Cos’e’ il ransomware? Come si diffonde? La guida su come difendersi



Cos’è il ransomware? Come si diffonde? Come liberarsene? A queste domande cerchiamo di dare delle risposte con questa breve guida su una delle attività più diffuse e dannose in ambito di cybersecurity.

Cos’e’ il ransomware?

Il ransomware è un programma informatico dannoso (“malevolo”) che può “infettare” un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l’accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un **riscatto** (in inglese, “ransom”) da pagare per “liberarli”.

La richiesta di pagamento, con le relative istruzioni, compare di solito in una finestra che si apre automaticamente sullo schermo del dispositivo infettato. All’utente viene

minacciosamente comunicato che ha poche ore o pochi giorni per effettuare il versamento del riscatto, altrimenti il blocco dei contenuti diventerà definitivo.

Ci sono due tipi principali di ransomware:

• i cryptor (che criptano i file contenuti nel dispositivo rendendoli inaccessibili);

• i blocker (che bloccano l'accesso al dispositivo infettato).

Come si diffonde?

Anche se in alcuni casi (non molto frequenti) il ransomware può essere installato sul dispositivo tramite sofisticate forme di attacco informatico (es: controllo da remoto), questo tipo di software malevoli si diffonde soprattutto attraverso comunicazioni ricevute via e-mail, sms o sistemi di messaggistica che:

• sembrano apparentemente provenire da **soggetti conosciuti e affidabili** (ad esempio, corrieri espressi, gestori di servizi, operatori telefonici, pubbliche amministrazioni, ecc.), oppure da **persone fidate** (colleghi di lavoro, conoscenti);

• contengono **allegati** da aprire (spesso "con urgenza"), oppure **link e banner** da cliccare (per verificare informazioni o ricevere importanti avvisi), ovviamente collegati a software malevoli.

Ransomware: 'occhio' al gratis

In altri casi, il ransomware può essere scaricato sul dispositivo quando l'utente:

• clicca link o banner pubblicitari su siti web (un canale molto usato è rappresentato dai siti per adulti) o social network;

• naviga su siti web creati ad hoc o “compromessi” da hacker per diventare veicolo del contagio ransomware.

Il ransomware può essere diffuso da malintenzionati anche attraverso software e app (giochi, utilità per il PC, persino falsi anti-virus), offerti gratuitamente per invogliare gli utenti al download e infettare così i loro dispositivi.

E’ bene ricordare che ogni dispositivo “infettato” ne può “contagiare” altri.

Il ransomware può diffondersi sfruttando, ad esempio, le sincronizzazioni tra dispositivi, i sistemi di condivisione in cloud, oppure può impossessarsi della rubrica dei contatti e utilizzarla per spedire automaticamente ad altre persone messaggi contenenti link e allegati che diventano veicolo del ransomware.

Come difendersi?

La prima e più importante forma di difesa è la prudenza. Occorre evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti (ad es. un operatore telefonico di cui non si è cliente, un corriere espresso da cui non si aspettano consegne, ecc.) e, in ogni caso, se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ognora il contenuto.

Anche se i messaggi provengono da soggetti a noi noti, è comunque bene adottare alcune piccole accortezze.

Ad esempio:

- non aprire mai allegati con estensioni “strane” (ad esempio, allegati con estensione “.exe” sono a rischio, perché potrebbero installare applicazioni di qualche tipo nel dispositivo);
- non scaricare software da siti sospetti (ad esempio,

quelli che offrono gratuitamente prodotti che invece di solito sono a pagamento);
- scaricare preferibilmente app e programmi da market ufficiali, i cui gestori effettuano controlli sui prodotti e dove è eventualmente possibile leggere i commenti di altri utenti che contengono avvisi sui potenziali rischi;
- se si usa un pc, si può passare la freccia del mouse su eventuali link o banner pubblicitari ricevuti via e-mail o presenti su siti web senza aprirli (così, in basso nella finestra del browser, si può vedere l'anteprima del link da aprire e verificare se corrisponde al link che si vede scritto nel messaggio: in caso non corrispondano, c'è ovviamente un rischio).

E' inoltre utile:

- installare su tutti i dispositivi un antivirus con estensioni anti-malware;
- mantenere costantemente aggiornati il sistema operativo oltre che i software e le app che vengono utilizzati più spesso;
- utilizzare dei sistemi di backup che salvino (anche in maniera automatica) una copia dei dati (sono disponibili soluzioni anche libere e gratuite per tutti i sistemi operativi). Con un corretto backup, in caso di necessità, si potranno così ripristinare i dati contenuti nel dispositivo, quantomeno fino all'ultimo salvataggio.

Come liberarsi dal ransomware?

Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di non ricevere i codici di sblocco, o addirittura di finire in "liste di pagatori" potenzialmente soggetti a periodici

attacchi ransomware.

La soluzione consigliata è quella di rivolgersi a tecnici specializzati capaci di sbloccare il dispositivo.

Un’alternativa efficace è quella di formattare il dispositivo: ma in questo caso, oltre ad eliminare il malware, si perdono tutti i dati in esso contenuti. Per questo è fondamentale (come suggerito) effettuare backup periodici dei contenuti (che è sempre una buona prassi) in modo da non perderli in caso di incidenti (es: danneggiamento del dispositivo, ecc.) o attacchi informatici che necessitano di interventi di ripristino.

E’ sempre consigliabile segnalare o denunciare l’attacco ransomware alla **Polizia postale** anche per aiutare a prevenire ulteriori illeciti.

https://www.key4biz.it/cose-il-ransomware-come-si-diffonde-la-guida-su-come-difendersi/319639/