Como ransomware pode manter seu negócio refém

Entenda os ataques de ransomware e como eles são realizados

Introdução

O ransomware é uma forma de malware que nega o acesso a dados ou sistemas até que a vítima pague uma taxa ao criminoso cibernético para que ele remova a restrição. Ele já existe há vários anos, mas ultimamente se tornou muito mais popular e lucrativo. CryptoLocker, CryptoWall e RSA4096 são exemplos de ransomwares conhecidos.

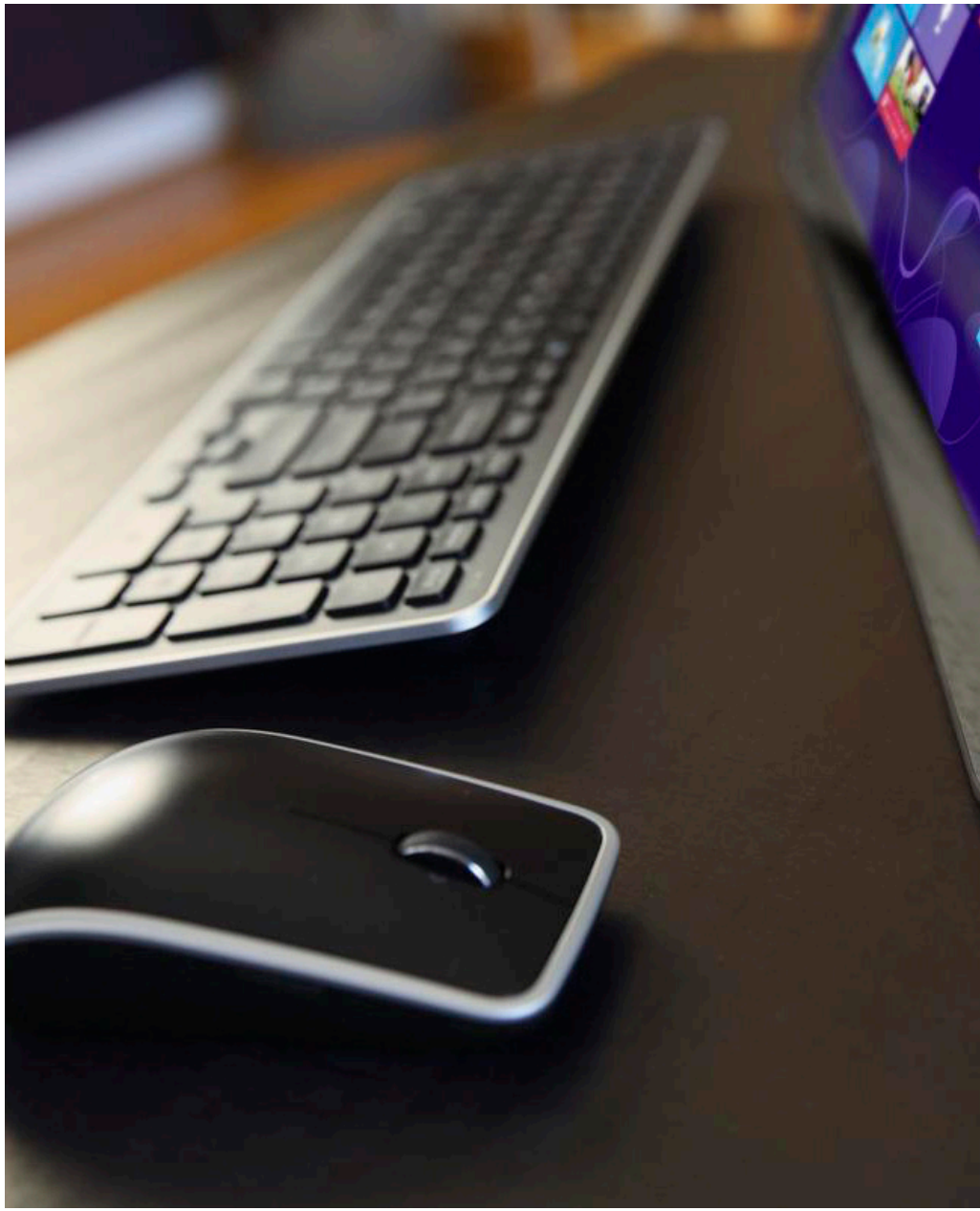
De acordo com o FBI, mais de US$ 209 milhões já foram pagos nos primeiros três meses de 2016[1] nos Estados Unidos, comparado a US$ 25 milhões em taxas durante todo o ano passado.

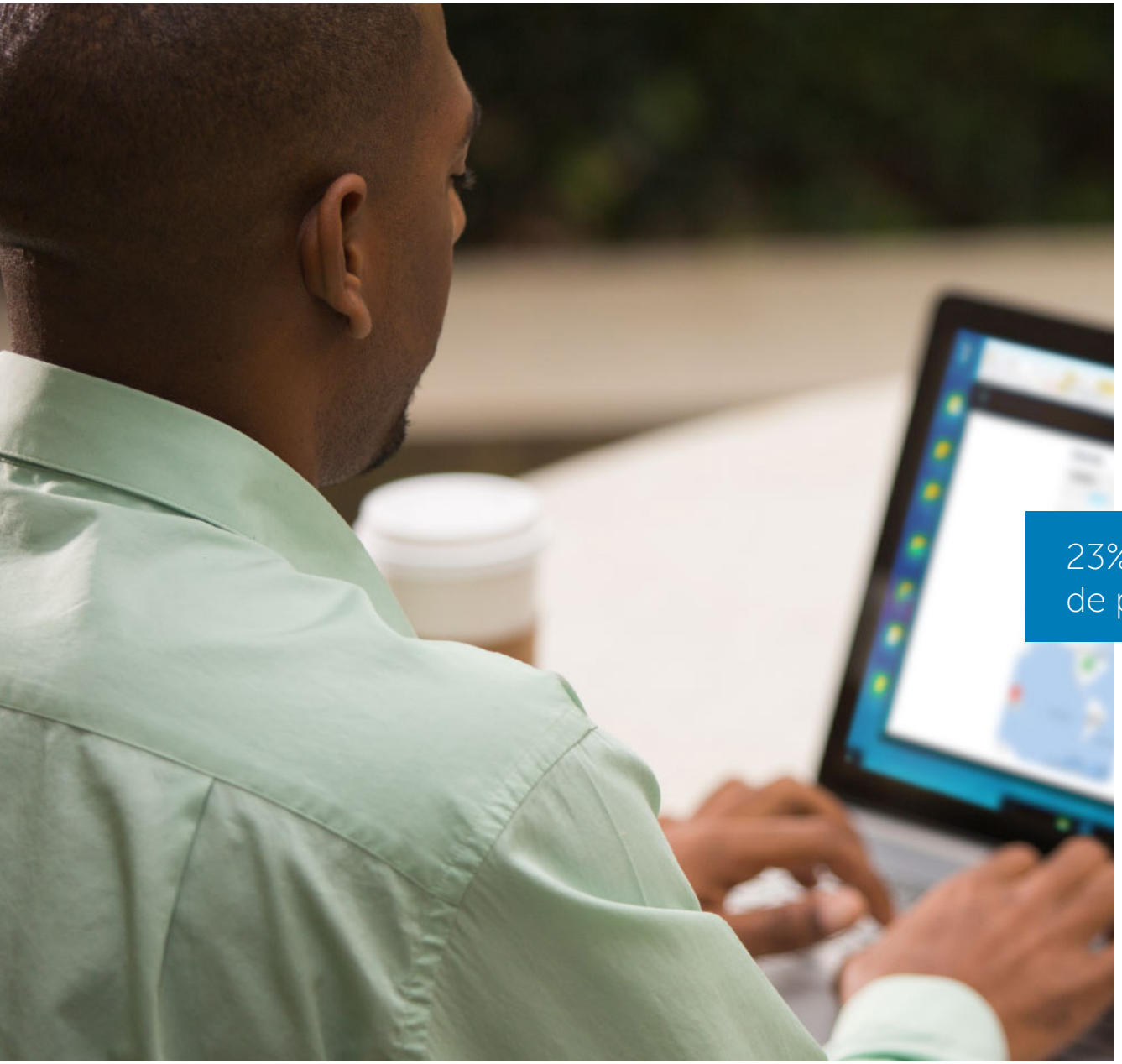
[1] http://sd18.senate.ca.gov/news/4122016-bill-outlawing-ransomware-passes-senate-committee

Como um ransomware funciona

Um ransomware pode entrar nos sistemas de diversas formas, quando a vítima faz download e instala um aplicativo mal-intencionado. Uma vez no dispositivo, o aplicativo será disseminado em todo o sistema e arquivos criptografados no disco rígido ou simplesmente bloqueará todo o sistema. Em alguns casos, ele pode bloquear o acesso ao sistema com a exibição de imagens ou de uma mensagem na tela do dispositivo para convencer o usuário a pagar uma taxa ao operador do malware para que uma chave de criptografia desbloqueie os arquivos ou o sistema.

Bitcoins são uma forma popular de pagamento de ransomware, pois a moeda digital é difícil de rastrear.





E-mails de phishing

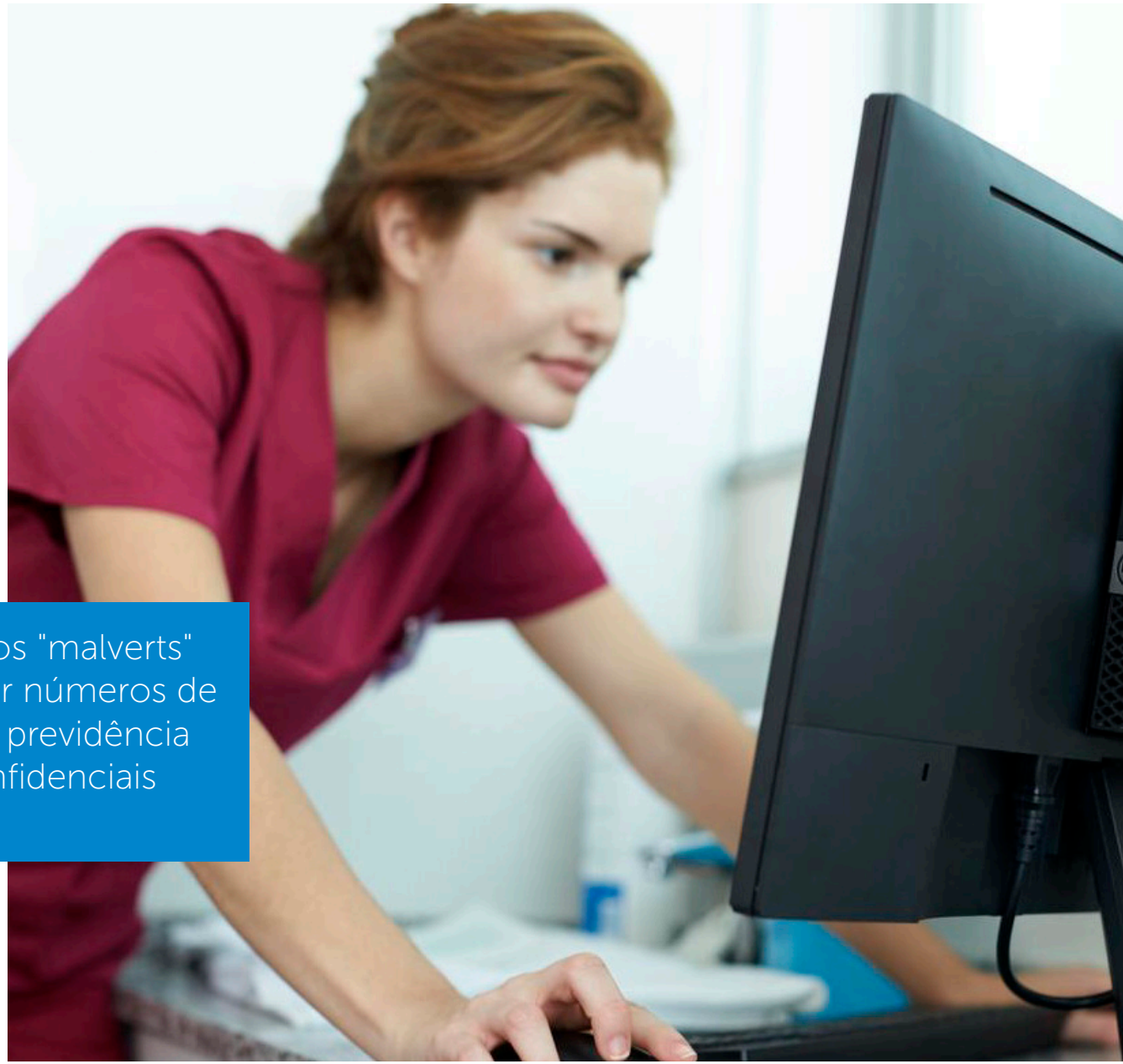
Um dos métodos mais comuns de distribuição de ransomware são os e-mails de phishing. Esses tipos de e-mails tentam fazer com que os destinatários abram a mensagem e cliquem no link de um site. O site pode solicitar informações confidenciais ou conter malware, como o ransomware, cujo download é feito no sistema da vítima.

23% dos destinatários abrem e-mails de phishing e 11% clicam nos anexos[1].

[1] Relatório de investigação de violação de dados da Verizon 2015

Malvertisements

Outra forma popular de distribuir ransomware é o "malvertising", ou publicidade mal-intencionada, que utiliza anúncios on-line para disseminá-lo. O invasor se infiltra nas redes publicitárias, algumas vezes como um anunciante ou uma agência falsa, e insere anúncios com malware em sites legítimos. Visitantes inocentes desses sites nem precisam clicar no anúncio para que seus sistemas sejam infectados.



Além de iniciar o ransomware, os "malverts" podem ser utilizados para extrair números de cartões de crédito, números de previdência social e outras informações confidenciais dos clientes.

Exploração de aplicativos e sistemas sem patch

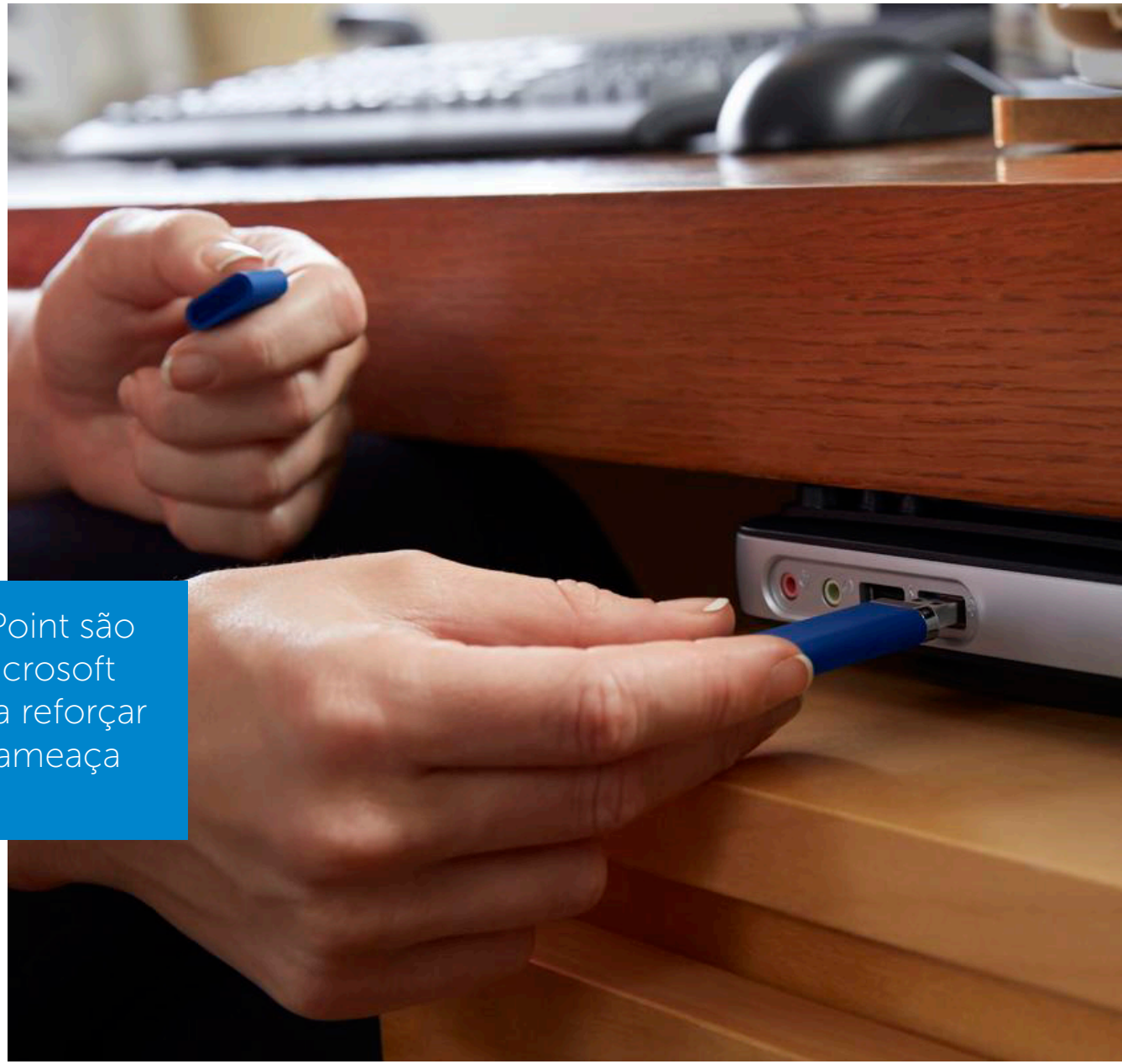
Vários ataques são baseados em vulnerabilidades conhecidas de sistemas operacionais, navegadores e aplicativos comuns. Os criminosos cibernéticos podem explorar essas vulnerabilidades para iniciar seus ataques de ransomware em sistemas desatualizados com os patches de software mais recentes.

Navegadores, aplicativos e sistemas operacionais sem patches podem conter vulnerabilidades que os criminosos cibernéticos podem explorar para iniciar ataques de ransomware.

Dispositivos externos

Dispositivos externos, como unidades USB, são usados para armazenar e transferir arquivos, o que os torna alvos de disseminação de ransomware em vários sistemas. Alguns desses arquivos contêm um recurso avançado, conhecido como macros, que pode ser utilizado por hackers para a execução do ransomware quando eles foremabertos.

Microsoft Word, Excel e PowerPoint são os alvos principais, embora a Microsoft tenha tomado providências para reforçar a segurança em relação a essa ameaça no Office 2016.



Por que os métodos tradicionais falham na prevenção de ataques de ransomware

Vários controles de segurança tradicionais geralmente falham em detectar ransomwares caso procurem somente por comportamentos atípicos e indicadores padrão de comprometimento. Uma vez no sistema, o ransomware se comporta como um aplicativo de segurança e pode negar o acesso a outros sistemas/programas. Normalmente, ele deixa os sistemas e arquivos subjacentes inalterados e restringe o acesso somente à interface.

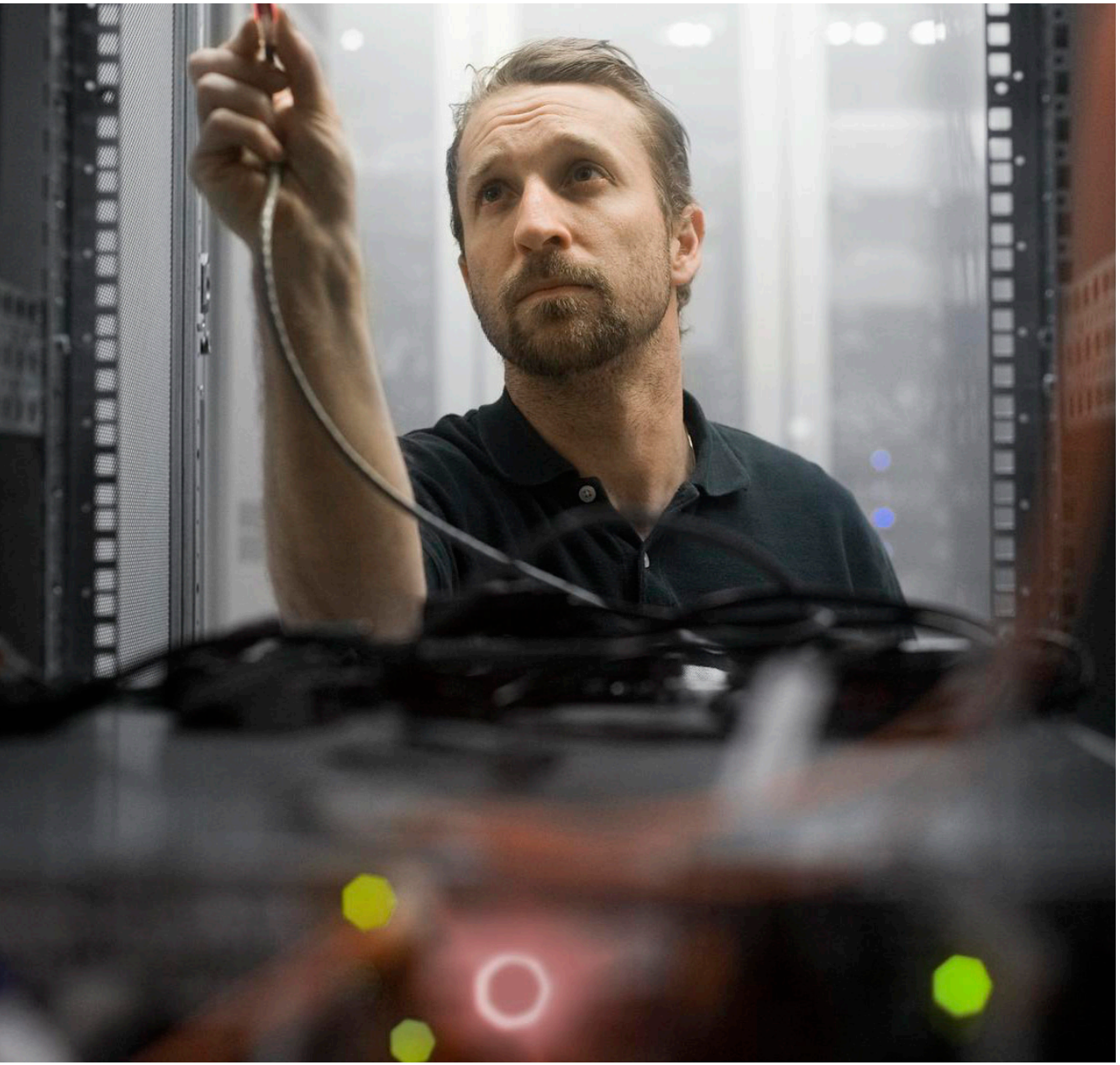
O ransomware, combinado com engenharia social, pode criar um ataque muito eficaz.

Ransomware oculto

O ransomware também pode entrar sem ser detectado em firewalls que não conseguem descriptografar e inspecionar o tráfego da Web criptografado por SSL. Soluções de segurança de rede legadas normalmente não têm capacidade de inspecionar tráfego criptografado por SSL/TLS ou seu desempenho é tão baixo que elas se tornam inutilizáveis ao realizar a inspeção. Além disso, os criminosos cibernéticos aprenderam a ocultar o malware em tráfegos criptografados.

O uso da criptografia por SSL/TLS (Secure Sockets Layer/ Transport Layer Security) continua em crescimento, o que resultou em invasões despercebidas e que afetaram pelo menos 900 milhões de usuários em 2015.[2]

[2] Relatório anual de ameaças da Dell Security de 2016



Conclusão

A SonicWALL e One Identity conseguem aprimorar a proteção em sua organização ao inspecionar todos os pacotes e governar todas as identidades. Dessa forma, seus dados são protegidos onde quer que eles estejam, além do compartilhamento de inteligência para mantê-lo seguro contra diversas ameaças, inclusive ransomware.

Acesse o site de Produtos de segurança de rede Dell SonicWALL.

Sobre a Dell Security

As soluções da Dell Security ajudam na criação e manutenção de uma base de segurança sólida com soluções interconectadas que abrangem toda a empresa. Desde endpoints e usuários a redes, dados e identidades, as soluções da Dell Security mitigam riscos e reduzem a complexidade para que seus negócios evoluam. www.dell.com/security

Se você tiver dúvidas sobre o possível uso destematerial, entre em contato com:

Dell
www.dell.com/security

Consulte nosso site para obter informações sobre osescritórios regionais ou internacionais.

Ebook-NS-Ransomware-US-VG-29223