SONICWALL®

2024

RAPPORTO SONICWALL SUL CYBERCRIME

AFFRONTARE L'INARRESTABILE CRESCITA DEL CYBERCRIME

sonicwall.com | @sonicwall

INTRODUZIONE

UNA NOTA DAL NOSTRO CEO

Quasi 18 mesi fa abbiamo avviato il nostro approccio orientato all'ascolto dei partner in tutta SonicWall, focalizzandoci sulla comprensione delle esigenze e dei punti critici dei nostri partner e clienti e utilizzando queste informazioni per migliorare il modo in cui forniamo i nostri prodotti e servizi.

Il 2023 è stato un anno importante, che ha iniziato a mostrare i risultati di questo approccio. Abbiamo aggiunto i servizi di Solutions Granted, un fornitore di servizi di sicurezza gestiti (MSSP, Managed Security Services Provider) leader del settore, che collabora con oltre un migliaio di fornitori di servizi gestiti (MSP, Managed Service Provider) in Nord America. Inoltre, abbiamo potenziato la nostra piattaforma di sicurezza cloud per la moderna forza lavoro remota con l'acquisizione di Banyan Security, aggiungendo così soluzioni SSE, tra cui Zero Trust Network Access (ZTNA), al crescente portafoglio di prodotti SonicWall.

Queste operazioni strategiche permettono ai nostri partner MSP di offrire ai loro clienti una protezione 24x7x365 con un team di analisti ed esperti delle minacce, senza dover creare un proprio SOC interno. Abbiamo anche esteso il portafoglio SonicWall al cloud per offrire ai partner e ai loro clienti una maggiore flessibilità, che sarà essenziale per lo sviluppo continuo della piattaforma di cybersecurity di SonicWall.

I clienti potranno contare su un numero crescente di soluzioni di sicurezza, dai firewall alla sicurezza in cloud, man mano che la piattaforma SonicWall si espande. Ma come dimostra il Rapporto SonicWall 2024 sul Cybercrime, gli attori delle minacce sono instancabili e continuano a creare nuove tattiche per colpire ogni punto dell'attuale superficie di attacco in continua crescita.

Con le intrusioni dannose in crescita del 6%, il malware dell'11% e il cryptojacking del 659%, la probabilità di subire un attacco aumenta in modo vertiginoso per ogni organizzazione.

In questo ambiente volatile, le misure di sicurezza di ieri non sono più sufficienti: le aziende di ogni dimensione hanno bisogno di soluzioni collaudate e di strategie proattive basate sulle informazioni più recenti sulle minacce.

SonicWall continua a pubblicare il Rapporto sul Cybercrime con i dati di threat intelligence più recenti non solo per fornire informazioni pratiche, ma anche per promuovere la propria roadmap e creare soluzioni in grado di aiutare i suoi partner. A nome della nostra rete di partner fidati e dell'intero team SonicWall, compresi i nostri ricercatori di minacce del Capture Labs, siamo lieti di condividere questa panoramica esclusiva sulla sicurezza informatica in continua evoluzione.

Bob VanKirk
Presidente e CEO
SonicWall

Piccole falle che generano grandi profitti

I cyber attacchi fanno sempre notizia. Gli attacchi a grandi aziende rinomate o amministrazioni locali finiscono regolarmente sulle prime pagine dei giornali. Per chi segue la sicurezza informatica più da vicino, la situazione non è molto diversa: le notizie sui siti specializzati in cybersecurity sono dominate dalle violazioni a società note come Mailchimp, MGM, Activision e 23andMe.

Leggendo tutte queste notizie si potrebbe pensare che il crimine informatico sia un problema che riguarda quasi esclusivamente le grandi aziende quotate a Wall Street. Purtroppo, nulla è più lontano dalla realtà. In un blog del 2023, l'agenzia CISA ha riferito che le **piccole imprese hanno tre volte più probabilità di essere prese di mira dai cybercriminali** rispetto alle grandi organizzazioni. E questi attacchi alle PMI provocano perdite per miliardi di dollari ogni anno.

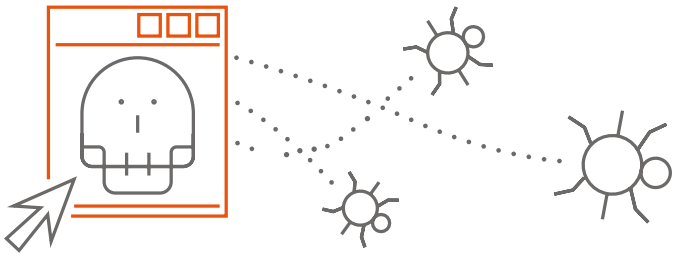
Questa è una delle ragioni principali per cui SonicWall è così impegnata a ricercare e pubblicare informazioni sulle minacce più recenti. Poiché le PMI rappresentano l'80% dei nostri utenti finali, i nostri dati offrono una visione del panorama delle minacce diversa da quella che troverete da altre parti, vale a dire un'analisi meno incentrata sui grandi gruppi multinazionali e più su aziende come la vostra.

Le principali tendenze del 2023

Forse la tendenza più rilevante che abbiamo notato nel 2023 è stata l'accelerazione. I ricercatori di minacce di SonicWall Capture Labs hanno notato un incremento del volume di attacchi a quasi tutti i livelli. **Il malware è aumentato dell'11% rispetto all'anno precedente, le minacce crittografate del 117% e il cryptojacking del 659%**. Questa tendenza si è confermata anche a livello regionale, dove gli aumenti del volume di attacchi hanno superato le diminuzioni in un rapporto di 3 a 1.

A differenza delle forze esterne contrastanti che avevamo osservato negli ultimi anni, nel 2023 gli attori delle minacce hanno mantenuto i loro metodi collaudati. Mentre ci si potrebbe aspettare che l'aumento del volume di attacchi malware e i livelli di phishing costantemente elevati siano stati accompagnati da un alto tasso di nuovi malware, abbiamo riscontrato esattamente il contrario: i malware mai visti prima rilevati sono *diminuiti* del 38% rispetto all'anno precedente.

Ma ciò non significa che gli attori delle minacce non abbiano perfezionato le loro capacità. I ricercatori di SonicWall hanno osservato la comparsa di file Microsoft OneNote come vettori iniziali per le minacce, oltre a massicce campagne per sfruttare le vulnerabilità di WinRAR e MOVEit.



I nostri dati continuano a registrare le vulnerabilità come il vettore più comune per il ransomware, e questo aspetto è destinato a rimanere tale man mano che il numero di vulnerabilità continua a crescere. **Nel 2023 è stato pubblicato un numero record di 28.834 CVE**, con un aumento del 15% rispetto ai dati del 2022. Nel mese di dicembre, i ricercatori di minacce di SonicWall hanno **scoperto e rivelato in modo responsabile la CVE-2023-51467**, una vulnerabilità che interessa ApacheOFBiz. Da allora sono stati osservati numerosi tentativi di sfruttamento.

Altre campagne hanno mostrato un livello di innovazione simile. Abbiamo osservato nuove campagne di phishing che indirizzano le potenziali vittime a pagine di login di Microsoft Outlook e American Express molto convincenti, oltre a campagne di phishing che utilizzano i codici QR per bypassare la tecnologia di scansione dei file. I cybercriminali hanno approfittato dell'inflazione e di condizioni economiche incerte per lanciare app di prestito fraudolente con funzionalità spyware e di furto delle credenziali. In altri casi hanno incorporato script di Google nei PDF per compiere furti di criptovalute, dimostrando la necessità di una maggiore vigilanza anche in ambienti apparentemente affidabili.

Dalle PMI alle grandi aziende, oggi e domani

Già ora si configura un panorama delle minacce futuro molto diverso da quello attuale, dove gli attori delle minacce continueranno a utilizzare ChatGPT e altre tecnologie di AI generativa per perfezionare i tentativi di phishing, eseguire attacchi BEC (Business Email Compromise) molto convincenti e scrivere rapidamente codice dannoso.

Ma l'intelligenza artificiale offre grandi opportunità anche ai professionisti della difesa. SonicWall è stata tra i primi ad adottare l'AI e il machine learning, con Capture ATP e RTDMI già in grado di rilevare molti di questi tipi di attacchi. Ma solo nei prossimi anni inizieremo a vedere il vero potenziale dell'AI come strumento di difesa.

Ai massimi dal 2019

Nel 2023, i ricercatori di minacce di SonicWall Capture Labs hanno registrato 6,06 miliardi di attacchi malware, con un aumento dell'11% rispetto all'anno precedente. Si tratta del volume di attacchi più alto a livello globale dal 2019, e indica che il malware è tornato ai livelli pre-pandemia mentre gli attori delle minacce diventano sempre più numerosi, intraprendenti e attivi.

Sebbene il malware sia cresciuto a livello globale, notiamo una combinazione di due tendenze diverse. Il malware è *diminuito* del 2% in Asia e in Europa, ma questo dato è stato ampiamente compensato da una forte crescita in America del Nord (+15%) e America Latina (+30%).

Questa divergenza è apparsa anche nei nostri dati specifici per settore. Il settore dell'istruzione, il più colpito dal malware nel 2022, ha registrato un calo del 3% nel 2023. Il malware rivolto alla sanità e al retail è invece aumentato del 20% e gli attacchi diretti alla pubblica amministrazione hanno registrato un picco del 38%. Ma il settore maggiormente colpito è stato quello finanziario, dove gli attacchi alle aziende sono *raddoppiati*. Questo aumento è stato sufficiente a rendere la finanza il settore più colpito che abbiamo osservato nel 2023, dopo un 2021 in fondo alla lista e un 2022 a metà della classifica.

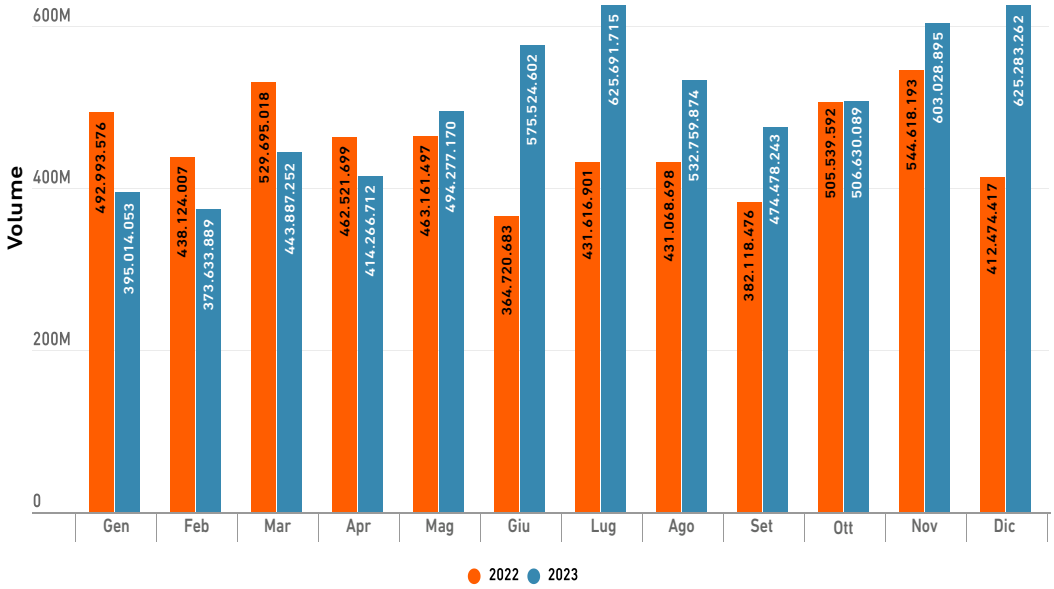
File OneNote malevoli

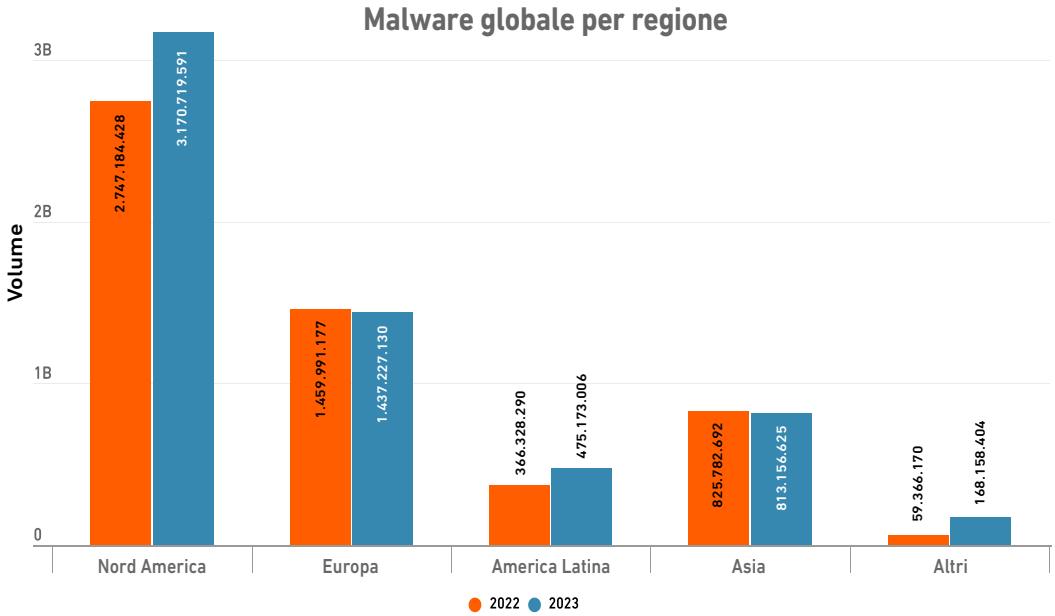
All'inizio del 2023, i ricercatori di SonicWall hanno notato che gli attori delle minacce utilizzavano un nuovo vettore iniziale per infettare i sistemi: i file Microsoft OneNote. Questi allegati dannosi venivano inviati per e-mail, insieme a una serie di tecniche di social engineering progettate per aumentare la probabilità che gli allegati venissero aperti dalla potenziale vittima cliccando sui file dannosi nascosti all'interno, attivando così l'esecuzione del payload.

I fornitori di soluzioni di sicurezza hanno rapidamente scoperto questo stratagemma e configurato il rilevamento in base a questi file di payload allegati. Gli attori delle minacce hanno quindi optato per un URL che, una volta cliccato, puntava al payload. Allo stesso tempo hanno iniziato a sovraccaricare il loro codice con byte nulli ripetuti alla fine dei file OneNote, portando le dimensioni dei file oltre i 500 MB nel tentativo di eludere molte soluzioni di scansione antivirus.

A marzo, tuttavia, l'uso di questi file aveva già iniziato a diminuire drasticamente, forse dopo che Microsoft aveva rilasciato un aggiornamento di Office che impediva l'apertura di file incorporati con estensioni pericolose in OneNote. Sebbene questa tendenza sia durata poco, si è diffusa a sufficienza per rendere i file OneNote il tipo di file Office dannoso più popolare per tutto il 2023, con Qakbot, AsyncRat, AgentTesla e altri che utilizzavano gli allegati OneNote come punto di accesso iniziale.

Volume di malware a livello globale





I PDF dannosi sono in aumento

L'uso di PDF dannosi è da tempo una delle tattiche preferite dagli attori delle minacce. Ma il loro uso è aumentato drasticamente nel 2023, passando da circa un quinto di tutti i tipi di file dannosi rilevati a quasi un terzo, un chiaro segno che questa tattica continua ad avere successo.

All'aumentare di questi attacchi è aumentata anche l'innovazione, portando alla creazione di molte varianti di rilievo. Nel 2023 SonicWall ha osservato diverse istanze di PDF contenenti codici QR: una, ad esempio, minaccia l'utente con la scadenza di una password Microsoft nel caso in cui non riesca a scansionare il codice.

Un altro PDF conteneva un URL dannoso creato con Google Script per tentare di eludere il rilevamento. Questa truffa complessa comprendeva un record di transazioni Bitcoin falso e una finta barra di "avanzamento del mining" che invitava le potenziali vittime a inserire informazioni finanziarie per ricevere i loro ipotetici fondi.

Come abbiamo visto negli ultimi anni, anche nel 2023 gli attori delle minacce hanno superato se stessi nel replicare marchi conosciuti e affidabili, e continuano a migliorare. Alcuni esempi includono PDF dannosi mascherati da ricevute di iTunes, avvisi relativi a tentativi di accesso multipli a un account Wells Fargo e persino una replica della pagina di accesso alla piattaforma di collaborazione RingCentral.

Tattiche principali degli attori delle minacce

I file PE (Portable Executable) regnano sovrani

I file PE continuano a essere il payload finale più utilizzato grazie alla facilità di distribuzione, all'uso di strumenti generici e alla semplicità di esecuzione. Nel 2023 abbiamo tuttavia notato un aumento del malware PE scritto in .NET. Probabilmente a causa della sua accessibilità e delle numerose funzionalità, la maggior parte del malware PE che abbiamo osservato viene ora scritto in .NET, incluse le principali famiglie di malware come RedLine, AgentTesla e AsyncRAT.

Fortunatamente, i malware PE sono tipi di file classificati come sospetti e vengono esaminati con cura per rilevare eventuali contenuti malevoli. E, sebbene alcuni autori di malware usino i file di script come vettori iniziali per altri malware o scrivano codice dannoso completo utilizzando JavaScript, VBScript, PowerShell o altri, i clienti SonicWall sono protetti: RTDMI offre un'eccellente funzione di rilevazione di script dannosi grazie alle eccezionali capacità di emulazione degli script.

WinRAR offre il fianco agli aggressori

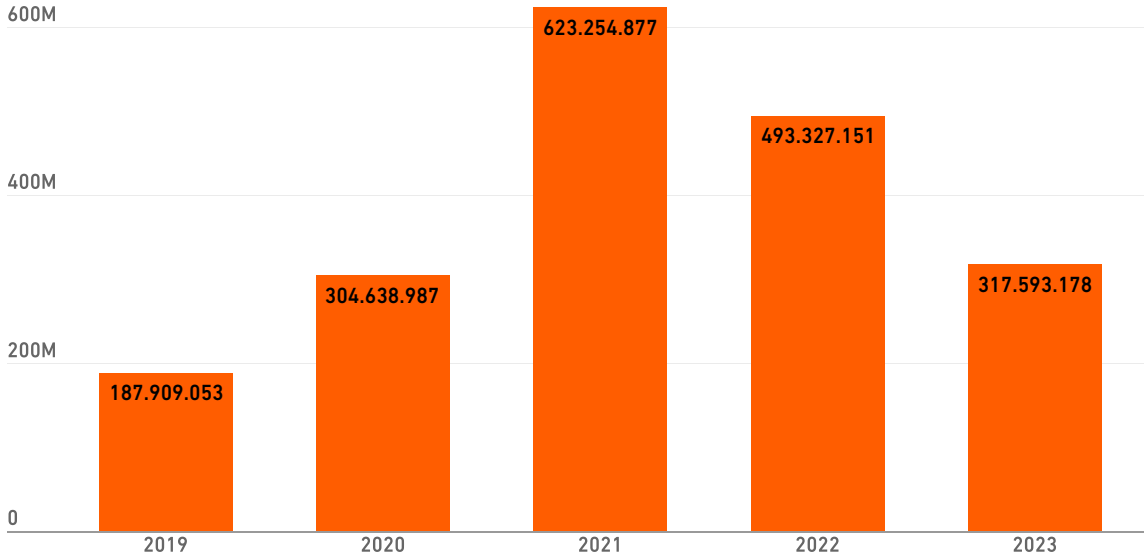
All'inizio del 2023, gli attori delle minacce hanno iniziato a sfruttare una nuova vulnerabilità di WinRAR, il popolare strumento di archiviazione di file Windows. Nella seconda metà dell'anno, diverse famiglie di malware stealer – tra cui AgentTesla, Remcos, Rhadamanthys e Guloader – sono state utilizzate in una serie di campagne che sfruttavano la CVE-2023-38831 per consentire agli aggressori di eseguire codice arbitrario all'interno degli archivi zip. A causa dell'ampia diffusione di WinRAR nelle imprese, queste campagne si sono rapidamente espanse a livello globale raggiungendo gli Stati Uniti, il Medio Oriente e l'Asia. Ora vengono associate a gruppi di hacker sponsorizzati da stati come Russia e Cina, tra cui Sandworm, APT28, APT 30 e altri.

Una minaccia da non sottovalutare

Il panorama degli attacchi ransomware ha continuato a evolversi nel 2023. I ricercatori di minacce di SonicWall Capture Labs hanno registrato 317,6 milioni di attacchi ransomware, con un calo del 36% rispetto all'anno precedente, ma pur sempre il terzo risultato più alto in assoluto. Questa tendenza si è riflessa in diverse regioni: in Nord America ed Europa il ransomware è diminuito di un terzo, in America Latina gli attacchi sono calati del 52%.

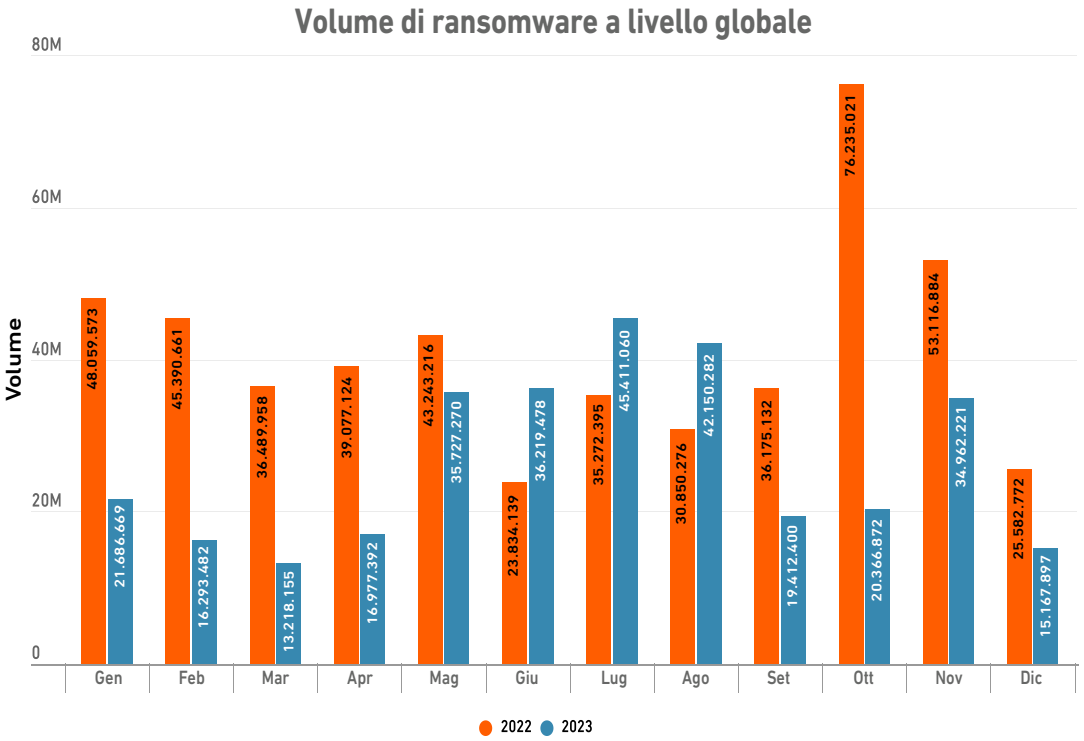
L'unica eccezione è l'Asia, dove i volumi di ransomware nel 2023 hanno segnato un aumento record del 1.627% rispetto al 2019, salendo a 17,5 milioni. Questo aumento è stato guidato dagli attacchi al settore finanziario. In maggio, il gruppo ransomware LockBit ha rubato 15 milioni di record dei clienti e 1,5 terabyte di dati interni dalla Bank Syariah Indonesia. In novembre anche la Industrial and Commercial Bank of China (ICBC), la più grande banca al mondo per attività, è stata attaccata da Lockbit. Secondo un rapporto di IDC pubblicato nel settembre 2023, circa tre quarti delle imprese in India sono state colpite da ransomware nel 2022, un numero che probabilmente ha continuato a crescere da allora.

Volume di ransomware per anno a livello globale



Il ransomware che ha dominato il 2023: LockBit

L'arresto di due affiliati non ha minimamente scalfito la struttura di LockBit, che è rimasto il gruppo ransomware incontrastato nel 2023. Ciò è dovuto probabilmente a innovazioni costanti come i programmi bug bounty per migliorare la qualità dei loro "prodotti", le attività di marketing e il rilascio periodico di versioni aggiornate dei toolkit con funzionalità migliorate. Dopo la violazione ai danni di LockBit 3.0 / "Black", SonicWall ha contattato gli attori delle minacce, che hanno poi richiesto un riscatto esorbitante (qui trovate tutti i dettagli.)



Perché il ransomware è ancora pericoloso

Se non abitate in una delle regioni maggiormente colpite dal ransomware, perché dovreste preoccuparvi di questa minaccia?

Nel nostro Sondaggio SonicWall 2023 sullo stato della cybersecurity avevamo chiesto ai clienti quali tipi di cyber attacco li preoccupava maggiormente. Ancora una volta, il ransomware occupava il primo posto con l'83%, superando phishing, minacce crittografate, malware fileless, attacchi IoT e altro ancora.

Nonostante il volume di attacchi ransomware sia diminuito tra i nostri clienti PMI, riteniamo che le loro preoccupazioni siano fondate.

Alcuni dati storici possono essere di aiuto. Un calo del 36% sembra molto significativo, finché non si considera la crescita del ransomware tra il 2020 e il 2022. Anche dopo questo calo, nel 2023 il ransomware occupava il terzo posto nella classifica annuale delle minacce. **E, con un aumento del 27% nella seconda metà del 2023 rispetto al primo semestre, il ransomware è di nuovo nella giusta direzione per eguagliare i picchi del 2021 e del 2022**.

Quando i fornitori di cybersecurity come SonicWall analizzano il ransomware e altre minacce, riescono a vedere solo quello che succede nel loro ecosistema. Mentre SonicWall (con la sua grande rete di partner e clienti MSP) ha notato un calo del ransomware nel corso del 2023, altri fornitori hanno registrato incrementi nello stesso periodo. Con l'aumento delle attività di controllo delle autorità, che rendono ogni attacco più rischioso, e il fatto che le PMI non sono più "facili prede" di attacchi indiscriminati, sembra che ora gli attori delle minacce si concentrino su attacchi meno numerosi ma più mirati, e con un maggiore potenziale di guadagno.

Ma ciò non significa che manchino gli obiettivi facili da colpire. Le organizzazioni spostano sempre più dati e flussi di lavoro nel cloud, ma spesso non proteggono queste istanze come farebbero sulla rete locale. E dato che gli attori delle minacce continuano a perfezionare gli attacchi ransomware alle piattaforme SaaS, una protezione insufficiente nel cloud può avere esiti disastrosi.

Al momento ci sono ancora enormi campagne ransomware in corso. Alla fine di maggio SonicWall ha osservato lo sfruttamento di una vulnerabilità critica zero-day con iniezione di codice SQL all'interno di MOVEit Transfer. Questo strumento di trasferimento dei file, particolarmente popolare e diffuso nelle imprese, è stato preso di mira dal gruppo ransomware Cl0p. Utilizzando la CVE-2023-34362, ha condotto un attacco alla supply chain che ha colpito circa 2.000 organizzazioni tra finanza, assicurazioni, sanità, istruzione e pubblica amministrazione, con un furto di dati che ha interessato oltre 62 milioni di persone.

È importante notare che vulnerabilità come questa sono state il vettore di ransomware più comune osservato da SonicWall nel 2023, e queste campagne hanno comportato pagamenti per il ransomware superiori a 1 miliardo di dollari per la prima volta nel 2023.

INTRUSIONI

Tentativi in aumento del 20%

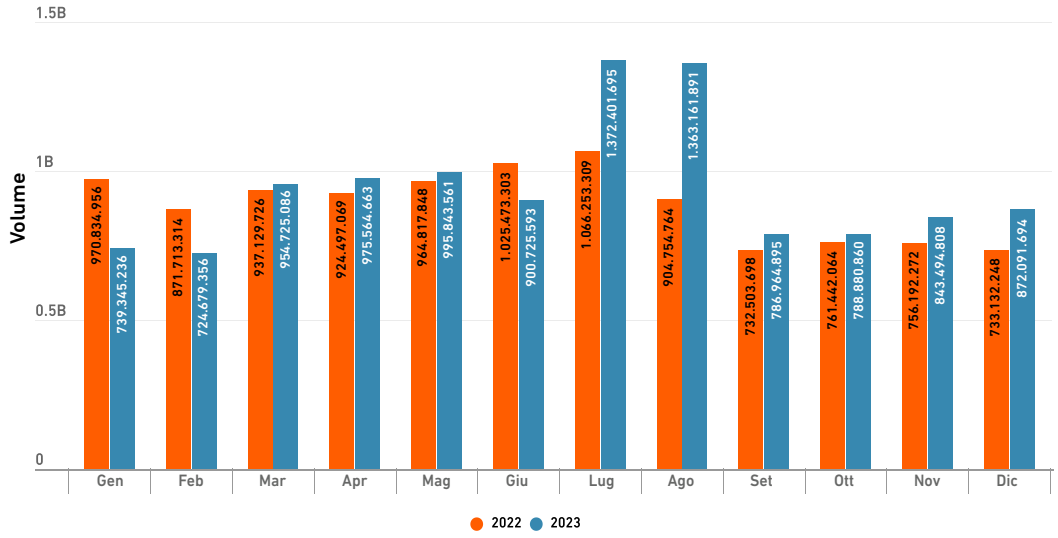
Il numero totale di tentativi di intrusione ha continuato a crescere nel 2023 salendo a 7,6 miliardi, con un aumento del 20% rispetto al 2022. Da quando SonicWall ha iniziato a registrare questa metrica nel 2013, il numero di tentativi di intrusione è aumentato di anno in anno e, nell'ultimo decennio, è cresciuto del 613%.

Sebbene una parte di questo aumento sia da attribuire a intrusioni di bassa gravità con attacchi ping e altre azioni solitamente benigne, sono aumentate anche le azioni di media ed elevata gravità, altrimenti note come "intrusioni dannose". Questi tentativi di intrusione hanno raggiunto 11,3 miliardi nel 2023, con un aumento del 6% rispetto all'anno precedente.

Le intrusioni dannose sono state rilevate in tutti i settori che abbiamo esaminato tra i nostri clienti. Le intrusioni di media ed elevata gravità sono aumentate del 19% nel campo dell'istruzione, del 34% nel settore retail, del 36% nella sanità, del 46% nella pubblica amministrazione e del 47% in campo finanziario.

Questi tentativi di intrusione provocano allarmi che devono essere esaminati dagli analisti di un SOC o dagli MSP insieme ad analisti di un SOC, generando un affaticamento da avvisi e sottraendo tempo prezioso ad altre iniziative critiche. Quando un'intrusione ha successo, i cybercriminali sono liberi di esfiltrare dati, eseguire codici dannosi, crittografare i sistemi e altro ancora, con il rischio potenziale di bloccare le operazioni e causare danni per migliaia o milioni di dollari a queste organizzazioni per gli interventi di risoluzione ed eventuali sanzioni per la conformità.

Intrusioni dannose a livello globale



Cos'è un tentativo di intrusione?

Un tentativo di intrusione malevola è un evento di sicurezza in cui un aggressore tenta di ottenere l'accesso non autorizzato a un sistema o a una risorsa sfruttando una vulnerabilità. Sebbene lo sfruttamento di vulnerabilità "zero-day" non pubblicate attiri maggiori attenzioni, le vulnerabilità più sfruttate sono generalmente pubbliche e pubblicate come CVE (vulnerabilità ed esposizioni comuni). Tuttavia, poiché non tutte le aziende applicano le patch allo stesso ritmo, gli aggressori hanno la possibilità di utilizzare il software o le appliance prive di patch come punto di accesso a una rete.

Una volta entrati nella rete, tentano di ottenere la persistenza nella rete e movimenti laterali sfruttando altre vulnerabilità nei sistemi privi di patch all'interno della rete.

SonicWall monitora il rilevamento e la prevenzione di exploit provenienti da sorgenti sia esterne che interne. Quando un codice che costituisce una vulnerabilità attraversa un firewall con prevenzione delle intrusioni abilitata, il firewall rileva e neutralizza tale codice e registra un tentativo di intrusione.

MINACCE CRITTOGRAFATE

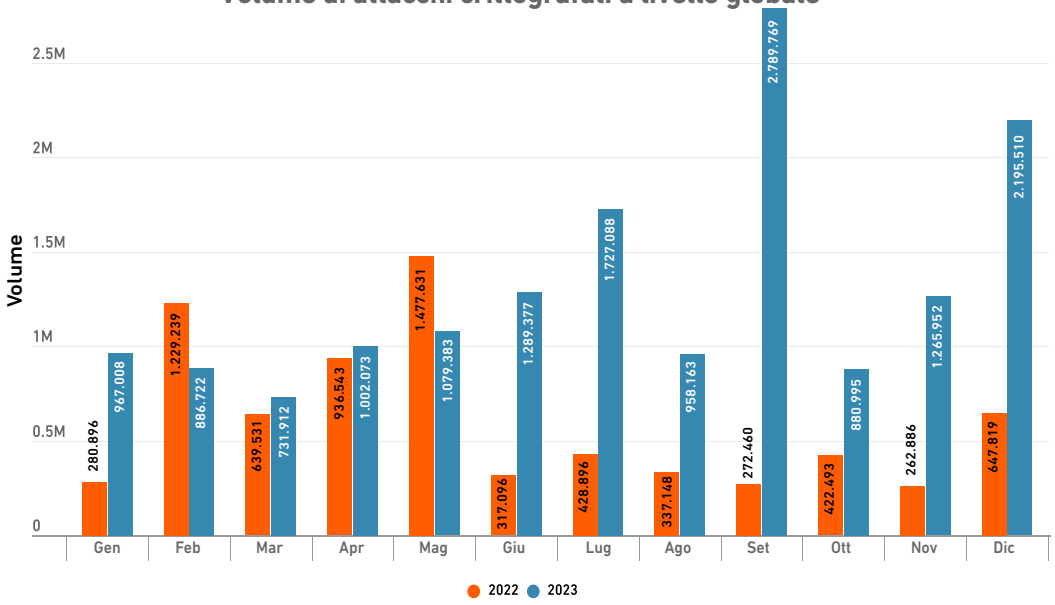
Attacchi crittografati più che raddoppiati

Nel 2023, i ricercatori di SonicWall Capture Labs hanno osservato 15,7 milioni di attacchi crittografati. Questa è la cifra più alta da quando abbiamo iniziato a registrare questo tipo di minaccia, pari a un aumento del 117% rispetto all'anno precedente.

Mentre il Nord America ha segnato un modesto aumento del 30%, in Europa, Asia e America Latina gli attacchi crittografati hanno registrato picchi a tre cifre, aumentando rispettivamente del 182%, 462% e 527%.

In alcuni settori che abbiamo esaminato ci sono stati incrementi ancora più marcati, tutti a tre cifre. La finanza ha registrato l'aumento minore: gli attacchi a questi clienti sono "solo" raddoppiati. Altri settori hanno registrato un aumento esponenziale delle minacce crittografate nel 2023, come ad esempio la sanità (252%), l'istruzione (429%), la pubblica amministrazione (629%) e il retail (680%).

Volume di attacchi crittografati a livello globale



Cosa sono le minacce crittografate?

La maggior parte delle società di analisi del settore ritiene che l'80-90% del traffico di rete sia attualmente crittografato, e pertanto è necessaria la scansione di questo tipo di traffico. Il TLS (Transport Layer Security) offre maggiore sicurezza per le sessioni web e le comunicazioni internet, ma i cybercriminali usano in misura crescente questo protocollo di crittografia per nascondere malware, ransomware, attacchi zero-day e altro ancora.

I firewall meno recenti e altri controlli di sicurezza tradizionali non dispongono della capacità o della potenza di elaborazione per rilevare, ispezionare e mitigare le minacce inviate attraverso il traffico HTTP, permettendo così agli attori delle minacce di distribuire ed eseguire gli attacchi con relativa facilità.

CRYPTOJACKING

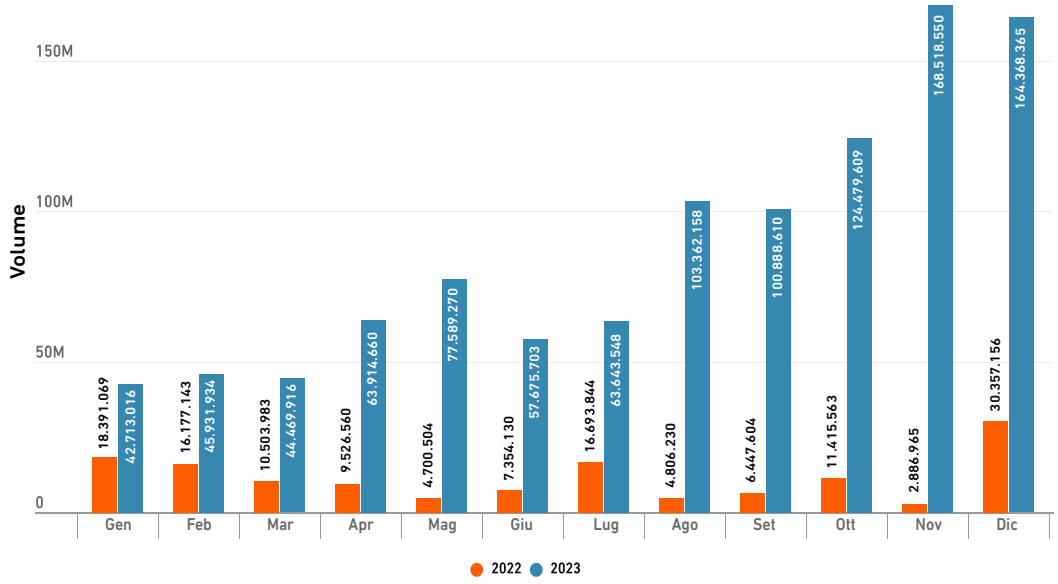
Perché è pericoloso (e perché è in aumento)

Nel rapporto sulle minacce dell'anno scorso abbiamo notato una novità preoccupante: il numero di attacchi di cryptojacking, che erano rimasti piuttosto bassi da quando abbiamo iniziato a monitorarli nel 2018, ha superato per la prima volta il limite di 100.000.

Come abbiamo scoperto in seguito, l'ascesa del cryptojacking era solo all'inizio. Nel 2023, il numero di attacchi di cryptojacking ha superato il volume totale del 2022 all'inizio di aprile e ha continuato a crescere. Alla fine dell'anno, i ricercatori di minacce di SonicWall Capture Labs hanno registrato *1,06 miliardi* di attacchi di cryptojacking, con un aumento del 659% rispetto ai totali del 2022. Questo aumento è stato favorito da volumi di attacchi senza precedenti nei mesi di novembre e dicembre, ciascuno con un numero di attacchi di cryptojacking superiore a quello riscontrato per l'intero 2022.

Notevoli incrementi sono stati rilevati anche in tutte le regioni. In Asia-Pacifico e America Latina, il cryptojacking è cresciuto rispettivamente dell'87% e del 116%. Ma gli aumenti più importanti sono stati registrati in Nord America (+596%) e in Europa (+1.046%).

Volume di cryptojacking a livello globale



Cos'è il cryptojacking?

Il cryptojacking è un tipo di attacco informatico in cui gli aggressori sfruttano le risorse di calcolo di una vittima per estrarre criptovalute senza il suo consenso o a sua insaputa. Prevede l'installazione di malware, spesso distribuito tramite e-mail di phishing o siti web compromessi, che viene eseguito in background sul computer, lo smartphone o il server della vittima. Questo malware utilizza la potenza di elaborazione e l'energia del dispositivo per risolvere problemi matematici complessi ("proof of work"), generando criptovalute per l'aggressore.

Lo stato attuale del cryptojacking

Nel 2023, gran parte degli attacchi di cryptojacking ha riguardato ancora una volta XMRig. Questo software open source è uno strumento legittimo facilmente reperibile in Internet, ma spesso viene utilizzato in modo improprio a causa della relativa facilità d'uso e di configurazione. È accessibile anche agli hacker meno esperti, ma gli utenti più avanzati sono in grado di modificare il codice nel tentativo di eludere il rilevamento e incrementare i profitti.

XMRIg viene spesso usato come trojan o inserito in altri pacchetti software o adware. Viene diffuso tramite phishing, malvertising, vulnerabilità, dropper dannosi, applicazioni software piratate e altro ancora. È efficiente e in grado di estrarre la criptovaluta Monero (nota anche come XMR, e spesso la criptovaluta preferita dai cybercriminali per le sue funzionalità di privacy) a una velocità relativamente elevata senza consumare troppe risorse di sistema. Tuttavia richiede una grande quantità di CPU poiché esegue il mining in background, e lo fa *costantemente*.

Per questo risulta particolarmente costoso, sia in termini di produttività – dal momento che il cryptojacking può rallentare in modo significativo le attività non di mining – sia in termini di denaro vero e proprio: la vittima paga non solo per il maggior consumo di energia, ma anche per dover sostituire i dispositivi che si surriscaldano o hanno una durata ridotta a causa di questi processi gravosi.

Inoltre è costoso per l'ambiente: nel solo biennio 2020-2021, il mining di Bitcoin ha avuto la stessa impronta di carbonio di 190 centrali elettriche a gas o di 38 milioni di tonnellate di carbone bruciato. L'energia totale richiesta da queste attività di mining supera il consumo di energia di molte nazioni sviluppate.

Il mining di criptovalute è stato classificato come uno dei settori più dannosi per l'ambiente. Uno studio di Scientific Reports ha rivelato che, dal 2016 al 2021, ogni euro di Bitcoin estratto ha causato 35 centesimi di danni al clima.

Nonostante il costo elevato, il mining di criptovalute non è illegale e il cryptojacking viene raramente perseguito, anche se questo potrebbe cambiare. Il 2024 ha già registrato un arresto di alto profilo per cryptojacking: la collaborazione tra Europol, forze dell'ordine ucraine e un provider di cloud ha portato all'arresto di una persona sospettata di aver estratto oltre 2 milioni di dollari in criptovalute.

Secondo i dati di SonicWall, il cryptojacking ha rappresentato un sesto di tutti i casi di malware nel 2023. Con la diffusione del mining illecito, potremmo iniziare a vedere lo stesso tipo di risposta comune da parte del settore pubblico e privato che era emersa all'inizio del boom del ransomware, intorno al 2020.

RTDMI rileva oltre 1,5 milioni di minacce

Nonostante l'aumento di quasi tutti i tipi di minacce, nel 2023 SonicWall Capture Advanced Threat Protection (ATP) con Real-Time Deep Memory Inspection (RTDMI) ha registrato un numero molto inferiore di varianti malware mai viste prima: 387.000, con un calo del 38% rispetto all'anno precedente.

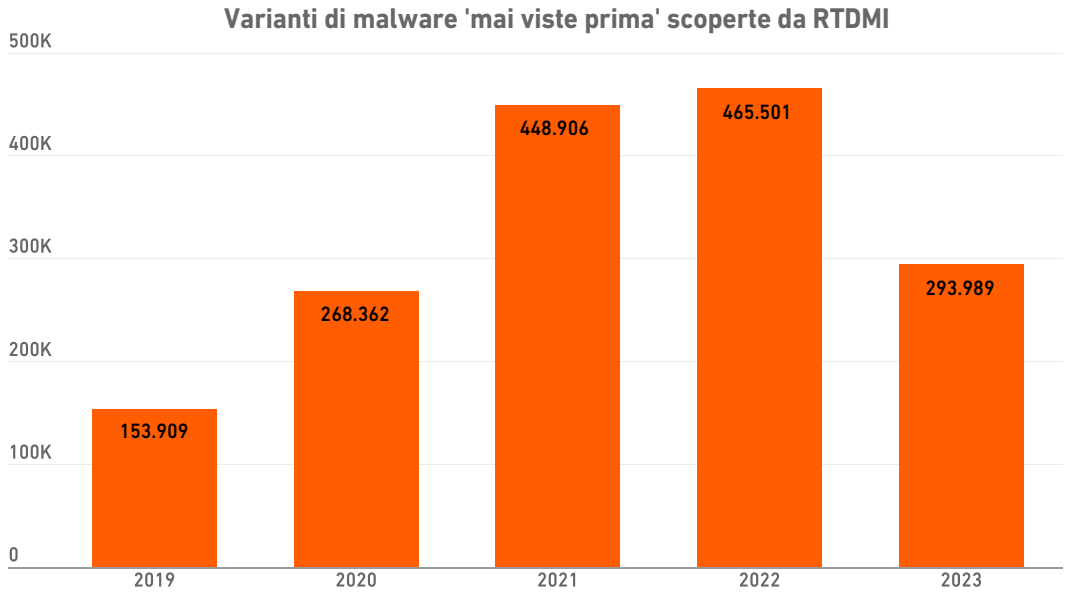
In combinazione con l'aumento del malware e i livelli di phishing costantemente elevati, questo dato offre informazioni utili sul panorama delle minacce nel 2023: gli attori delle minacce non desistono, ma per il momento trovano varianti che funzionano e le usano ripetutamente. Il mese di dicembre, in particolare, ha registrato meno varianti del solito, scendendo al livello più basso dall'agosto 2020.

Per chiarezza occorre dire che vengono ancora create molte nuove varianti di malware: le oltre 800 varianti mai viste prima al giorno che in media hanno colpito i clienti nel 2023 sono state sufficienti per superare il record di 1,5 milioni di rilevamenti in un anno. Ma il ritmo delle innovazioni sembra essere rallentato, almeno temporaneamente.

RTDMI migliora la sicurezza delle credenziali

Mentre gli attori delle minacce hanno preferito utilizzare soluzioni collaudate nel 2023, SonicWall ha trascorso lo stesso periodo di tempo migliorando i propri strumenti e prodotti. Abbiamo aggiunto un nuovo modulo engine a RTDMI, migliorando notevolmente la capacità di rilevamento dei furti di credenziali tramite HTML.

Il phishing HTML sfrutta uno dei metodi di truffa più comuni per rubare le credenziali, con pagine notevolmente offuscate tramite reindirizzamento di iframe, javascript, caricamento dinamico e altri metodi per non destare sospetti. L'aggiunta di questo nuovo modulo consente di rilevare questi file altamente offuscati. Il contenuto HTML viene esaminato in sicurezza in un ambiente sandbox e deoffuscato fino allo stato finale, per osservare con chiarezza l'attività o l'intento dannoso senza mettere a rischio la rete.



Attacchi "zero-day" e attacchi "mai visti prima"

Un "attacco zero-day" è uno dei concetti di cybersecurity più conosciuti, in quanto viene spesso utilizzato in violazioni di alto profilo. Questi attacchi sono minacce completamente nuove e sconosciute che colpiscono una vulnerabilità "zero-day", cioè non ancora protetta (tramite patch, aggiornamenti, ecc.) dal fornitore o dall'azienda presa di mira.

Al contrario, SonicWall monitora il rilevamento e la mitigazione di "attacchi mai visti prima", vale a dire firme di attacchi sconosciute che SonicWall Capture ATP identifica come dannose per la prima volta. Queste presentano spesso caratteristiche simili ai modelli di attacchi zero-day esistenti, che SonicWall è in grado di identificare grazie all'elevato volume di attacchi analizzati.

COSA SI PUÒ FARE

Come dimostra la crescente ondata di minacce descritte in questo rapporto, non è possibile evitare di essere presi di mira. Tuttavia, ci sono diverse misure che potete adottare per rafforzare il vostro approccio globale alla cybersecurity:

1. **Abilitare l'autenticazione a più fattori (MFA)**
   La tecnologia MFA migliora notevolmente la sicurezza dell'autenticazione: anche se qualcuno riesce ad accedere alle vostre password, non sarà in grado di accedere ai vostri account poiché è necessaria una seconda autenticazione da parte dell'utente, cioè voi.
2. **Applicare rapidamente le patch**
   Sebbene le vulnerabilità zero-day facciano più notizia, la maggior parte degli exploit tenta di sfruttare le vulnerabilità note da mesi o anni.
3. **Eseguire valutazioni di sicurezza periodiche**
   Questo vi aiuterà a identificare le vulnerabilità, valutare i rischi e rafforzare in modo proattivo le difese, garantendo una solida protezione contro le minacce in continua evoluzione.
4. **Organizzare corsi di sicurezza ricorrenti**
   La sicurezza informatica avanza di pari passo con la tecnologia. Per creare una forza lavoro più informata e vigile, le aziende dovrebbero organizzare corsi di formazione base e pratiche di routine per incoraggiare i dipendenti a non cliccare su link sospetti e addestrarli a identificare e segnalare potenziali rischi per la sicurezza.
5. **Scansionare il traffico crittografato**
   Gli esperti stimano che oggi l'80-90% di tutto il traffico di rete sia crittografato. Tuttavia, molti firewall esistenti *non dispongono* delle funzionalità o della potenza di elaborazione per rilevare, ispezionare e mitigare i cyber attacchi diffusi attraverso il traffico HTTP, e tanto meno TLS 1.3, per cui gli aggressori usano la crittografia per distribuire ed eseguire malware. Secondo i dati di SonicWall, il malware diffuso tramite HTTPS è aumentato del 117% dal 2022 al 2023. A livello globale, SonicWall ha registrato 15,8 milioni di attacchi crittografati nel 2023, quasi quanto nel 2021 e 2022 messi insieme. La crescita del traffico crittografato e delle minacce crittografate evidenzia la necessità di garantire la scansione di tutto il traffico.
6. **Estendere la protezione al cloud**
   Le aziende trasferiscono sempre più dati e flussi di lavoro nel cloud e, di conseguenza, hanno bisogno di approcci più completi e flessibili che includano soluzioni Security Service Edge (SSE) e Zero-Trust Network Architecture (ZTNA) per proteggere i loro ambienti di lavoro ibridi.

Per informazioni di Threat Intelligence aggiornate e notizie sul settore, seguite il blog di SonicWall.

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035
www.sonicwall.com

SonicWall

SonicWall è un precursore della sicurezza informatica con oltre 30 anni di esperienza e di impegno continuo verso i propri partner. Grazie alla capacità di creare, scalare e gestire la sicurezza informatica in ambienti cloud, ibridi e tradizionali in tempo reale, SonicWall può fornire in modo rapido ed economico soluzioni di sicurezza dedicate a qualsiasi tipo di organizzazione in tutto il mondo. Mediante i dati del proprio centro di ricerca sulle minacce, SonicWall garantisce una protezione completa contro gli attacchi informatici più elusivi e fornisce informazioni pratiche sulle minacce ai partner, ai clienti e alla comunità di cybersecurity.

A livello di miglior prassi, SonicWall ottimizza di routine le sue metodologie di acquisizione, analisi e reportistica dei dati. Ciò include adeguamenti al filtraggio dei dati, cambiamenti a livello delle fonti dei dati e consolidamento dei feed delle minacce. I dati pubblicati nei rapporti precedenti possono essere stati adeguati per periodi, regioni e settori industriali diversi.