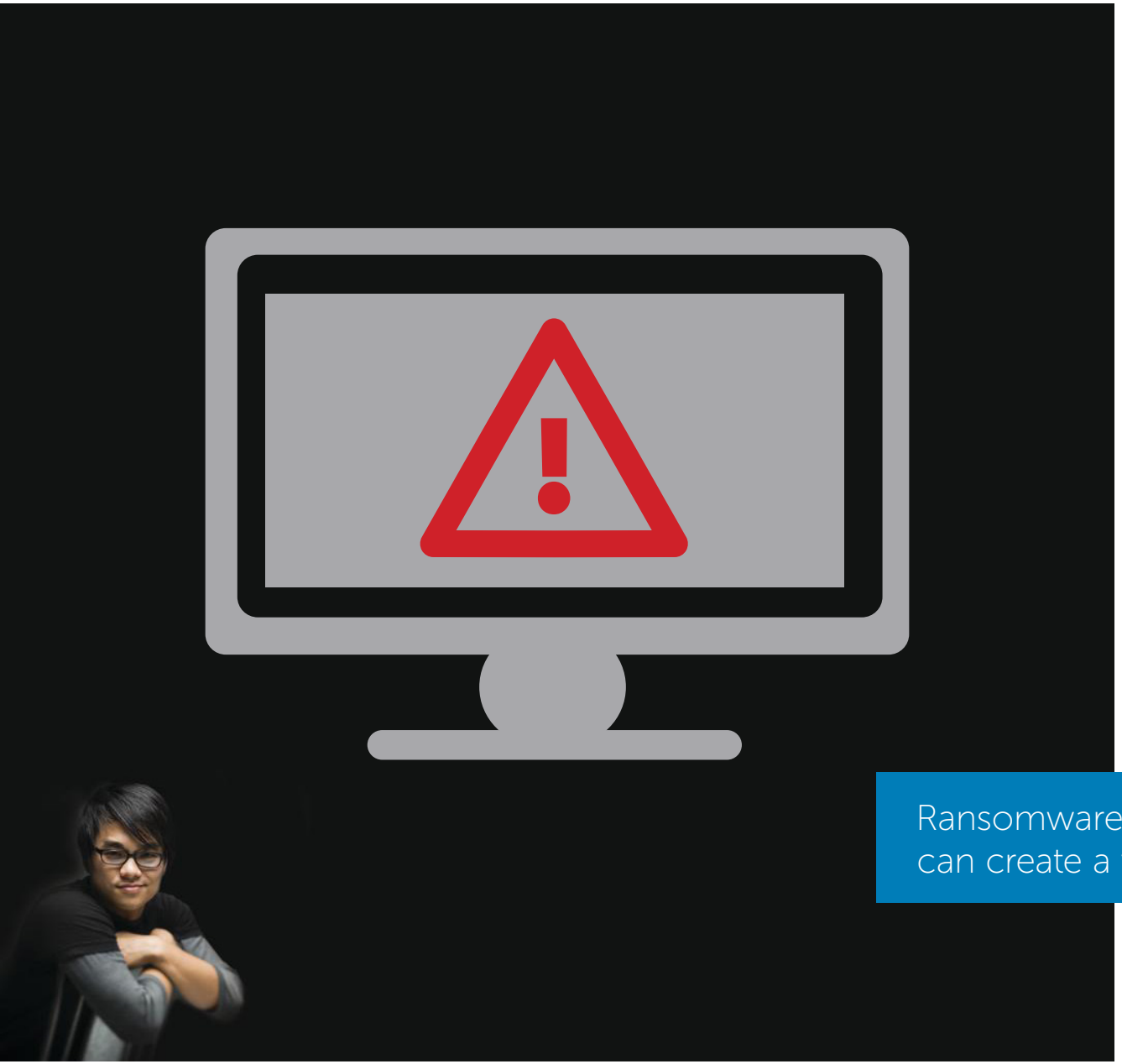
Unpatched operating systems, browsers and applications may contain vulnerabilities that cybercriminals can exploit to launch ransomware attacks.

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.



Microsoft Word, Excel and PowerPoint are prime targets, although Microsoft has taken steps to tighten security for this threat in Office 2016.



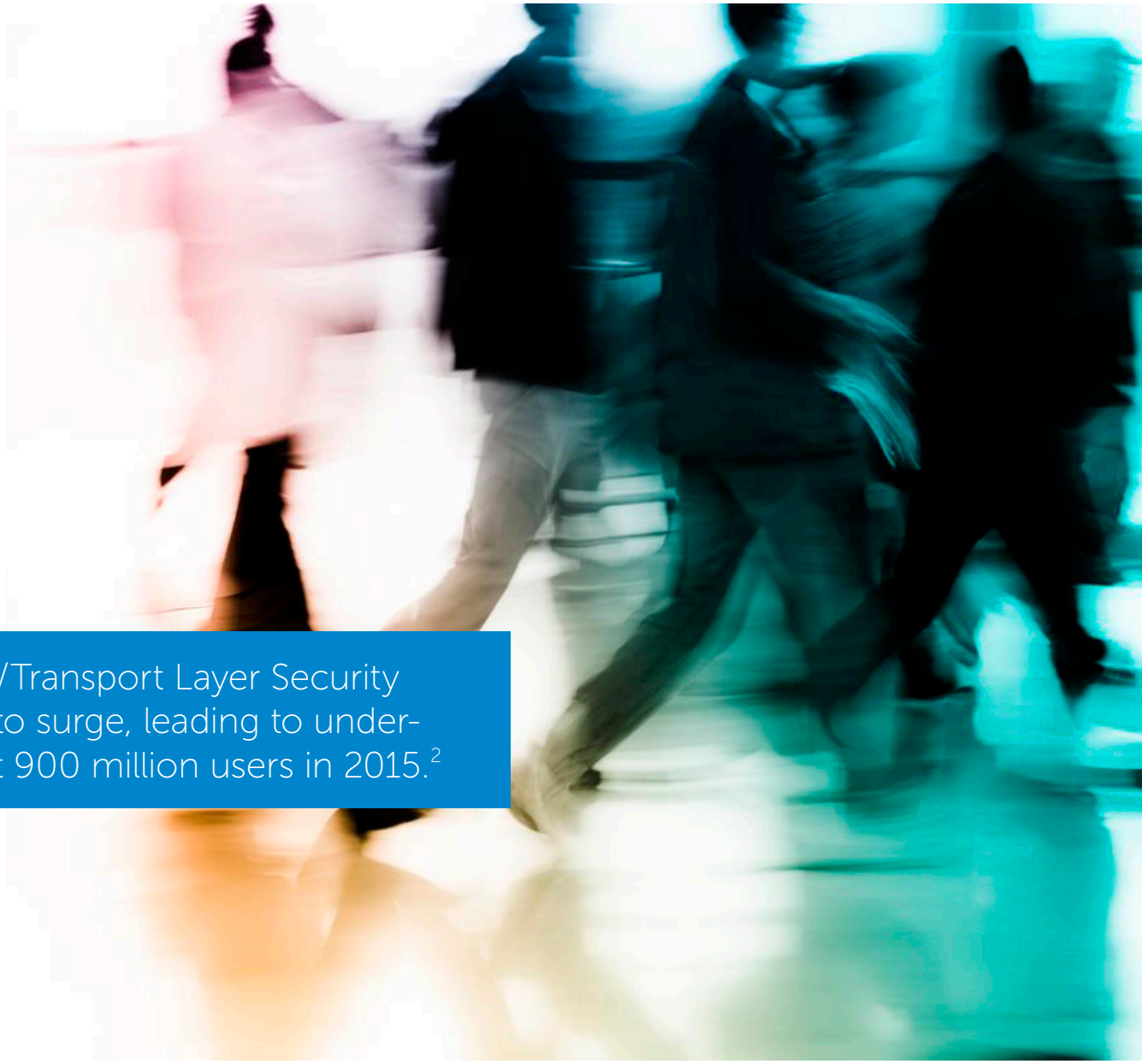
Why traditional methods fail to prevent ransomware attacks

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.

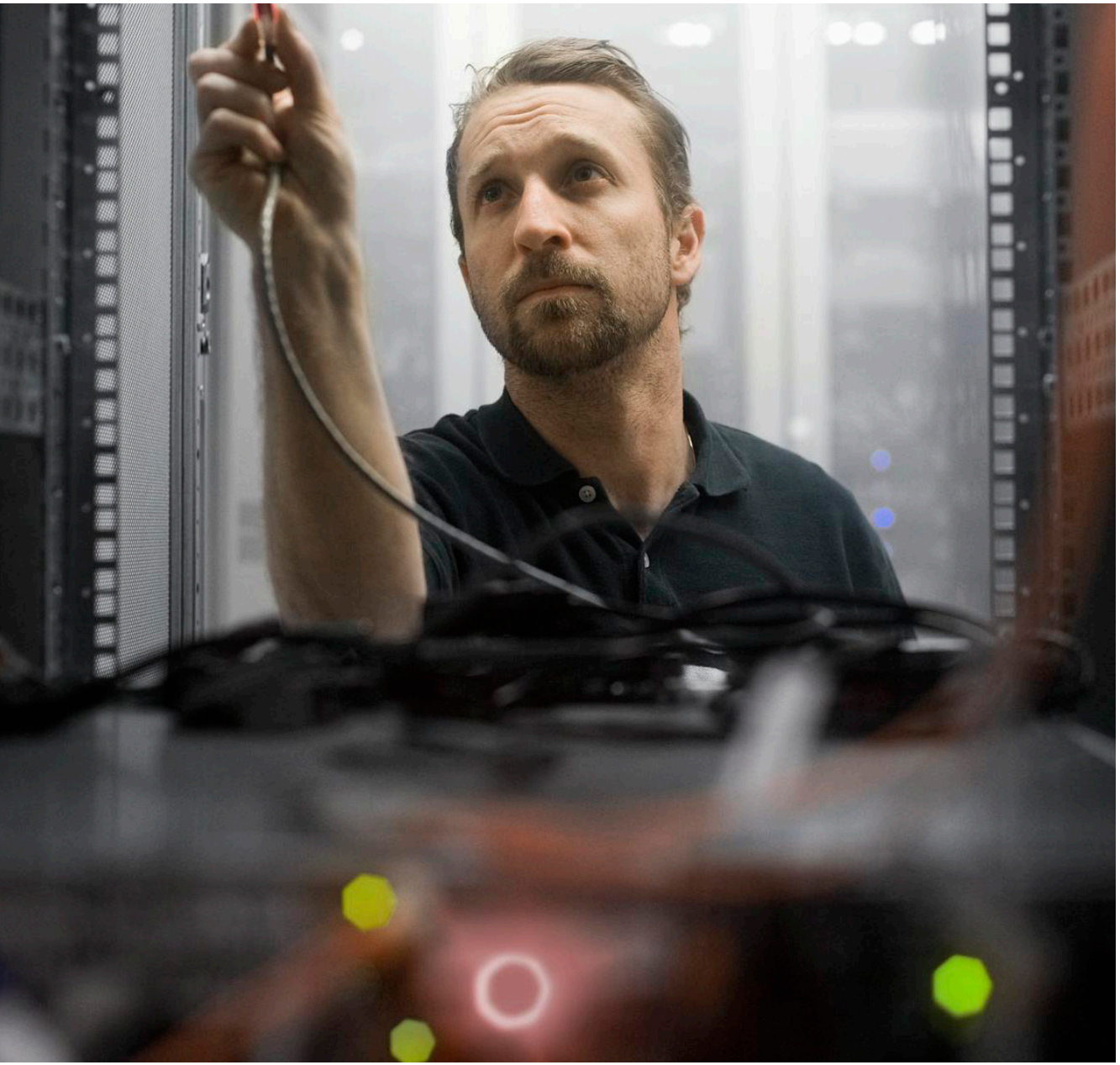
Hidden ransomware

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 to surge, leading to under-the-radar hacks affecting at least 900 million users in 2015.[2]

[2] 2016 Dell Security Annual Threat Report



Conclusion

Dell Security 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 Dell SonicWALL Network Security Products web page.

About Dell Security

Dell Security solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can drive your business forward. www.dell.com/security

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

Dell
5455 Great America Parkway,
Santa Clara, CA 95054
www.dell.com/security

Refer to our Web site for regional and international office information.

Ebook-NS-Ransomware-US-VG-29223