SONICWALL®

I TUOI DATI IN OSTAGGIO

Perché il ransomware è il metodo preferito dai criminali informatici di oggi

BLOCCA IL RANSOMWARE UNA VOLTA PER TUTTE

Gli autori delle minacce e i criminali informatici sono sempre stati abili nel violare le reti e rubare dati, ma spesso serviva tempo e fatica per trasformare quei dati in valuta reale.

Con l'introduzione dei ransomware non è più necessario esfiltrare i dati e rivenderli sui mercati clandestini.

Oggi è più semplice violare una rete e crittografarne i dati, per poi chiedere un riscatto alla vittima dell'attacco. In mancanza di una strategia di sicurezza informatica proattiva in tempo reale, alle aziende resta ben poco da fare.

La presente guida spiega cosa sono i ransomware e come le soluzioni sandbox basate su cloud possono mitigare gli attacchi prima che violino il tuo ambiente e prendano in ostaggio i tuoi dati... e la tua azienda.

Introduzione

Pag. 3 - Ransomware: sei protetto contro i prossimi attacchi?

Pag. 4 - Le sette peculiarità degli attacchi ransomware più efficaci

Pag. 5 - Ransomware-as-a-Service (RaaS) – la nuova normalità

Pag. 6 - L'importanza delle sandbox di rete per bloccare i ransomware

Pag 7 - Bloccare il ransomware con Capture ATP

Pag 8 - SonicWall Capture ATP contro il malware più recente

SONICWALL®

Ransomware: sei protetto contro i prossimi attacchi?

Sarai tu la prossima vittima di un ransomware? I cybercriminali riusciranno a crittografare i tuoi dati e tenerli in ostaggio finché non pagherai un riscatto?

Tutte le aziende, di qualsiasi dimensione e settore in tutto il mondo, sono esposte al rischio di un attacco ransomware. I media riportano generalmente gli attacchi subiti dai grandi istituti, come il caso dell'Hollywood Hospital che nel 2016 è rimasto offline per oltre una settimana dopo che un ransomware ne aveva crittografato i file e richiesto un'ingente somma per decrittografarli.

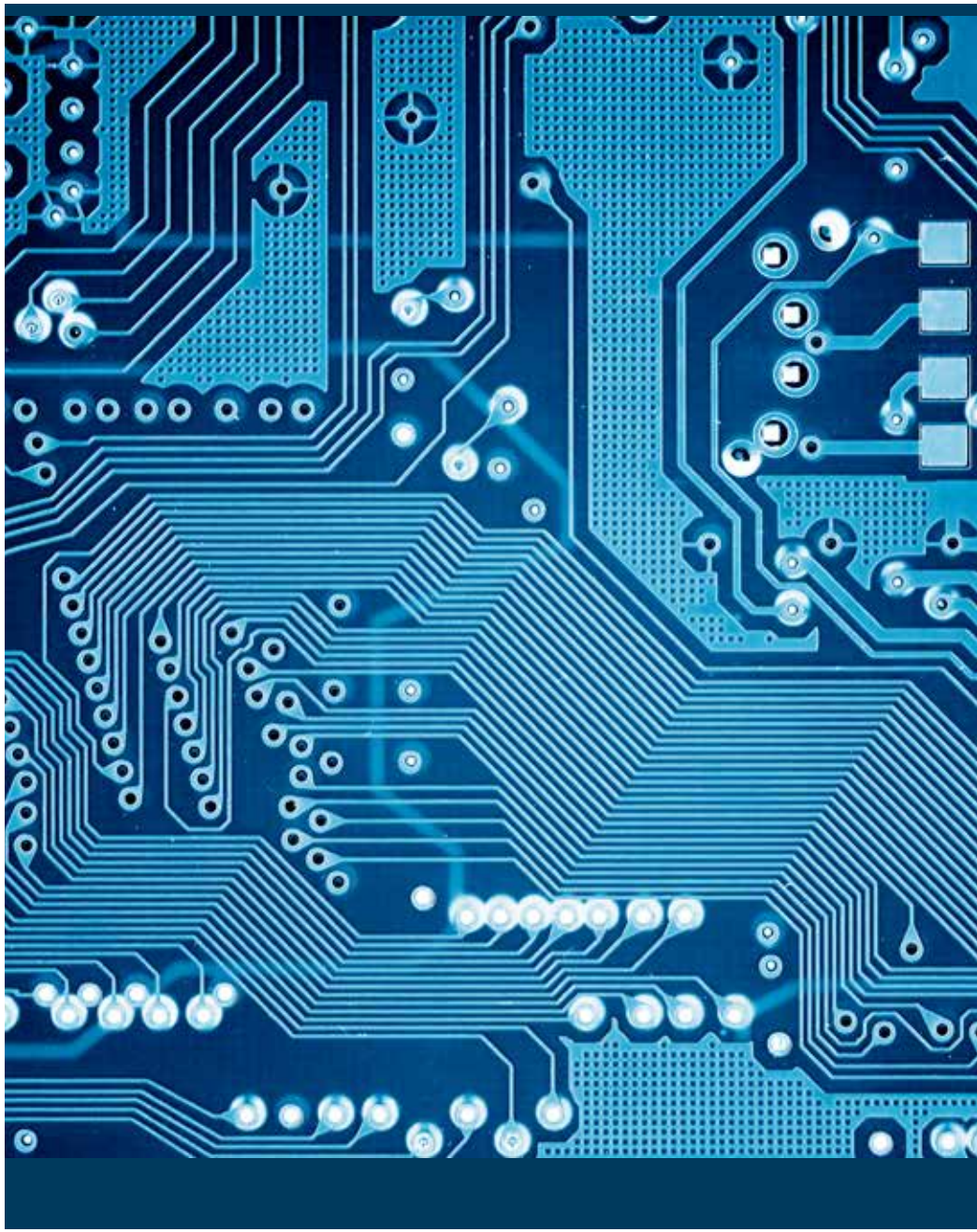
Tuttavia il fenomeno riguarda anche le piccole aziende. Secondo una ricerca di Kaspersky, infatti, le più colpite sono proprio le piccole e medie imprese: nell'arco di 12 mesi il 42% delle PMI ha subito un attacco ransomware.

Di queste, una su tre ha pagato il riscatto, ma una su cinque non è più tornata in possesso dei propri file, pur avendo pagato. Che si lavori in una grande organizzazione o in una piccola azienda, siamo comunque esposti a questo rischio.

LEGGI LA STORIA COMPLETA >

SONICWALL®

Le sette peculiarità degli attacchi ransomware più efficaci



Nel 2016 SonicWall ha rilevato un aumento del 600% delle famiglie di ransomware. Nel nostro Annual Threat Report 2017 abbiamo esaminato un'ampia varietà di forme di ransomware e vettori di attacco, alcuni efficaci, altri meno.

Da cosa dipende quindi l'efficacia di un attacco ransomware? Per difendersi meglio da una delle forme di malware più insidiose della storia occorre comprendere le sette caratteristiche distintive della strategia di una campagna ransomware.

1. Ricerca intelligente del bersaglio da colpire

Un hacker esperto sa come trovare le vittime giuste in un'azienda e quale messaggio utilizzare per colpirle. Sa anche che enti pubblici e servizi sanitari sono un ambiente ideale.

Sebbene le aziende stiano educando il personale a prestare maggiore attenzione, molti utenti continuano a cliccare su e-mail e post dei social media abilmente falsificati. Inoltre, gli hacker possono accedere a qualunque database pubblico per la generazione di lead e trovare le vittime ideali per una campagna di phishing.

2. Distribuzione efficace

Dato che il 65% degli attacchi ransomware avviene tramite e-mail, un malintenzionato può facilmente inviare un allegato infetto al reparto contabilità dichiarando che si tratta di una fattura non pagata. Un attacco di questo tipo ha messo in ginocchio per due settimane l'azienda di servizi BWL di Lansing, nel Michigan, e le è costato circa 2,4 milioni di dollari.

GUARDA L'ELENCO COMPLETO >

SONICWALL®

Ransomware-as-a-Service (RaaS) – la nuova normalità

I modelli di business comportano sempre la scelta di un metodo di distribuzione: vendita diretta, distributori o una combinazione di entrambe le opzioni? Lo stesso principio vale per chi sviluppa ransomware.

Molti scelgono di creare un codice efficace e venderlo come kit, una soluzione che elimina molti rischi e l'onere della distribuzione e permette di incassare comunque una parte dei proventi.

Nel corso dell'anno passato, e fino agli attacchi WannaCry su vasta scala, tra un picco e l'altro si è registrato un certo numero di piccoli attacchi mirati, basati su exploit kit rielaborati. SonicWall ha scoperto un panorama vario e caotico di malware elaborati da sviluppatori sia esperti che dilettanti, ransomware modificati e RaaS riassemblati.

- Trumplocker
- AlmaLocker
- Jigsaw
- Lambda
- Derialock
- Shade
- Popcorn
- Jaff

Di recente un autore ha mostrato quanto sia facile lanciare un attacco ransomware in appena un'ora pur **non avendo alcuna competenza di pirateria informatica**.

Cosa significa questo per un'azienda come la tua? È il caso di preoccuparsi? In parole semplici, la presenza di attacchi da più fonti comporta un maggior numero di attacchi. Ma per fortuna c'è SonicWall a proteggerti.

CONTINUA A LEGGERE >

SONICWALL®

L'importanza delle sandbox di rete per bloccare i ransomware

I firewall di nuova generazione sfruttano le firme e l'euristica con grande efficacia, ma quando si tratta di proteggersi dagli attacchi dannosi attualmente in circolazione, non sono più sufficienti. Gli attacchi mirati e le minacce zero-day richiedono l'uso di un sistema sandbox aggiuntivo per garantire una protezione realmente efficace.

Le minacce esterne stanno aumentando in modo preoccupante. Gli aggressori combinano la natura opportunistica dell'automazione e l'approccio dei produttori di software per sviluppare costantemente le proprie minacce, con l'obiettivo di arrivare inosservati il più lontano possibile.

Considerando i danni che un'azienda subisce nel caso di una violazione dei dati o di un attacco ransomware, individuare un codice maligno prima che entri e agisca nella propria rete è ormai un imperativo per le organizzazioni IT.

La vera sfida non consiste tanto nel ransomware in sé, che magari è già diffuso su internet, bensì negli attacchi mirati e nelle minacce zero-day.

Gli attacchi mirati vengono perpetrati con un codice mai visto prima, creato ad hoc per l'organizzazione presa di mira, mentre le minacce zero-day sfruttano le vulnerabilità appena scoperte per le quali non sono ancora disponibili patch correttive.

Le aziende dovrebbero preoccuparsi soprattutto per questi tipi di aggressioni, che in genere sono ben più efficaci e dannose delle precedenti controparti. Dunque, qual è il modo migliore per impedire che una minaccia si diffonda all'interno della propria rete?

Scarica il rapporto IDC gratuito per capire come le sandbox aiutano a prevenire le minacce avanzate.


IDC

IDC ANALYST CONNECTION

Addressing Advanced Threats Through Multiple Sandbox Options

Rapporto IDC gratuito

Contrastare le minacce avanzate con diverse opzioni della sandbox

SCARICA IL RAPPORTO >

SONICWALL®

Bloccare il ransomware con Capture ATP

SonicWall Capture Advanced Threat Protection (ATP) è un servizio sandbox multi-engine basato su cloud, progettato per rilevare e bloccare attacchi zero-day sconosciuti (ad es. ransomware) a livello del gateway, con funzioni di risoluzione automatica.

ATP è l'unico servizio di rilevamento delle minacce avanzate che utilizza il sandboxing multilivello in combinazione con l'emulazione completa del sistema e tecniche di virtualizzazione per analizzare il comportamento del codice sospetto.

Questa potente combinazione consente di rilevare più minacce rispetto alle soluzioni sandbox basate su un unico motore, che sono specifiche per l'ambiente di calcolo e suscettibili a tecniche di evasione.

- **Blocco del ransomware in tempo reale**
- **Analisi di un'ampia varietà di file**
- **Analisi multi-engine delle minacce avanzate**
- **Rapida distribuzione delle firme di riparazione**
- **Creazione di rapporti e avvisi**
- **Blocco fino all'identificazione**

Per ulteriori informazioni sul servizio SonicWall Capture Advanced Threat Protection (ATP), scarica la scheda tecnica o visita **sonicwall.com/capture**.

Come funziona Capture ATP?

SCARICA LA SCHEDA TECNICA >

SONICWALL®

Demo: SonicWall Capture ATP contro il malware più recente

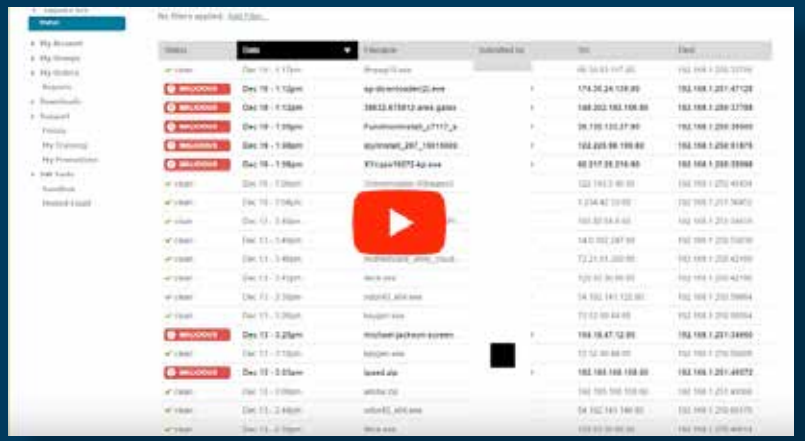
SonicWall Capture Advanced Threat Protection, un servizio basato su cloud disponibile per i firewall SonicWall, rileva e blocca le minacce avanzate al gateway finché non viene identificata la loro natura, proteggendo i clienti dal crescente pericolo delle minacce zero-day (ad es. ransomware).

Quanto è potente Capture ATP? Abbiamo preso il malware più recente e pericoloso che si trova in internet e lo abbiamo sottoposto alla tecnologia SonicWall per mostrare come riusciamo a bloccare le minacce avanzate reali che ogni giorno mettono a rischio la sicurezza delle aziende.

Con il solo utilizzo di Gateway Anti-Virus (GAV) e Capture ATP, dimostriamo come il malware viene identificato e neutralizzato in tempo reale. Capture ATP riesce a scoprire quello che il malware intende fare con le applicazioni, il sistema operativo, il software e l'hardware.

A quel punto, un'infrastruttura di intelligence globale delle minacce distribuisce rapidamente le firme di riparazione delle minacce appena rilevate a tutte le appliance di sicurezza di rete SonicWall, prevenendo un'ulteriore infiltrazione.

Per i clienti, questo si traduce in un'elevata efficacia in termini di sicurezza, in tempi di risposta rapidi e in una riduzione del costo totale di proprietà.



GUARDA LA DEMO COMPLETA >

SONICWALL®

Informazioni su SonicWall

Da oltre 25 anni SonicWall è il partner di fiducia nel campo della sicurezza. Dalla protezione di rete alla sicurezza degli accessi fino alla protezione dell'email, SonicWall ha costantemente ampliato la sua gamma di prodotti permettendo alle aziende di fare innovazione, accelerare e crescere. Con oltre un milione di dispositivi di sicurezza in quasi 200 paesi e aree del mondo, SonicWall consente 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

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

SONICWALL®