SONICWALL

CMIT Solutions of Metrolina mitiga i cyber attacchi con SonicWall Capture Client

CMIT Solutions ha scelto SonicWall per proteggere i suoi clienti con una piattaforma di cybersecurity completa.

Fondata nel 1996 come azienda per la formazione e il supporto IT personalizzati, CMIT Solutions conta oggi più di 900 leader di settore e personale tecnico per offrire supporto IT in tutta l'America del Nord. Nel 2008, CMIT Solutions ha adottato un modello di fornitura di servizi gestiti e da allora si è concentrata sul mercato delle piccole e medie imprese (PMI) locali.

Esigenze dell'azienda

A causa della crescente minaccia posta dai ransomware e da altri attacchi, i fornitori di servizi di sicurezza gestiti (MSSP) come CMIT Solutions hanno sempre più bisogno di una soluzione di sicurezza endpoint con gestione e reportistica completamente centralizzate per tutte le aziende a cui offrono i loro servizi.

La soluzione

Per mitigare i cyber attacchi e altre minacce, CMIT Solutions of Metrolina ha iniziato a installare SonicWall Capture Client nelle sedi di tutti i suoi clienti. Un cliente di lunga data, che si affida al team di CMIT Solutions per gestire e supportare le sue 9 sedi aziendali, 150 endpoint e 15 server, ha scelto di implementare per i suoi servizi gestiti IT una combinazione di prodotti SonicWall, tra cui nove firewall NGFW della serie TZ e appliance di accesso remoto SonicWall. La soluzione includeva anche SonicWall Capture Client, un prodotto anti-malware basato sul rilevamento comportamentale progettato per bloccare gli attacchi prima e durante l'esecuzione e fornire misure di risoluzione anche in seguito.

Cosa è successo

Nel maggio 2021, questo cliente è stato colpito da una campagna di ransomware che ha tentato di lanciare 4.021 attacchi contro 162 tra endpoint e server. L'attacco è iniziato quando un dipendente ha aperto l'e-mail di un fornitore con un allegato Excel dannoso, attivandone così il contenuto interno. Da questo endpoint, l'attacco ha mappato rapidamente la rete, scaricato file aggiuntivi per propagare l'attacco e – sfruttando un exploit di Windows SMB – ha tentato di diffondersi in altre sedi dell'organizzazione, attaccando PC e server. Allo stesso tempo ha cercato di raggiungere i server in altre posizioni della rete mediante l'elevazione dei privilegi su Netlogon di Windows. Nel giro di due minuti, il malware ha fatto più di 1.000 tentativi di connessione a tre server di comando e controllo (C&C) in Europa dell'Est.

CMIT Solutions
Your Technology Team

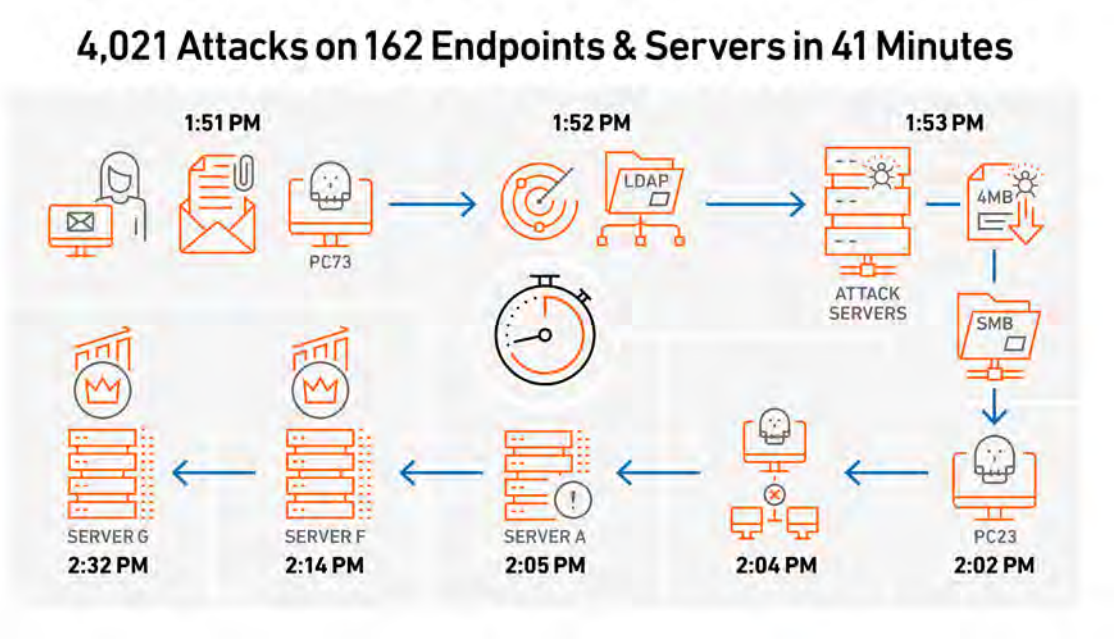
"La difesa in profondità funziona! Siamo soddisfatti delle prestazioni di Capture Client e degli altri componenti del nostro stack di sicurezza, che hanno aiutato il nostro team a limitare e a riprendersi da questo attacco. La mission di CMIT è quella di impedire ai criminali di distruggere il valore delle aziende, offrendo un eccellente supporto ai clienti e garantendo la completa efficienza dei sistemi. Ma se un aggressore riesce a superare i nostri controlli di sicurezza, siamo ugualmente pronti a ripristinare i sistemi e le informazioni, in modo che i nostri clienti abbiano la possibilità di non pagare un riscatto per accedere ai loro dati."

Emory Simmons
Presidente

Profilo del Cliente

Azienda	CMIT Solutions of Metrolina
Settore	MSSP
Paese	USA
Sito web	cmitsolutions.com/metrolina

CASE STUDY



I risultati

Alla fine, l'attacco non è riuscito a crittografare neppure un endpoint. Mentre un servizio di sicurezza DNS di terze parti ha inizialmente bloccato l'accesso al server C&C, il team di CMIT Solutions ha iniziato a ricevere segnalazioni che SonicWall Capture Client aveva bloccato ed eliminato il ransomware "Win32/Teerac - f91e9b0.exe", seguite dalla notifica che "HackTool.Win32.LAZAGNE.AC" era stato bloccato e rimosso sia da un server che dal PC originariamente infettato.

In definitiva, l'attacco è stato bloccato grazie a una combinazione di tecnologie avanzate e alla reazione immediata del team di CMIT Solutions, che ha immediatamente avviato il processo di risposta scollegando le macchine dalla rete tramite l'apposita funzione di Capture Client, bloccando i tunnel VPN tra i vari siti e consentendo a Capture Client di bloccare i movimenti laterali tra siti e server. Dal solo PC originariamente infettato sono partiti 4.021 tentativi di attacco a 162 endpoint e server. SonicWall Capture Client ha rilevato e bloccato i movimenti laterali, ha eliminato il ransomware e distrutto l'HackTool.

Una lezione da imparare

L'attacco è stato rapidamente bloccato, ma ha messo in evidenza quattro aspetti che avrebbero ulteriormente diminuito il tempo necessario al team di CMIT Solutions per reagire all'incidente:

1. Impostare Capture Client in modo da scollegare gli endpoint appena viene rilevato un malware avrebbe permesso di bloccare la prima minaccia ai server 49 minuti prima. Inoltre avrebbe consentito di isolare il PC originariamente infettato 81 minuti prima, riducendo il tempo utilizzato per cercare altre vittime nella rete WAN.
2. Attivando il filtraggio Geo-IP di SonicWall in base ai paesi di origine sarebbe stato impedito il download iniziale del malware.
3. Impostando la prevenzione delle intrusioni (IPS) sui firewall SonicWall per bloccare anche le minacce di medio livello, e non solo quelle di alto livello, avrebbe bloccato i tentativi di exploit per accedere a Windows.
4. Una maggiore consapevolezza da parte degli utenti finali avrebbe potuto impedire completamente questo attacco.

Indipendentemente dall'esito di questo attacco, CMIT Solutions prevede di rafforzare ulteriormente la sicurezza degli endpoint attivando queste funzionalità sui firewall SonicWall di nuova generazione. In questo modo, solo i computer con Capture Client installato potranno accedere a Internet.

Vantaggi di SonicWall Capture Client

- **Blocca gli attacchi avanzati prima e durante l'esecuzione**
- **Fornisce protezione e ripristino dai ransomware**
- **Offre visibilità sulle vulnerabilità delle applicazioni**
- **Applica policy per l'uso del web lontano dal firewall**
- **Consente di visualizzare e gestire facilmente lo stato dei tenant**

Scarica una prova gratuita di Capture Client:

SonicWall.com/Capture-Client

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

CaseStudy-CMIT-Metrolina-COG-4874