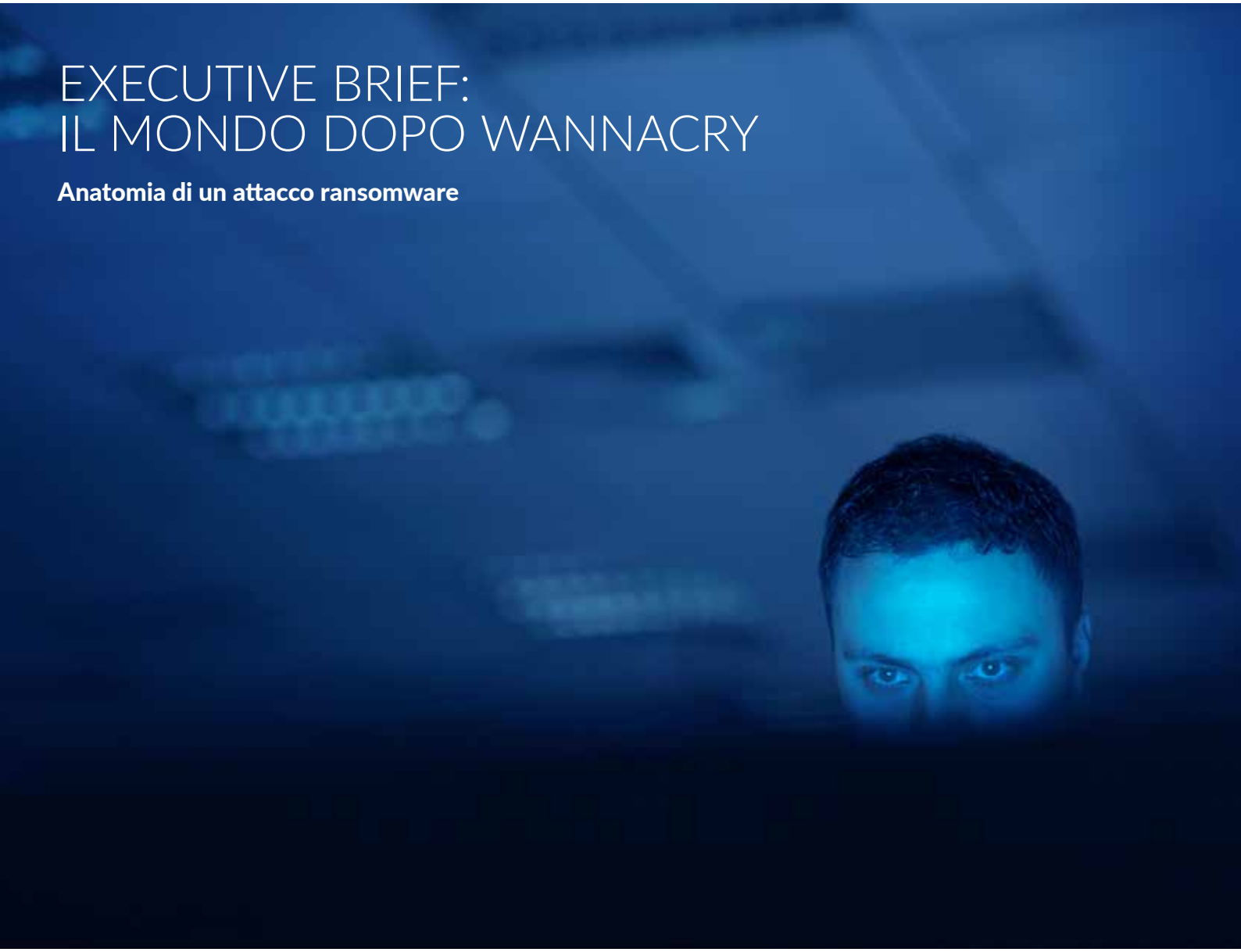
SONICWALL

EXECUTIVE BRIEF: IL MONDO DOPO WANNACRY

Anatomia di un attacco ransomware



Abstract

La mancanza di iniziativa nell'acquisire le best practice nel campo della sicurezza di rete porta spesso a risultati devastanti. Un recente attacco ransomware ha monopolizzato i titoli dei giornali e avuto un impatto globale. Questo brief si propone di analizzare come i cybercriminali hanno effettuato questo attacco, le sfide continue che esso rappresenta per l'IT e le lezioni apprese per evitare attacchi futuri.

Una storia comune

È stata una storia fin troppo comune. Di recente, i criminali informatici hanno violato la rete di un'azienda attraverso il phishing in un'e-mail contenente il ransomware WannaCry. Un allegato e-mail è stato aperto su un computer non protetto da patch, causando conseguenze devastanti. Alla domanda sul perché il sistema non fosse stato aggiornato con le patch, il proprietario dell'azienda ha risposto «Non pensavo che la patch fosse così importante».

Anatomia di un attacco

Se si considera con quanta facilità questa azienda avrebbe potuto evitare la violazione, viene veramente «voglia di piangere» («WannaCry»). Questo particolare attacco di ransomware su larga scala ha infettato oltre 250.000 sistemi in più di 150 paesi, comprese numerose strutture sanitarie nel Regno Unito e addirittura un paio di importanti società di telecomunicazioni in Spagna.

WannaCry non è che un esempio delle minacce che risultano dalla combinazione di un ransomware e un worm, in grado di sfruttare un *exploit* del protocollo di condivisione file SMB. L'ipotesi è che un kit di exploit (in questo caso, EternalBlue) sia stato creato da certe agenzie governative e, quindi, presumibilmente rubato da criminali informatici.

Sebbene finiscano sempre più spesso nei titoli dei giornali, gli attacchi ransomware non sono nulla di nuovo. Gli exploit sono un evento quotidiano. La scusa di dire «Non ne sapevo nulla» non varrà ancora per molto.

Nell'aprile del 2017, Shadow Brokers ha pubblicato illegalmente EternalBlue come parte di un dump contenente molti altri exploit sviluppati dalla NSA. I criminali hanno quindi sfruttato gli elementi di tale kit di exploit per creare una nuova forma di ransomware estremamente aggressiva in grado di sfruttare un attacco in stile worm contro macchine connesse in rete, utilizzando varie funzioni di lettura/scrittura del sistema operativo Windows. Questo particolare exploit riguarda diverse versioni di sistemi operativi Microsoft Windows, tra cui numerose versioni attualmente a fine vita. Sebbene Microsoft abbia rilasciato un gran numero di patch per affrontare questa vulnerabilità, l'attacco mantiene la sua pericolosità, in quanto molte grandi organizzazioni non hanno applicato la patch.

La prima versione del pacchetto worm/ransomware era dotata di un *kill switch* utilizzato accidentalmente per disattivare la funzionalità worm e che ne ha rallentato l'avanzata. Tuttavia, le oltre 20 versioni successive alla prima non presentano questo punto debole. Inoltre, è importante utilizzare tecnologie in grado di arrestare ogni versione nota di ransomware e tecnologie che possano rilevare gli attacchi di nuovi ransomware.

Conclusione

Oltre 114 nuovi virus e varianti vengono creati ogni sessanta secondi. *WannaCry* non è certamente il primo exploit a sfruttare questa forma di attacco e sicuramente non sarà l'ultimo. Le organizzazioni devono prendere atto di queste nuove realtà sull'attuale campo di battaglia informatico.

Per saperne di più. Leggete il nostro Brief sulle soluzioni: 7 best practice per fermare il ransomware.

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per eventuali domande in merito all'utilizzo potenziale del presente materiale, si prega di contattare:

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

Per maggiori informazioni, visitare il nostro sito web.
www.sonicwall.com