SONICWALL

COME IL RANSOMWARE PUÒ PRENDERE IN OSTAGGIO LA TUA AZIENDA

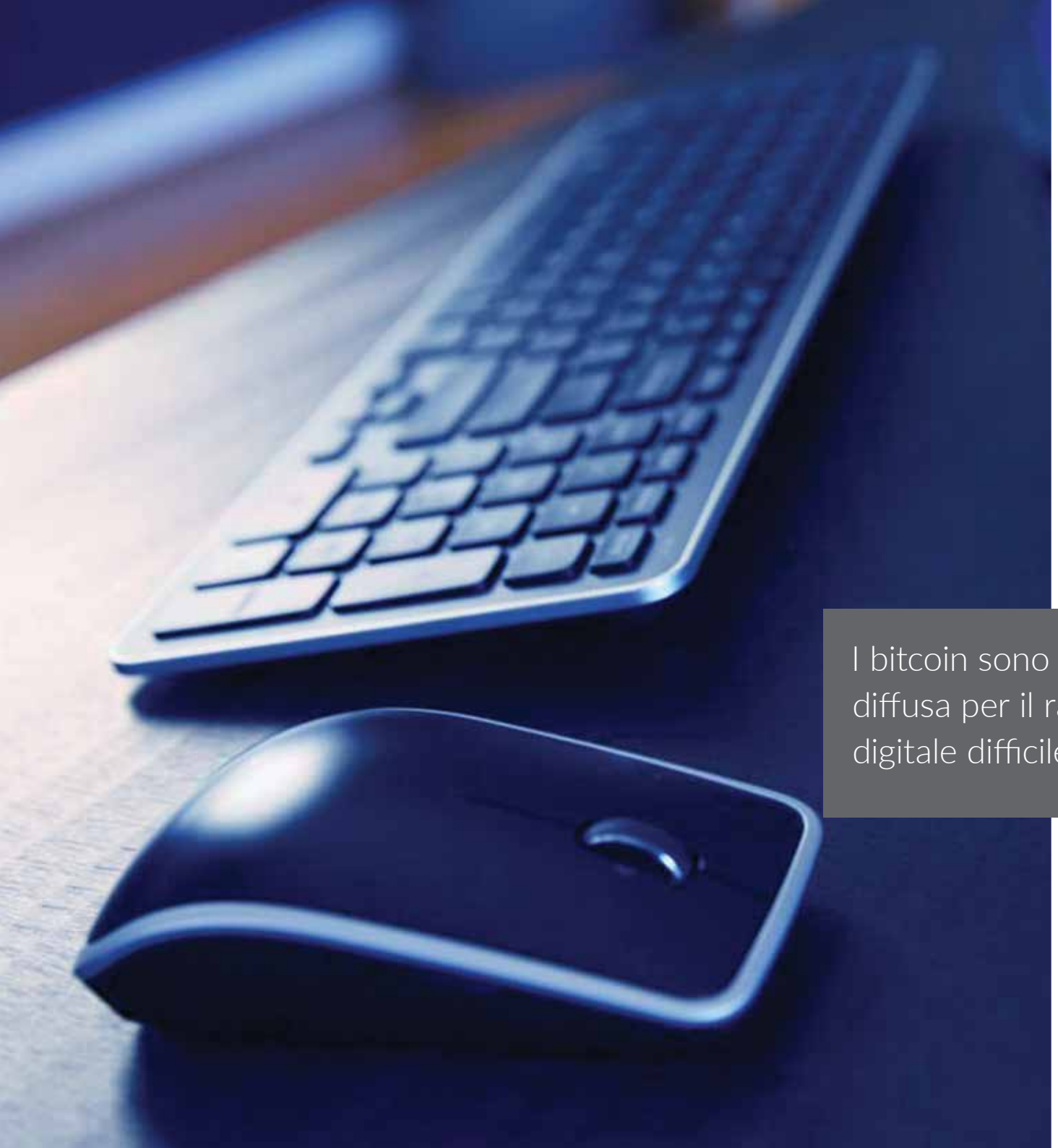
Cosa sono gli attacchi ransomware e come vengono distribuiti

Introduzione

Il ransomware è una forma di malware che impedisce l'accesso ai dati o ai sistemi fino a quando la vittima non paga un riscatto per rimuovere questa limitazione. Il ransomware esiste da diversi anni, ma ultimamente è diventato molto più popolare e redditizio. CryptoLocker, CryptoWall e RSA4096 sono solo alcuni esempi di ransomware conosciuti.

Secondo l'FBI, nei primi tre mesi del 2016[1] sono già stati pagati più di 209 milioni di dollari di riscatto negli Stati Uniti, rispetto ai 25 milioni di dollari dell'anno precedente.

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



Come funziona il ransomware

Il ransomware può infiltrarsi in un sistema utilizzando vari metodi per indurre la vittima a scaricare e installare un'applicazione dannosa. Una volta installata su un dispositivo, l'applicazione si insinua nel sistema e cripta i file sul disco fisso oppure blocca l'intero sistema. In alcuni casi può bloccare l'accesso al sistema visualizzando immagini o un messaggio sullo schermo del dispositivo dell'utente, in modo da convincerlo a pagare un riscatto all'operatore del malware per ottenere la chiave di crittografia necessaria per sbloccare i file o il sistema.

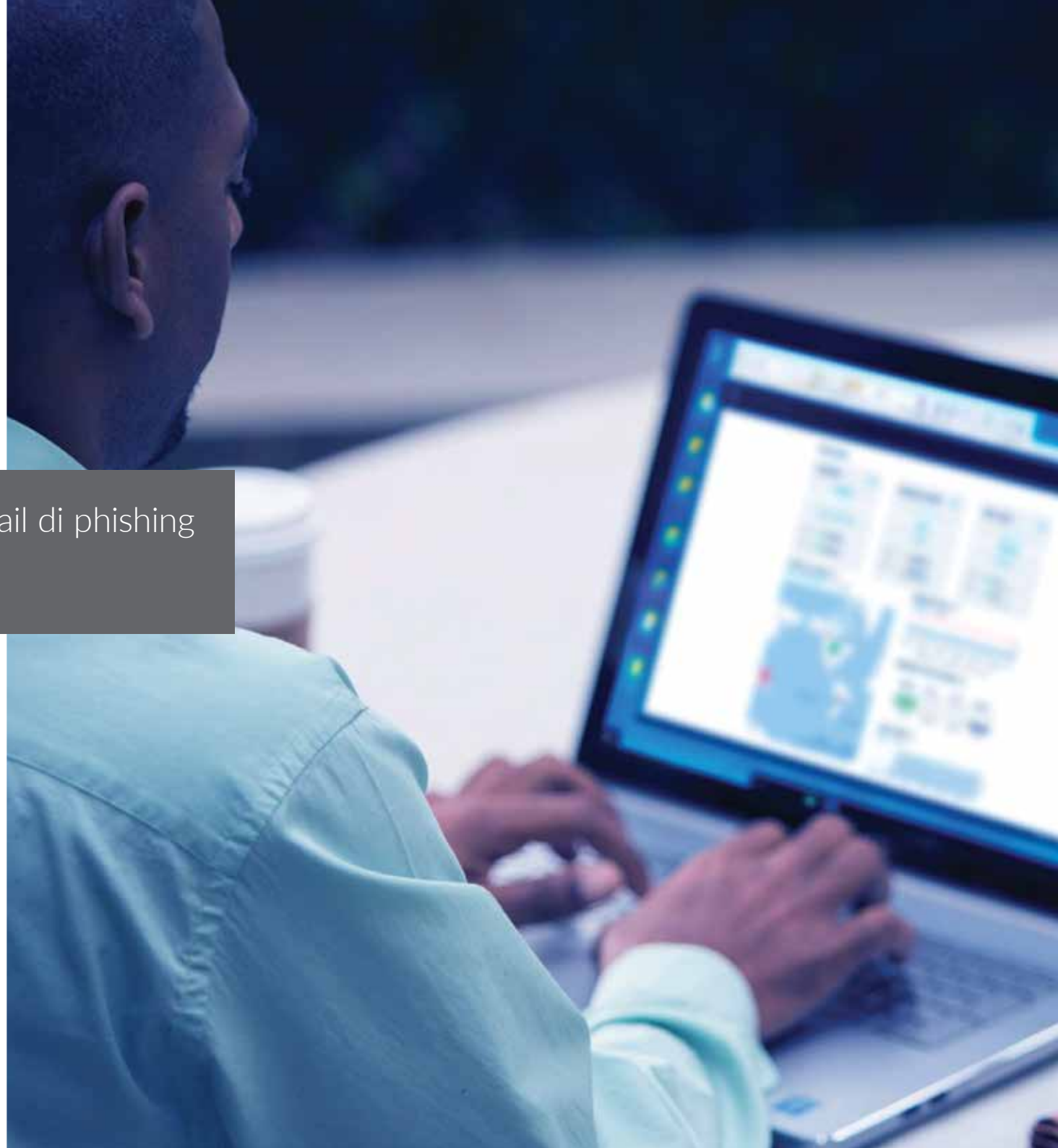
I bitcoin sono una forma di pagamento molto diffusa per il ransomware, essendo una valuta digitale difficile da rintracciare.

SONICWALL®

E-mail di phishing

Uno dei metodi più comuni per distribuire il ransomware sono le e-mail di phishing, che cercano di indurre i destinatari ad aprire un messaggio e-mail e a cliccare su un link a un sito web. Questo sito può richiedere l'inserimento di informazioni sensibili o può contenere malware, ad esempio ransomware, che verrà scaricato sul sistema della vittima.

Il 23% dei destinatari apre le e-mail di phishing e l'11% clicca sugli allegati[2].

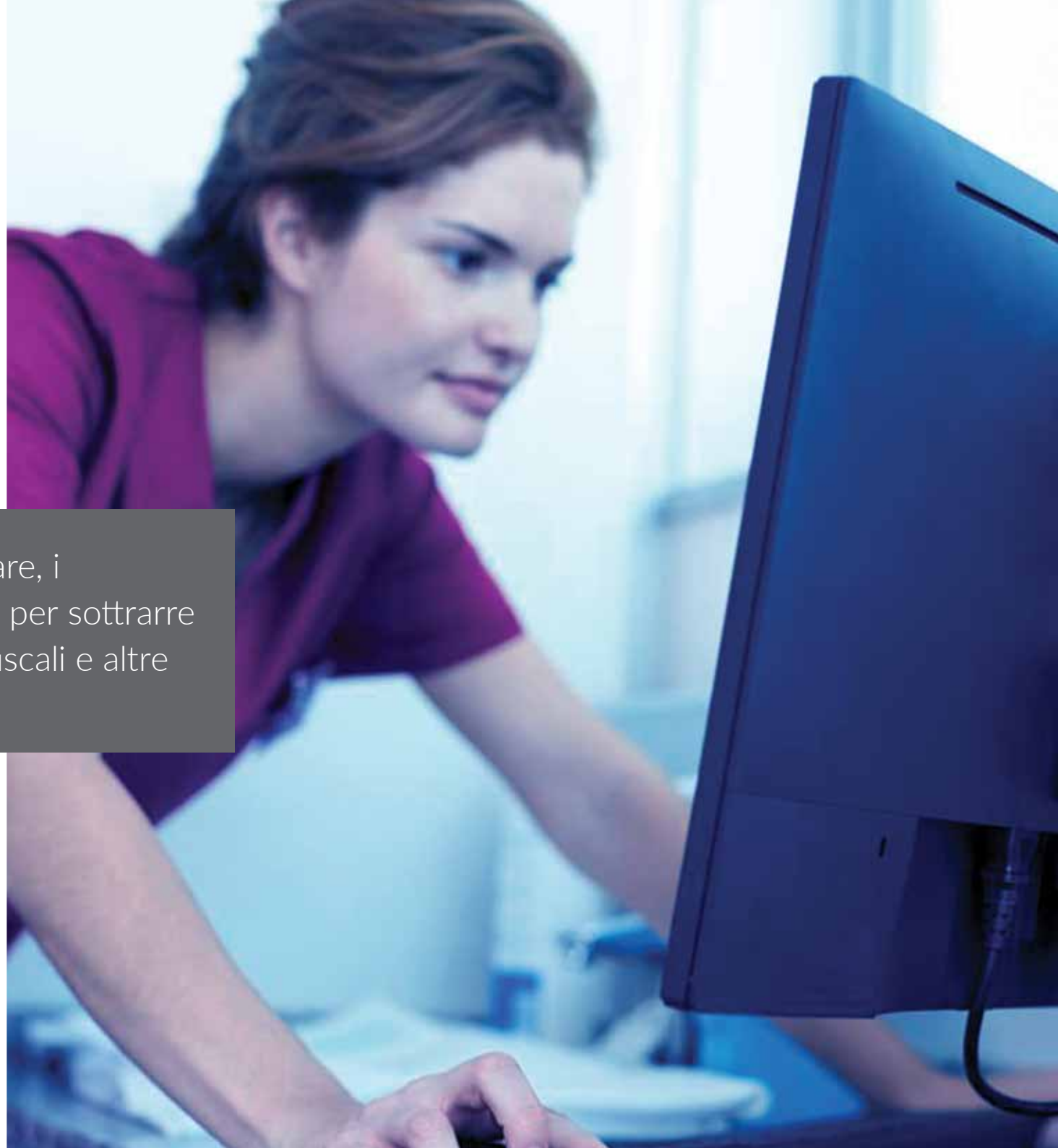


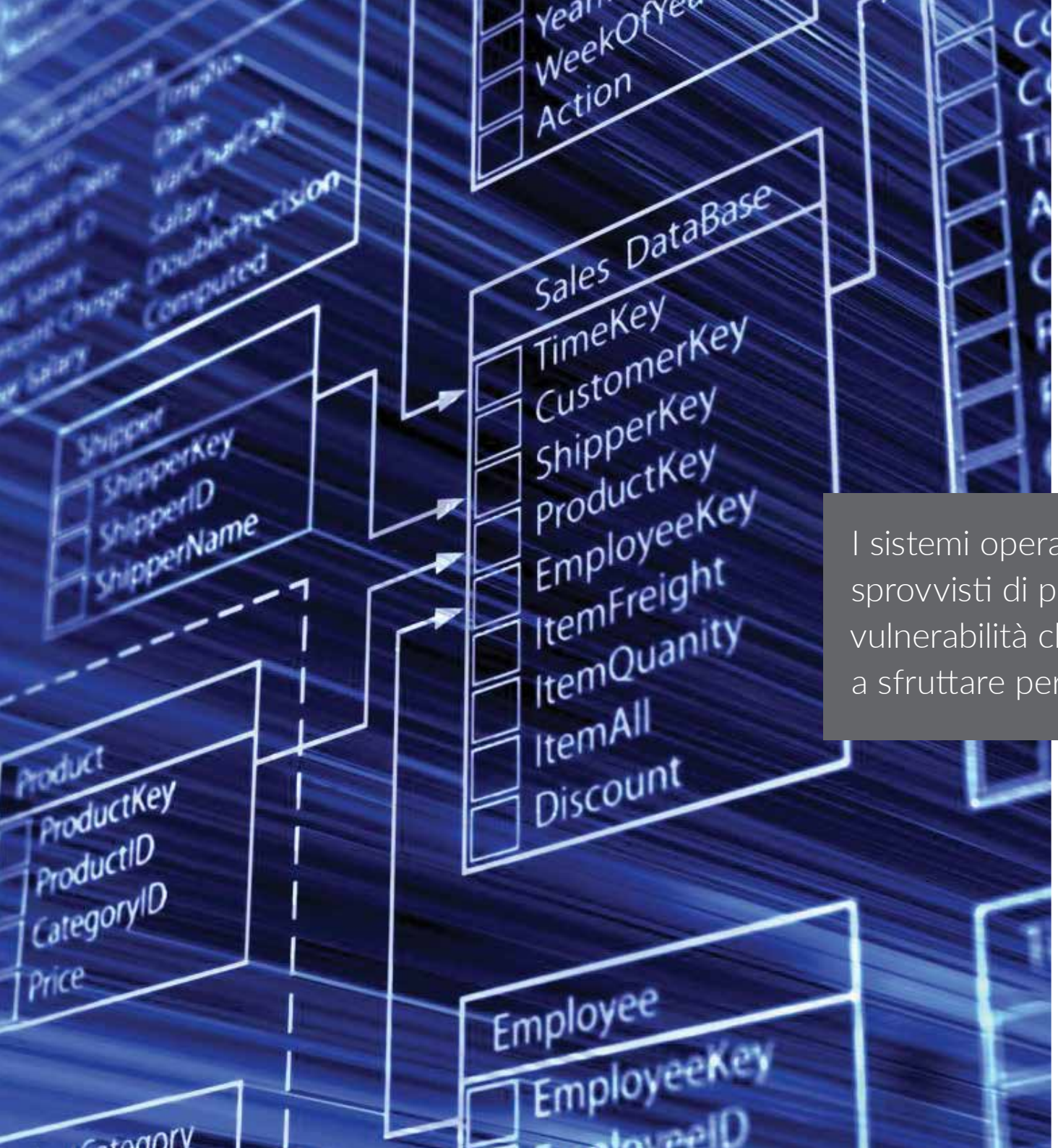
2 2015 Verizon Data Breach Investigation Report

Malvertisement

Un'altra forma di distribuzione del ransomware molto diffusa è il cosiddetto malvertising, una contrazione del termine "malicious advertising", che utilizza le pubblicità online per diffondere il ransomware. L'autore dell'attacco si infiltra nei network pubblicitari, a volte presentandosi come un inserzionista o un'agenzia, e inserisce pubblicità contenenti malware in siti web legittimi. Gli ignari visitatori di questi siti non devono neppure cliccare sulla pubblicità, e già il loro sistema è infetto.

Oltre che per lanciare il ransomware, i “malvert” possono essere utilizzati per sottrarre numeri di carte di credito, codici fiscali e altre informazioni riservate.



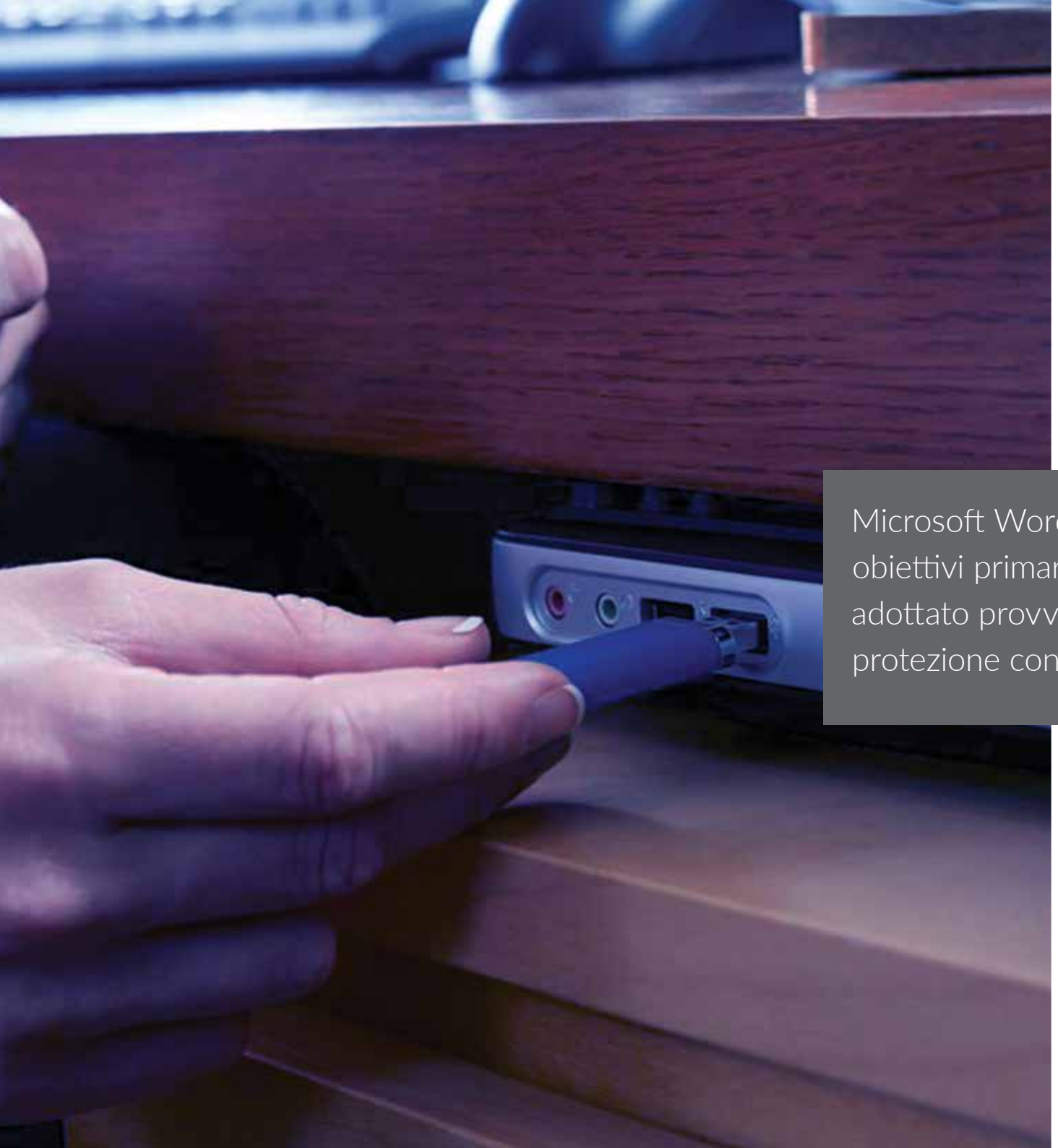


Sfruttamento di sistemi e applicazioni privi di patch

Molti attacchi sono basati su vulnerabilità note di sistemi operativi, browser e applicazioni di uso comune. I criminali informatici sono in grado di sfruttare queste vulnerabilità per lanciare i loro attacchi ransomware verso sistemi che non sono aggiornati con le patch software più recenti.

I sistemi operativi, le applicazioni e i browser sprovvisti di patch possono contenere vulnerabilità che i criminali informatici riescono a sfruttare per lanciare attacchi ransomware.

SONICWALL®



Dispositivi esterni

I dispositivi esterni come le unità USB, utilizzati per archiviare e trasferire i file, sono bersagli ideali per diffondere il ransomware su più sistemi. Alcuni di questi file contengono una funzionalità avanzata, ovvero le macro, che può essere utilizzata dagli hacker per eseguire il ransomware quando il file viene aperto.

Microsoft Word, Excel e PowerPoint sono obiettivi primari, sebbene Microsoft abbia adottato provvedimenti per migliorare la protezione contro questa minaccia in Office 2016.

SONICWALL®

Perché i metodi tradizionali non riescono a prevenire gli attacchi ransomware

Molti dei tradizionali controlli di sicurezza spesso non sono in grado di rilevare il ransomware in quanto analizzano solo comportamenti anomali e indicatori di compromesso standard. Una volta installato su un sistema, il ransomware si comporta come un'applicazione di sicurezza e può negare l'accesso ad altri sistemi/programmi. In genere limita unicamente l'accesso all'interfaccia, senza compromettere i file e i sistemi sottostanti.

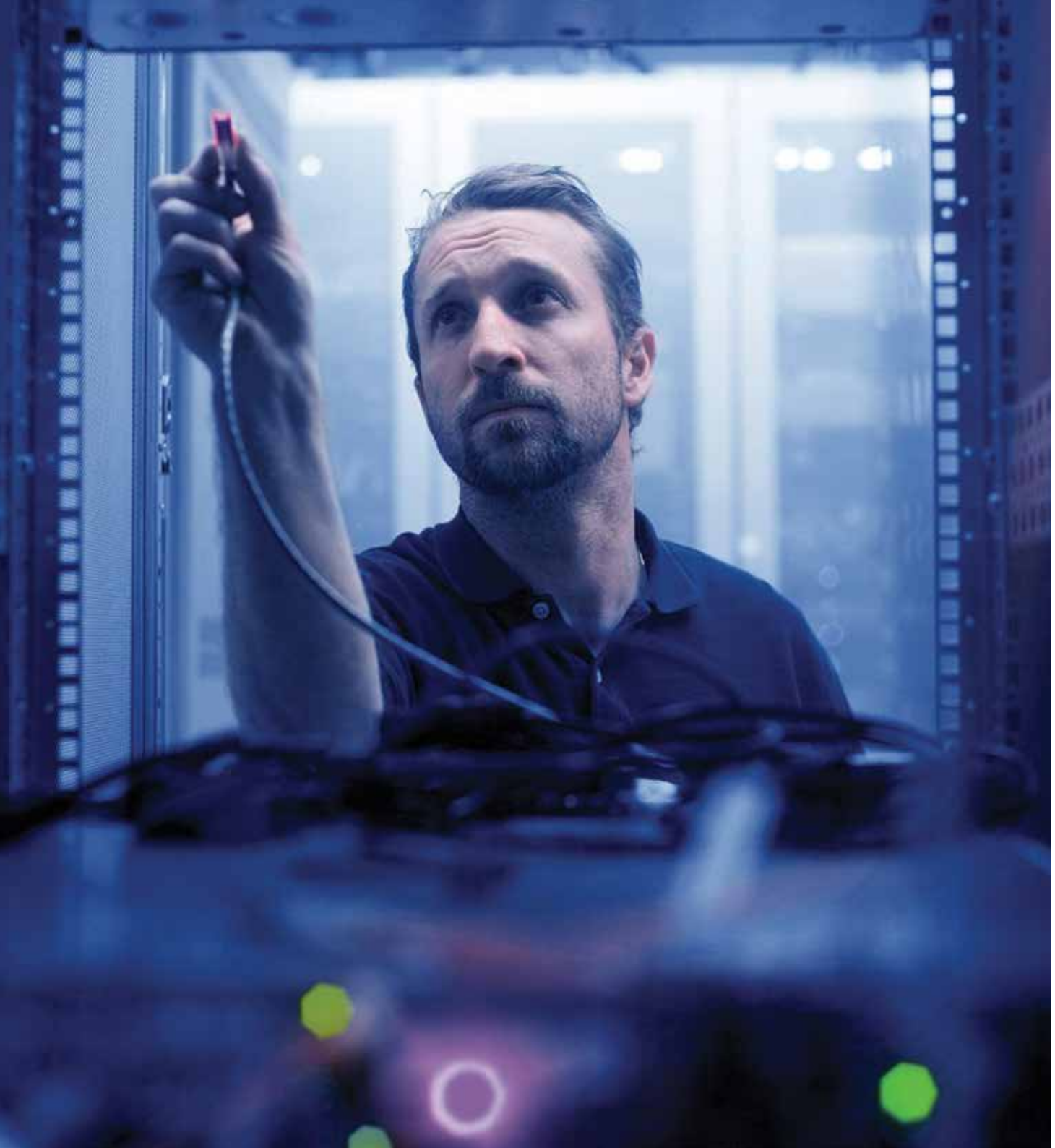
Il ransomware, se abbinato al "social engineering", può creare un attacco molto efficace.

Ransomware nascosto

Il ransomware può anche eludere il controllo dei firewall che non sono in grado di decrittografare e ispezionare il traffico web crittografato tramite SSL. Le tradizionali soluzioni di sicurezza per la rete non hanno la capacità di esaminare il traffico SSL/TLS crittografato, oppure le loro prestazioni sono così limitate da renderle inutilizzabili in fase di analisi. I criminali informatici hanno ormai imparato come nascondere il malware nel traffico crittografato.

L'uso della crittografia SSL/TLS (Secure Sockets Layer / Transport Layer Security) continua ad aumentare, con almeno 900 milioni di utenti colpiti da un attacco informatico nel 2015.[3]

3 Report annuale sulle minacce di SonicWall Annual Threat Report, 2016



Conclusioni

SonicWall può potenziare la sicurezza nella tua organizzazione mediante l'analisi di ogni pacchetto e la gestione di ogni identità. Questo approccio protegge i tuoi dati in qualsiasi luogo e offre una difesa efficace contro numerose minacce, tra cui il ransomware, grazie alla condivisione delle informazioni.

Visita la pagina web con i prodotti per la sicurezza della rete di SonicWall.

SONICWALL®

Informazioni su SonicWall

Da oltre 25 anni SonicWall è il partner di fiducia nel campo della sicurezza. Dalla sicurezza della rete alla protezione degli accessi fino alla sicurezza dell'email, SonicWall ha costantemente ampliato la sua gamma di prodotti consentendo alle organizzazioni di fare innovazione, accelerare e crescere. Con oltre un milione di dispositivi di sicurezza in quasi 200 paesi e aree del mondo, SonicWall permette ai suoi clienti di guardare al futuro con fiducia.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Consulta il nostro sito Web per informazioni sulle sedi regionali e internazionali.
www.sonicwall.com

Ebook-NS-Ransomware-EU-IMAG-29223 -D1

SONICWALL®