E-BOOK

5 motivi per cui è impossibile impedire il ransomware

NetApp

Sommario

Alla luce del numero di attacchi ransomware di alto profilo condotti nel corso degli anni e delle gravi conseguenze di tali episodi, potresti pensare che sia necessario ottimizzare i metodi di prevenzione in modo da eliminare completamente questo fenomeno in tempi brevi.

Prendiamo in esame una minaccia, che in passato era onnipresente, ovvero i kit di exploit, come il famigerato Angler, che creavano enormi problemi ai team di sicurezza dell'epoca. Questi kit di exploit sono ormai un lontano ricordo grazie all'incessante lavoro dei ricercatori.

Il ransomware, invece, è ancora ovunque e la prevenzione totale da queste minacce è praticamente impossibile. Cerchiamo di capire perché.

5

È redditizio

I criminali sono più motivati che mai, poiché traggono enormi guadagni dagli attacchi portati a termine con successo. Il riscatto medio pagato dalle organizzazioni degli Stati Uniti, del Canada e dell'Europa è passato da 115.123 USD nel 2019 a 312.493 USD nel 2020, un incremento del 171%. La media del primo trimestre fiscale del 2021 è stata di 850.000 USD. A partire dal 2019, gli incidenti legati al ransomware sono aumentati del 65%. La frequenza degli attacchi continuerà a crescere: si stima, infatti, che dalla media attuale di un attacco ogni 11 secondi si passerà a un attacco ogni 2 secondi entro il 2031. Questi attacchi diventeranno sempre più diffusi. Con queste cifre è facile comprendere il motivo per cui il ransomware continua a essere una delle attività criminali più popolari.

E anche se le forze dell'ordine sconsigliano di farlo, le organizzazioni continuano a pagare il riscatto. È naturale che le aziende vogliano proteggere i propri dati, ma il costo dell'interruzione dell'attività è spesso più grave del riscatto in sé, quindi pagare è spesso l'opzione più conveniente.

4

È economico

I costi necessari per creare una campagna di ransomware sono molto contenuti. Attualmente, un criminale può acquistare un kit per il ransomware pronto per l'uso spendendo una somma relativamente bassa. Il kit contiene tutto ciò che serve per implementare un attacco e riscuotere il pagamento, compresi i servizi di crittografia, il dropper del payload e gli strumenti di offuscamento. Un tipico abbonamento di ransomware-as-a-service (RaaS) parte da poco più di 100 USD al mese. Le varianti più complesse e potenti possono costare migliaia di euro, ma anche il potenziale di guadagno sarà più alto. Vengono forniti anche piani di supporto per consentire ai criminali di ottenere il massimo valore dal servizio.

3

È di comprovata efficacia

Il ransomware è un business redditizio. Dimentica lo stereotipo dei malfattori incappucciati che operano in stanze buie: il ransomware è una rete sofisticata paragonabile a qualsiasi programma di partnership aziendale. Uno degli ultimi esempi di RaaS è DarkSide, individuato per la prima volta all'inizio dell'agosto 2020 e passato a un modello di distribuzione RaaS entro novembre dello stesso anno. Sulla base degli eventi riportati, la richiesta tipica è compresa tra 200.000 e 2 milioni di USD per ottenere le chiavi di sblocco dei dati. Oltre a ottenere ottime rendite, gli operatori del ransomware DarkSide agiscono anche come dei "Robin Hood digitali", ovvero prelevano denaro da grandi aziende redditizie e, in alcuni casi, distribuiscono parte dei ricavi alle persone meno abbienti attraverso donazioni di beneficenza. I rapporti pubblicati dai siti che si occupano di violazioni indicano almeno 90 vittime di DarkSide fino a oggi. In totale, sui siti di DarkSide sono ospitati attualmente oltre 2 TB di dati rubati e questo è un altro incentivo per il pagamento.

2

Offre un ROI rapido

Un altro motivo dell'interesse suscitato dal ransomware è che una volta entrato in un'organizzazione, generalmente attraverso allegati email, URL dannosi, protocolli di desktop remoto insicuri o pubblicità dannosa ("malvertising"), si muove velocemente. Il software scansiona la rete in modo da individuare i file, criptandone il contenuto e chiedendo un riscatto. Purtroppo, una volta iniziato il processo di crittografia è impossibile tornare indietro. Attualmente si è diffusa una nuova metodologia allarmante che prevede il furto dei dati ancora prima di crittografarli. Nel maggio 2021, la Colonial Pipeline, fornitore del 45% del carburante della costa orientale degli Stati Uniti, è stata colpita da un attacco ransomware. L'attacco è stato effettuato da DarkSide o da un affiliato. Oltre a bloccare i sistemi informatici della Colonial Pipeline, DarkSide ha rubato oltre 100 GB di dati aziendali. Da questo furto è emerso che il gruppo applica una doppia estorsione alle vittime. Infatti, oltre a chiedere del denaro sbloccare i computer colpiti, è stato richiesto un pagamento aggiuntivo per i dati acquisiti, minacciando di diffonderli pubblicamente se non avessero ricevuto i soldi.

1

Le persone sono inaffidabili

Finora abbiamo preso in esame il motivo della diffusione del ransomware, senza spiegare in che modo sia possibile contrastarlo. Pur essendo possibile prevenire numerosi attacchi attraverso una gestione più efficace delle patch, è necessario considerare un fattore che più di tutti contribuisce a rendere impossibile l'eliminazione del ransomware: le persone.

Ti fidi dei tuoi dipendenti e pensi che non danneggerebbero mai intenzionalmente la tua organizzazione. Tuttavia, se i dipendenti non sono estremamente attenti ai possibili pericoli derivanti da email e link dannosi o da tentativi di phishing potranno sempre verificarsi nuove infezioni di ransomware.

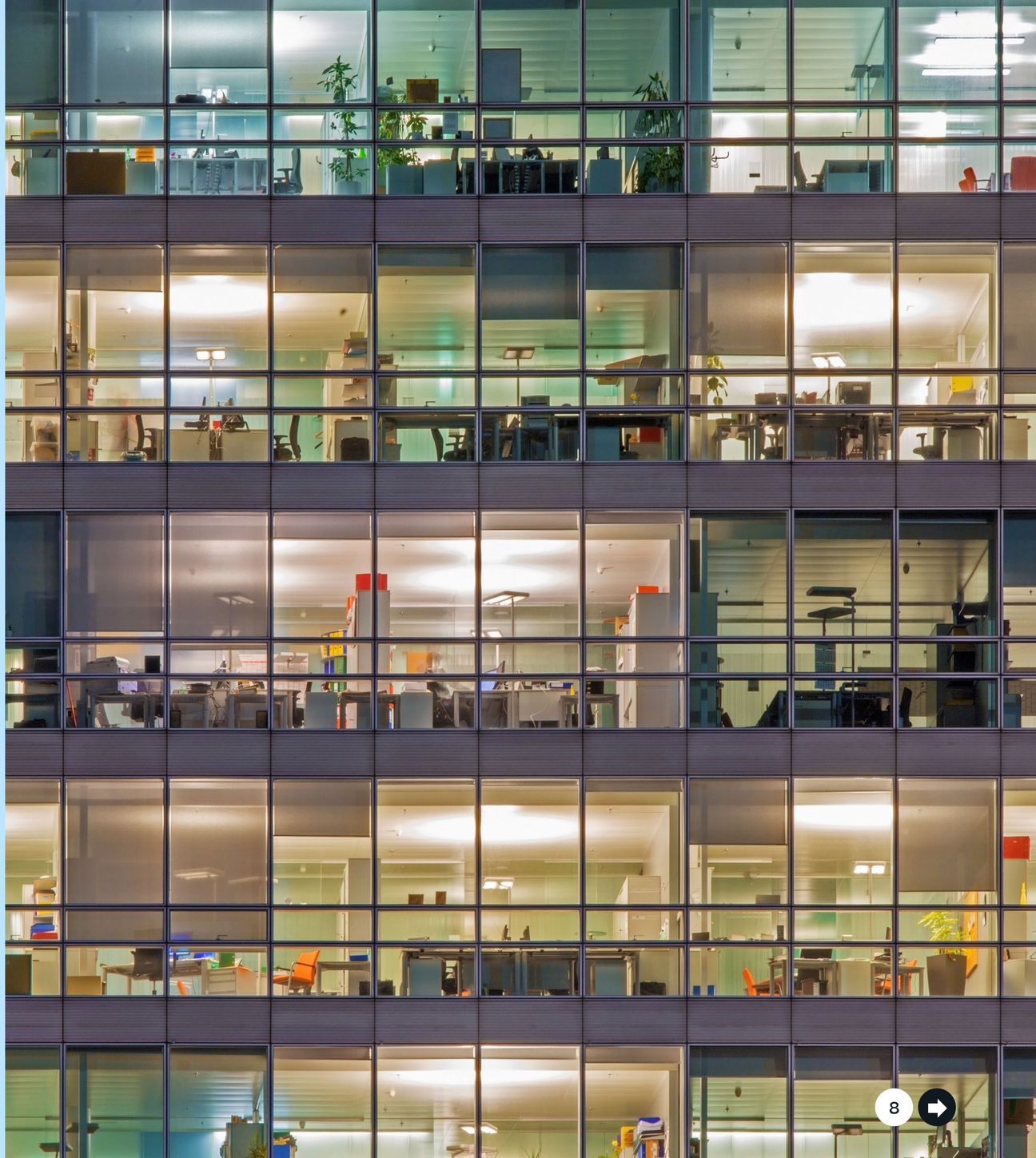
Molti lettori conosceranno probabilmente la formazione obbligatoria per la sicurezza informatica. La formazione è una strategia utile, ma anche i dipendenti più attenti in termini di sicurezza potrebbero commettere un errore di giudizio nel fare clic su un link o aprire un'email. E se non si applicano politiche di sicurezza iper-restrittive nello svolgimento del proprio lavoro, è sufficiente un errore di valutazione per causare un disastro. Occorre eseguire il rilevamento delle minacce entro pochi secondi, non minuti, ore o ancora di più.

Protezione ransomware "zero trust"

Se non è possibile prevenire il ransomware, in che modo è possibile proteggersi?

I tuoi dipendenti devono accedere ai dati per svolgere il proprio lavoro, proprio come avviene per il ransomware, diventando il principale vettore di attacco. Le politiche e i ruoli che limitano l'accesso ai dati possono contribuire alla protezione, ma anche ostacolare la produttività se eccessive o troppo rigorose.

Allora è necessario anticipare con un rilevamento precoce, un'analisi del comportamento degli utenti e l'applicazione di azioni automatiche in caso di schemi sospetti. E tutto questo in pochi secondi.



NetApp® Cloud Insights offre questo tipo di rilevamento con la funzione Cloud Secure. Cloud Secure consente di monitorare le attività, rilevare le anomalie e automatizzare le risposte.

- **Monitora l'attività dell'utente**
  Per identificare accuratamente le violazioni viene acquisita e analizzata ogni attività dell'utente, on-premise e negli ambienti di cloud ibrido. I dati vengono raccolti utilizzando uno strumento di raccolta dati leggero e stateless, installato su una VM nell'ambiente del cliente. Queste informazioni comprendono anche i dati dell'utente di Active Directory e dei server LDAP, oltre all'attività dei file dell'utente dello storage NetApp ONTAP® nei data center e nel cloud.

  Cloud Secure rileva le anomalie nel comportamento dell'utente creando un modello comportamentale per ciascun utente. Da quel modello comportamentale rileva i cambiamenti anomali nell'attività dell'utente e analizza tali modelli di comportamento per determinare se la minaccia è costituita da un ransomware o da un utente malintenzionato. Questo modello comportamentale consente di ridurre i falsi positivi.

- **Rileva le anomalie e identifica i potenziali attacchi**
  I ransomware e i malware attuali sono molto sofisticati: utilizzano estensioni e nomi di file casuali che rendono inefficace il rilevamento tramite soluzioni basate sulle firme (elenchi di blocco). Cloud Secure utilizza algoritmi avanzati di machine learning per scoprire attività insolite sui dati e rilevare un potenziale attacco. Questo approccio fornisce un rilevamento dinamico e preciso e riduce i falsi rilevamenti.

- **Automatizza le politiche di risposta**
  Cloud Secure avverte in caso di potenziale attacco ransomware e offre diverse politiche di risposta automatica per proteggere i tuoi dati.

  Crea una copia NetApp Snapshot™ quando rileva un comportamento insolito. I tuoi dati sono protetti in modo da poterli recuperare rapidamente, limitando qualsiasi potenziale interruzione in caso di falso positivo.

Blocca la possibilità per un utente di accedere ai dati:
- In caso di rilevamento di un comportamento anomalo dell'utente (lettura/scrittura).
- In caso di rilevamento di un comportamento insolito in termini di eliminazione dei file.

Cloud Secure offre un controllo dettagliato degli accessi, consentendo agli amministratori di identificare rapidamente i dati compromessi e l'origine dell'attacco, in modo da porvi rimedio e recuperare la situazione in poco tempo.

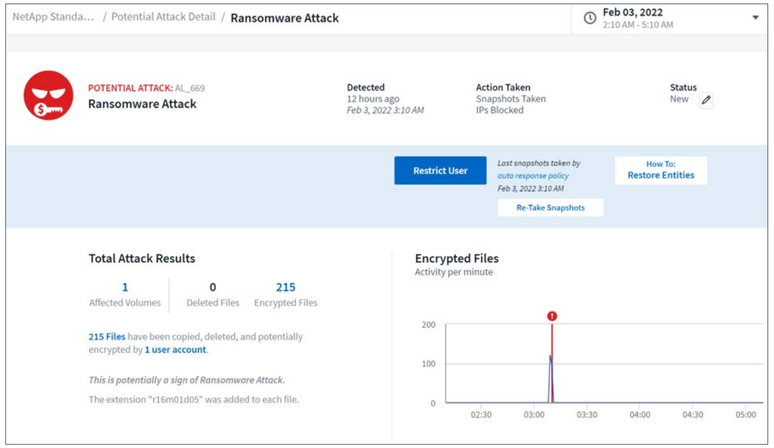


Figura 1) Dashboard di Cloud Secure che evidenzia un attacco ransomware.

Se ti interessa saperne di più su Cloud Secure, puoi iscriverti alla nostra prova gratuita di 30 giorni. **Scopri di più e inizia la prova gratuita.**

A proposito di NetApp

In un mondo di generalisti, NetApp abbonda di specialisti. Abbiamo un unico obiettivo: aiutare la tua azienda a ottenere il massimo dai dati. NetApp porta i servizi dati enterprise che utilizzi regolarmente nel cloud e la semplice flessibilità del cloud nel data center. Le nostre soluzioni leader del settore funzionano nei diversi ambienti dei clienti e con i principali cloud pubblici nel mondo.

In veste di azienda di software data-centric e basata sul cloud, solo NetApp può aiutarti a creare data fabric unici, semplificare e connettere il cloud, oltre a fornire in maniera sicura i dati, le applicazioni e i servizi appropriati alle persone corrette, in qualsiasi momento e ovunque esse si trovino.

NetApp