DIGITAL4TRADE

Cryptolocker, ecco come e quando recuperare i file

di Gianluigi Torchiani

10 Aprile 2017

La prevenzione resta l'arma più efficace per evitare il pericolo ransomware. Ma in certi casi è possibile comunque salvare il salvabile, senza cedere al ricatto del cybercrime

Immaginate di essere al lavoro o casa vostra, una giornata come tante, davanti al computer come tutti i giorni. Improvvisamente lo schermo cambia e compare un messaggio di questo tipo:

Oppure questo.

Purtroppo e già lo avrete capito, significa che siete stati colpiti da un ransomware, la più nota variante del quale è il famosissimo Cryptolocker. Questo significa che tutti i vostri file personali (documenti, fogli excel, immagini e video) sono stati criptati e diventano dunque sostanzialmente inaccessibili. La richiesta dei cybercriminali, che sono riusciti a colpire probabilmente sfruttando la nostra innata curiosità (apertura di un file all'apparenza innocuo, click su un link), è quella di un riscatto, generalmente da pagare in Bitcoin, per riavere indietro i vostri file decrittati. La prima domanda a questo punto è: pagare o non pagare? La risposta che si può dare è che – nella maggioranza dei casi – quando si paga i file vengono effettivamente restituiti integri dai cybercriminali. Non tanto per improbabili ragioni d'onore, quanto piuttosto per salvaguardare il proprio business nel lungo termine. Se infatti si diffondesse la voce che i pagamenti per i cryptolocker sono inutili, nel giro di poco tempo nessuno pagherebbe più il riscatto. D'altra parte però, non esiste nessuna garanzia che il singolo cybercriminale segua un ragionamento così lineare e che, dunque, alla fine decritti effettivamente i file.

Il consiglio più giusto da un punto di vista "sociale" è però sempre quello di non pagare il riscatto richiesto: inviando il vostro denaro ai criminali informatici, non farete altro che confermare che il ransomware funziona. Dunque incoraggerete la preparazione di ulteriore ransomware ai danni di parenti, amici e colleghi e, magari, in futuro nuovamente voi stessi. Ammettiamo dunque che abbiate deciso per l'opzione più limpida. Cosa si può fare per riavere indietro i file criptati? Purtroppo in molti casi, una volta che il ransomware ha infettato il computer o il vostro dispositivo, c'è poco da fare salvo che non abbiate eseguito un backup o installato idonee misure di sicurezza.

Le regole da seguire per evitare i cryptolocker

Regole che sono abbastanza note ma che ricordare per l'ennesima volta non fa di certo male:
1. Assicurarsi che il vostro software di endpoint security sia aggiornato e funzionante.
2. Assicurarsi che il vostro computer sia aggiornato e che tutte le patch siano applicate. Non solo il sistema operativo, ma anche il browser e le applicazioni di terze parti, Java compreso.
3. Molti codici maligni vengono distribuiti attraverso link all'interno di email o di messaggi dei social media, ragion per cui non cliccate su link sospetti o su allegati presenti nelle email, anche se utilizzate un email filtering.
4. Usate il web filtering per prevenire la vostra navigazione su siti infettati da codici maligni – l'80% dei siti infetti sono siti legittimi che sono stati compromessi.
5. Eseguite backup regolari dei vostri file importanti e, se potete, salvateli offline, dove non potranno essere individuati in caso di attacco ai vostri file attivi.
6. Proteggetevi sia in rete, sia nell'endpoint. CryptoLocker richiede una connessione di rete e la Network security può intercettare il tentativo di accesso al server di comando e controllo e bloccarlo. Il malware sarà ancora nel vostro sistema, ma non potrà abilitare il pericoloso payload che cripta le vostre informazioni

Come e quando recuperare i file criptati

Nel caso in cui, sfortunatamente, non abbiate messo in atto questo tipo di protezioni, non dovete del tutto disperare. Esistono infatti ancora delle possibilità di recuperare tutti i vostri file e documenti senza cedere all'odioso ricatto dei cybercriminali. Innanzitutto ci sono degli strumenti disponibili, come Crypto Sheriff è – sviluppato appositamente dall'iniziativa no more ransom – che aiutano a definire il tipo di ransomware che ha infettato il vostro dispositivo. Esistono infatti centinaia di famiglie diverse di ransomware in giro per il mondo e migliaia di varianti. In particolare questo è possibile nei casi in cui:
1) Gli autori del malware hanno fatto un errore d'implementazione ed è possibile forzare la codifica. È il caso, per esempio, dei ransomware Petya e CryptXXX.
2) Gli autori del malware si pentono delle loro azioni e pubblicano le chiavi oppure rilasciano

una master key, come nel caso di TeslaCrypt.
3) Le forze dell'ordine sequestrano un server sul quale sono contenute le chiavi e le condividono. Un esempio è il caso di CoinVault.
Grazie a queste casistiche esistono dunque degli strumenti di decrittazione che permettono di recuperare le vecchie copie dei tuoi dati. Qui si trova un elenco abbastanza esaustivo elaborato dall'iniziativa No more ransom, suddiviso per le diverse famiglie di ransomware.

Le strade alternative per fregare il ransomware

Nel caso il nostro ransomware non faccia parte di queste famiglie esistono poi delle strade alternative, tra cui la più comune è l'utilizzo di Shadow Explorer che, in buona sostanza, permette di recuperare i backup automatici di Windows, se il virus non li ha cancellati. Come spiega il distributore di soluzioni di sicurezza Achab, infatti, alcuni cryptovirus sono così furbi e cattivi che cancellano anche queste copie di riserva, altri invece non le toccano. Se la vittima è stata particolarmente fortunata, le copie di riserva potrebbero non essere state toccate. Una volta in esecuzione, viene mostrata una finestra che permette di scegliere quale "fotografia" del sistema si desidera visualizzare. Si possono quindi esplorare tutte le cartelle e una volta individuato il file che interessa basta fare clic con il tasto destro del mouse e scegliere Export per recuperare la versione desiderata.
Una vera e propria ultima spiaggia è PhotoRec, un software cross platform in grado di andare a cercare i file attraverso le tracce nascoste nei meandri del proprio dispositivo.
Naturalmente la rete è ricca di siti che promettono di riuscire a decrittare i dati infettati dai cryptolocker, con servizi più o meno a pagamento.

In ogni caso, considerando che malware e cryptolocker non sono altro che tipi di malware contenenti codici maligno, vanno sempre comunque rimossi dal proprio pc. Per fortuna la rete pullula di strumenti, spesso offerti gratuitamente dai principali vendor del settore, che permettono in pochi passi una rimozione efficace. Insomma, qualcosa si può fare, ma l'unica vera arma efficace per contrastare ransomware e cryptolocker resta la prevenzione.