RANSOMWARE

La tecnica di utilizzare dei virus e malware per "tenere in ostaggio" un computer e chiedere un riscatto è vecchia di anni (una trentina, più o meno, se si fa risalire il primo attacco del genere al 1989) ma è solo a cavallo tra 2016 e 2017 che i ransomware (letteralmente "virus del riscatto") sono saliti alla ribalta mondiale.
Merito (o colpa, a seconda dei punti di vista) di virus come WannaCry, che nel maggio 2017 è stato capace di infettare centinaia di migliaia di computer (tra i 200 e i 300 mila, secondo alcune stime) nel giro di poche ore. Anche se l'intervento di un ricercatore in sicurezza informatica britannico ha arginato la diffusione del virus del riscatto, da molti esperti del settore è stato considerato come il peggior attacco informatico degli ultimi anni (se non di tutti i tempi): per velocità di contaminazione e portata dell'attacco, WannaCry ha messo in serio pericolo il funzionamento di uffici pubblici, ospedali, catene di montaggio e fabbriche.

Cosa sono i ransomware

Per capire la pericolosità di questa tipologia di virus informatico è necessario, prima di tutto, comprendere cosa sono e cosa significa ransomware. Come detto, la traduzione letterale dall'inglese è "virus del riscatto", definizione che in qualche modo ci aiuta già a capirne il funzionamento. Questa famiglia di malware – non esiste un solo tipo di virus del riscatto, infatti – è in grado di bloccare il funzionamento del computer, facendo sì che l'utente non riesca a effettuare il login nel suo profilo utente (mostrando, solitamente, un avviso dell'FBI o della Polizia di Stato) o utilizzando la crittografia per rendere illeggibili i file presenti all'interno del disco rigido (questi ransomware sono chiamati *cryptolocker*, dal momento che utilizzano la crittografia per bloccare i file). WannaCry, tanto per fare un esempio, appartiene proprio a questa seconda categoria.

Come si diffondono i ransomware

La posta elettronica è il canale di diffusione prediletto dagli hacker. In particolare, i cyber criminali mettono in atto campagne di phishing sempre più elaborate per ingannare gli utenti e "forzarli" a scaricare il virus del riscatto e installarlo sul loro computer. Come ogni altra campagna di phishing, il malware si autoreplica e si diffonde nel web, sfruttando la rubrica email del computer infettato.

Come funzionano i ransomware

Anche se il risultato finale è lo stesso – computer bloccato e inutilizzabile – il funzionamento del virus del riscatto varia a seconda della famiglia di malware che infetta il computer. Nel caso di quello che viene definito "virus della Polizia"), il ransomware blocca l'accesso al sistema informatico mostrando un falso avviso della Polizia Postale o dell'FBI, chiedendo una somma – solitamente non troppo elevata – per sbloccare l'accesso al dispositivo. Nel secondo caso, quello dei *cryptolocker* alla WannaCry, l'utente potrà ancora accedere al suo computer, ma i file (documenti di testo, filmati, file musicali e anche cartelle) saranno crittografati e quindi inutilizzabili. Anche in questo secondo caso sarà richiesto il pagamento di un riscatto per ottenere la chiave di sblocco dell'algoritmo crittografico.
Gli utenti, inoltre, avranno a disposizione un determinato lasso di tempo (solitamente una settimana, a volte anche di meno) per pagare il riscatto: in caso contrario gli hacker non forniranno la chiave di sblocco e l'unica soluzione sarà quella di formattare il computer.

Cosa succede se non paghi?

Anche se può sembrare la soluzione più semplice e immediata, pagare il riscatto non è mai la soluzione migliore. Questo finanzierebbe solamente la rete di malintenzionati che guadagnano da questo tipo di attacchi hacker. Non c'è nessuna assicurazione, poi, che i pirati informatici forniscano effettivamente la chiave di sblocco: potrebbe anche accadere che i criminali "scappino con il bottino", lasciando l'utente senza file e senza soldi.

Come difendersi dai ransomware

Se vi chiedete come evitare i ransomware, la risposta è semplice: basta non scaricarli dalla posta elettronica e installarli nel computer. Necessario, insomma, fare un po' di attenzione quando si naviga a non scaricare file da mittenti o siti sconosciuti. Per difendersi dai ransomware è altrettanto importante aggiornare con costanza il sistema operativo del computer e installare un antivirus che riesca a individuare i malware prima che infettino il dispositivo. Fondamentale, poi, avere un backup con il quale ripristinare il PC nel caso in cui non si riesca a bloccare preventivamente l'infezione del ransomware: ciò permetterà di avere una copia di tutti i file presenti sul disco rigido senza che sia necessario pagare il riscatto.
È quindi importante, per gli utenti singoli così come ancora più importante per le aziende, leggere una guida al ransomware, sapere cos'è, come si prende e come difendersi rimuovendo il virus dal proprio computer e decriptando i file. Grazie ad una prevenzione fatta di consapevolezza del rischio si può evitare infatti di essere

attaccati da ransomware e di doversi trovare a pagare un riscatto tra l’altro senza la certezza di recuperare i file perduti.