Ransomware: cosa sono? Come proteggersi?

Date : 26 settembre 2016

Malware che criptano i files e chiedono soldi per ripulire la macchina: la diffusione e i metodi attuali per proteggersi dai ransomware.

E’ uno degli strumenti di attacco più efficienti e semplici da attuare: il ransomware.

Si tratta di un virus informatico della famiglia dei cosiddetti “trojan” ed è in grado di rendere invisibili o inaccessibili i files sulla macchina colpita, richiedendo un riscatto da pagare per rimuovere la limitazione.

Quanto possano essere pericolosi potete leggerlo qui, dove vi parliamo di devastanti attacchi operati tramite ransomware a discapito di varie strutture ospedaliere.

La tecnica è molto semplice: la macchina affetta da ransomware non smette di funzionare ma tutti i files - documenti di testo, foto, filmati, musica - vengono resi illeggibili tramite algoritmi di cifratura. La vittima è costretta poi a pagare un riscatto al fine di riottenere l’accesso ai propri files.

Gli attacchi con ransomware sono oggi perpetrati in tutto il mondo ma possiamo collocare la loro nascita in Russia.

Il padre di questa tecnica d’attacco fu il biologo Joseph Popp che, nel 1989, scrisse il trojan “AIDS”, noto anche come “PC Cyborg”, il quale eseguiva un playload mostrando all’utente un messaggio in cui si leggeva che la licenza di un qualche software installato era scaduta, criptava poi i file dell’hard disk e obbligava l’utente a pagare 189 dollari alla “PC Cyborg Corporation” per sbloccare il sistema.

Il metodo d’infezione più comune, tramite modalità differenti, è sicuramente l’apertura da parte della vittima di allegati infetti all’interno di email di phishing.

Dal 2010 in poi iniziarono a diffondersi in maniera notevole le prime versioni di ransomware come Cryptolocker, Cryptowall o TorrentLocker. I trojan in questione si presentavano sotto forma di fatture o note di credito e venivano inviate direttamente in allegato al messaggio,

successivamente, azionato l’attacco, il riscatto era richiesto in bitcoin.

La diffusione dei ransomware è stata a dir poco virale, nel giugno 2013 software house McAfee, specializzata in software di sicurezza, ha rilasciato un report che mostrava un aumento impressionante delle registrazioni di ransomware: più del doppio rispetto all’anno precedente - per un totale di 250.000 attacchi.

CryptoLocker, un worm ransomware apparso alla fine del 2013, ha ottenuto circa 3 milioni di dollari prima di essere reso innocuo dalle auorità.

Con il tempo le mail sono diventate sempre più convincenti, hanno cominciato a contenere codici di tracking di corrieri espresso, risultavano relative a bollette di gestori di energia o ad operatori telefonici. Gli allegati infetti si sono rafforzati e spesso passano incolumi a test di antivirus, una volta aperti rivelano immediatamente la loro natura di malware infettando così i contenuti della macchina su cui si sta navigando.

Recentemente si è diffuso un nuovo metodo d’attacco: alcuni siti web compromessi attecchiscono sui sistemi degli utenti che vi accedono che sono resi vulnerabili da browser con componenti non aggiornate.

A parte alcuni casi specifici, relativi soprattutto a ransomware obsoleti che ormai raramente sono utilizzati dagli hackers, ancora non è stata trovata una via di difesa standard per recuperare i contenuti perduti.

Siamo quindi totalmente impotenti dinanzi ad un ransomware? No, almeno per quanto riguarda la prevenzione. Uno dei metodi più efficienti è sicuramente eseguire periodicamente copie di backup per ripristinare eventualmente i file criptati.

La minaccia è divenuta molto pericolosa, tanto che nel luglio scorso l’agenzia europea di polizia Europol ha unito le forze con varie società di sicurezza informatica per lanciare un’iniziativa mondiale al fine di combatterla.

L’iniziativa, denominata “No More Ransomware” (questo il link al sito: https://www.nomoreransom.org/) , si propone non solo di aiutare le vittima a recuperare il controllo dei propri files ma anche di sensibilizzare ed educare la popolazione al fine di mantenere pulite le macchine. La homepage del sito contiene quattro strumenti di decodifica per ransomware, tra cui il famigerato CryptXXX e le famiglie CoinVault e Bitcrytor, che l’utente può scaricare e tentare sulla macchina infetta.

Speranzosi dell’efficienza di simili iniziative quello che possiamo fare in quanto utenti è, come detto, prevenire: tenere il più possibile aggiornati i propri software, utilizzare un sistema antivirus testato e stare molto attenti ad aprire qualunque tipo di mail, anche quelle che sembrano più innocue.