# Ransomware:tutto ciò che bisogna sapere

**Sei occupato. Sei stanco. Vuoi solo giocare a Pokémon Go o accedere alla intranet dell'azienda. A prescindere dal motivo, ogni volta che fai clic su "Ricordamelo più tardi" alla richiesta di aggiornamento di un software, rendi il dispositivo vulnerabile al ransomware.**

**Questo è solo uno dei tanti modi in cui il ransomware può accedere al sistema. Il malvertising, le e-mail di phishing e persino schemi sofisticati di pen drive sono tattiche comuni che gli hacker utilizzano per compromettere il sistema. Esaminiamo in modo più approfondito una situazione tipica.**

## Fai clic su "Ricordamelo più tardi"

Nessun software è perfetto. Gli sviluppatori identificano regolarmente bug nei propri programmi e rilasciano patch per ripararli. Quando si ritarda l'aggiornamento di plug-in o applicazioni, gli hacker possono sfruttare facilmente le vulnerabilità note. In merito a un exploit kit diffuso, Flash ha registrato che i tentativi andati a buon fine sono stati l'80%. Che si tratti di Flash, Silverlight, o persino Google Chrome, bisogna effettuare gli aggiornamenti e applicare le patch con regolarità.

## Sei stato infettato

Ormai sul dispositivo, il ransomware prende il controllo dei sistemi colpiti. Quindi utilizza uno scambio asimmetrico di chiavi per crittografare i file. Di fatto, è in grado di mescolare i dati senza il consenso dell'utente, e solo lo sviluppatore del ransomware ha la chiave per risolverlo. Alcune forme di ransomware si diffondono anche nella rete. Gli esperti di sicurezza prevedono che questa auto-propagazione diventerà preponderante.

## Compare una richiesta di riscatto

Una volta completata l'infezione, sullo schermo compare un messaggio con la richiesta di pagare un riscatto in bitcoin per riavere i propri dati. In genere la cifra del riscatto varia dai 200 ai 10.000 dollari, ma alcune istituzioni hanno pagato un prezzo molto più alto. Un ospedale in California ha sborsato 17.000 dollari in cambio dei propri dati. Questo dopo aver perso 100.000 dollari al giorno a causa dell'impossibilità di svolgere la propria attività.

Gli esperti di sicurezza consigliano di non pagare il riscatto. Alcuni tipi di ransomware non possono nemmeno liberare i file oppure li distruggono automaticamente. I ricercatori di Talos hanno scoperto che questi tipi di ransomware dannoso e distruttivo sono sempre più diffusi. Come emerge dal Report semestrale sulla cybersecurity 2016, i ricercatori sulle minacce indicano che l'integrità dei dati è un nuovo problema relativo al ransomware. Non si può essere sicuri che gli autori degli attacchi mantengano integri i dati che crittografano e le potenziali ricadute per le cartelle cliniche o i progetti tecnici manomessi, ad esempio, possono essere enormi.

Inoltre, pagando il riscatto si finanzia un'attività criminale. Finché possono ottenere dei guadagni con queste strategie, gli hacker continueranno a creare tipi di ransomware ancora più potenti.

## Come bloccare il ransomware

Il modo migliore per prepararsi ad affrontare il ransomware è quello di implementare un approccio alla sicurezza a più livelli.

### Prima dell'attacco

È possibile rafforzare la propria posizione difensiva in alcuni semplici modi. Va presa in considerazione l'idea di utilizzare un partner di disaster recovery come piano B per mantenere l'operatività aziendale nel caso in cui avvenga il peggio. Ma si possono adottare anche misure più semplici. Fare regolarmente il backup dei file per proteggere i dati importanti. Installare i blocchi per gli annunci pubblicitari e aggiornare sempre il software quando viene richiesto.

Tuttavia, i blocchi per gli annunci pubblicitari da soli non possono rilevare e bloccare tutto il malvertising o identificare i collegamenti ipertestuali dannosi. Bisognerebbe usare Cisco® Umbrella, che può essere installato in meno di 5 minuti. Rileva i siti dannosi e blocca le richieste a livello host.

### Durante l'attacco

Con Umbrella la maggior parte dei file ransomware verrà bloccata a livello di DNS, addirittura prima che possa raggiungere il dispositivo dell'utente finale. Nonostante i migliori sforzi di prevenzione, nessun metodo garantisce una protezione completa dal ransomware.

Serve visibilità su ciò che accada nella rete e bisogna essere in grado di identificare gli attacchi nel momento in cui si verificano. Il rilevamento delle minacce di Cisco Stealthwatch™ controlla il traffico di rete e nota se si verifica qualcosa di anomalo, come un'infezione ransomware, e avvisa quindi che il sistema è stato compromesso.

# Ransomware:tutto ciò che bisogna sapere

Cisco offre strumenti potenti per bloccare i tentativi di esecuzione dei file:

- Umbrella protegge il sistema bloccando la richiesta del file all'infrastruttura della chiave di crittografia. Ciò significa che il ransomware non può comunicare e ottenere le informazioni necessarie per crittografare i dati.
- Mentre Umbrella blocca la richiesta, il Next-Generation Firewall di Cisco blocca la connessione, offrendo una protezione ulteriore.
- Se un file riesce a superare il livello DNS e il firewall, Cisco Advanced Malware Protection (AMP) for Endpoints riesce a bloccare l'esecuzione del file e quindi fa un passo avanti. Analizza in continuazione qualsiasi attività dei file nel sistema, offrendo la possibilità di individuare e rimuovere tutti i file dannosi.

## Dopo l'attacco

Se il sistema è già stato compromesso dal ransomware, bisogna determinare la portata dei danni e impedirne la diffusione. AMP è in grado di bloccare l'esecuzione di file malware noti e rimuovere il file sull'endpoint.

Per interrompere la diffusione del ransomware in una rete, la segmentazione dinamica con la tecnologia Cisco TrustSec® identifica le parti della rete raggiunte dal ransomware e ne impedisce la diffusione.

Vuoi saperne di più? Consulta cisco.com/go/ransomware.



C11-737870-00 09/16