Ransomware (cavalli di Troia crittografanti)

I criminali seguono strategie diverse per carpire denaro da vittime ignare. Un approccio frequente è quello di crittografare i file dell'utente, che potrà accedervi solo dopo aver pagato un «riscatto» – forse...!

Come proteggersi dal ransomware:

- **Eseguite regolarmente una copia di sicurezza (backup) dei vostri dati.**
  Assicuratevi di scollegare dal sistema il supporto su cui salvate il backup subito dopo averlo creato. In caso contrario l'attacco di un ransomware potrebbe crittografare anche i dati del supporto di backup.
- **Tenete sempre aggiornati il software e i componenti aggiuntivi installati.**
  Assicuratevi che tutte le applicazioni, le app e i componenti aggiuntivi dei browser installati siano sempre aggiornati. Attivate sempre, se possibile, la funzione di aggiornamento automatico dei vari software.
- **Fate attenzione alle e-mail sospette.**
  Prestate attenzione ogni volta che ricevete un'e-mail inaspettata, anche se sembra provenire da un mittente conosciuto. Non seguite le istruzioni date nel testo, non aprite allegati e non fate clic su nessun link.
- **Utilizzate un programma antivirus.**
  Il programma antivirus deve aggiornarsi sempre in automatico. In caso contrario, sussiste il rischio che nuovi software dannosi non vengano riconosciuti.

Funzionamento

Non ci vuole molto: in alcuni casi basta aprire un allegato e-mail dannoso o un sito Internet infetto per consentire a un cavallo di Troia crittografante di insediarsi nel sistema e rendere i dati inutilizzabili cancellandoli o crittografandoli.

Dopo che i file del sistema sono stati criptati dal ransomware, sullo schermo appare una «schermata di blocco», ossia un messaggio con il quale viene chiesto alla vittima di pagare a chi ha sferrato l'attacco una determinata somma di denaro in una criptovaluta perché i file cifrati vengano liberati e quindi si possa tornare a utilizzarli (ricatto). L'uso di una valuta di Internet complica l'individuazione degli autori dell'attacco.

Per la diffusione del ransomware i criminali mirano soprattutto alle imprese, poiché dispongono di enormi quantità di dati critici per la loro operatività e quindi sono più disposte a pagare somme di riscatto ingenti per evitare una perdita di dati fondamentali. Ciò non toglie che anche gli utenti privati possano cadere vittima di un'infezione con un cavallo di Troia crittografante e subire la conseguente perdita di dati.

Cosa fare in caso di danno

La misura più importante si adotta prima che si verifichi il problema: create regolarmente delle copie di sicurezza dei dati (backup)! Naturalmente, un'eventuale infezione del sistema è una scocciatura che comporta un certo lavoro (riformattare e ripristinare), ma si può risolvere. L'importante è che i dati personali siano al sicuro, anche da altre minacce. Ulteriori informazioni sono disponibili nella nostra «fase 1 – Salvare i dati (https://www.ebas.ch/it/1-salvare-i-dati/) ».

Sconsigliamo vivamente di pagare il riscatto! Non c'è nessunissima garanzia che la vittima riotterrà effettivamente la possibilità di accedere ai file cifrati. Inoltre, pagando il riscatto si finanzia il «modello commerciale» dei criminali e si permette loro di sferrare ulteriori attacchi con ransomware danneggiando altre vittime.

Come procedere se avete subito un danno:

- **Spegnete il dispositivo «con le maniere forti».**

Se notate qualche irregolarità nel vostro sistema e sospettate la presenza di ransomware o malware in generale, spegnete il dispositivo «con le maniere forti»! In altre parole, staccate la corrente al dispositivo – estraete immediatamente il cavo di alimentazione o premete il pulsante di accensione e spegnimento per almeno 5 secondi. Questo è l'unico modo per salvare il maggior numero possibile di dati. Agli smartphone e ai tablet non si può semplicemente staccare la corrente, questi dispositivi vanno spenti «normalmente».

- **Pulite il dispositivo con un sistema live.**
  Se possibile e fattibile, avviate il dispositivo con un sistema live come «Desinfec't (https://www.heise.de/download/product/desinfect-71642) » di «c't», da utilizzare per eseguire una scansione e una pulizia e per risalvare i dati. Altrimenti, portate il dispositivo da uno specialista che eseguirà queste operazioni per voi.
- **Se note, applicate delle routine di decriptazione.**
  Siti Internet come www.nomoreransom.org (https://www.nomoreransom.org/it/index.html) mostrano se sono già note delle routine di decriptazione per un ransomware, che si possono scaricare e applicare.
- **Cambiate tutte le vostre password.**
  Ulteriori informazioni sono disponibili nella «fase 4 – Proteggere gli accessi online (https://www.ebas.ch/it/4-proteggere-gli-accessi-online/) ».
- **Informate le autorità.**
  Informate il Centro nazionale per la cibersicurezza (NCSC) compilando il modulo di segnalazione (https://www.report.ncsc.admin.ch/it/) e sporgete denuncia all'ufficio di polizia locale.

Breachstortion

Una strategia di attacco relativamente recente, molto simile e spesso abbinata al ransomware, è la cosiddetta «breachstortion». L'elemento chiave della truffa non è tanto la crittografia dei dati, quanto piuttosto la minaccia di pubblicare informazioni sensibili che danneggerebbero la reputazione della vittima (in genere un'impresa). Per salvaguardare la sua fama, la vittima viene invitata a versare agli hacker una certa quantità di denaro.

Questa strategia si basa sulla paura della vittima e mira ad accentuare la forza della richiesta di riscatto dell'aggressore – se la vittima non è disposta a trasferire la somma necessaria per decrittografare i dati.

Il ransomware rappresenta una precisa famiglia di malware (software dannoso) che si diffonde solitamente attraverso allegati dannosi alle e-mail o pagine Internet infette. Una volta installato, il ransomware cifra i file presenti sul computer della vittima e su eventuali unità e supporti di memorizzazione collegati (come le chiavette USB). I file cifrati diventano quindi inutilizzabili.