Infezioni da CryptoLocker e CryptoWall: dati in ostaggio

Ultimamente si stanno moltiplicando i casi di infezione da questa particolare categoria di virus. Il contagio sembra riguardare esclusivamente i computer dotati di sistemi operativi Windows. Abbiamo deciso di scrivere due righe in merito a fronte dei numerosi PC infetti che sono giunti nel nostro laboratorio nei giorni scorsi per mettere in guardia gli utenti che ancora ignorano questo pericolo.

COME FUNZIONA:

Diversamente da altri tipi di malware, Cryptolocker e CryptoWall sono ransomware che presentano entrambi il prefisso "crypto" perché, rispetto a noti malware (virus Polizia di Stato, Polizia Postale, Guardia di Finanza, ecc.) non cercano di bloccare l'intero sistema ma mirano a provocare un danno ancora maggiore rendendo i dati dell'utente totalmente illeggibili: **documenti e file personali**, in particolare file di Microsoft Office, Open document e altri documenti, immagini e file di Autocad vengono **crittografati utilizzando una coppia di chiavi generate dinamicamente utilizzando l'algoritmo di cifratura asimmetrica RSA a 2048 o 4096 bit**, praticamente inespugnabile. Dopo che il danno è stato fatto l'utente ne viene informato e gli viene richiesto il pagamento di un riscatto (da qui in termine "*ransonmware*"). Nel caso in cui l'utente non provveda a pagare entro un limite di tempo definito la chiave privata viene cancellata rendendo i file definitivamente irrecuperabili.

SI PUO' EVITARE DI PAGARE IL RISCATTO?

A metà circa del 2014 grazie a un'azione coordinata a livello internazionale tra vari enti tra cui l'FBI, è stato possibile mettere le mani sui database di chiavi private prelevate dai sistemi utilizzati dagli sviluppatori di questo ransomware. Si è quindi potuto allestire un servizio online (www.decryptcryptolocker.com) che ha dato modo a migliaia di utenti di recuperare i propri file. Tuttavia questo servizio si è dimostrato totalmente inutile con i PC infettati di recente. Di conseguenza, secondo il parere dei maggiori esperti di ingegneria informatica, l'unico modo per riavere indietro i propri file è quello di pagare il riscatto, in quanto l'unica azione alternativa che si potrebbe intraprendere per tentare un recupero fai-da-te è quella di un attacco di tipo bruteforce che però richiederebbe moltissimo tempo e una potenza di calcolo enorme. Sottostare ai ricatti non è mai bello, e sembra anche che alcuni utenti che hanno pagato il riscatto non si sono poi visti recapitare il programma per decifrare i propri file rimanendo fregati due volte.

PREVENIRE E' MEGLIO CHE CURARE

Dato che le speranze di recuperare i dati sono minime, l'unico metodo per non rimanere fregati è la **prevenzione**. Ecco alcuni consigli utili:

- **Dotarsi di un buon sistema antivirus**, come ad esempio Kaspersky Internet Security. Diffidate da quelli gratuiti in quanto non garantiscono lo stesso livello di protezione di quelli a pagamento: se ci tenete davvero ai vostri dati forse è il caso di spendere qualche euro per una maggiore sicurezza.

- Anche se avete il miglior antivirus sul mercato e lo avete aggiornato all'ultimo secondo dovete **assolutamente evitare di aprire allegati email sospetti**: è questo infatti il metodo principale col quale si sta diffondendo questo tipo di malware. Quindi evitate assolutamente d aprire email di cui non siete assolutamente certi del contenuto.

- E' buona norma effettuare una **scansione antivirus completa** e successivamente **creare un punto di ripristino** del sistema: ciò può dare qualche speranza per il recupero dei dati.

- **Evitate assolutamente siti con contenuti pornografici** perché sono spesso fonte di infezione.

- **Effettuare periodicamente una copia di backup dei vostri dati** su media scollegati dal PC e dalla rete in quanto questo virus non lascia scampo neanche alle periferiche e agli altri PC collegati in rete: **se un PC viene infettato l'intera rete viene irrimediabilmente compromessa**. I backup andrebbero quindi memorizzati su supporti quali CD, DVD e pendrive o harddisk esterni che però dovranno essere scollegati dal PC subito dopo il backup. Per maggiore sicurezza è sempre bene effettuare **due copie di backup degli stessi dati su due media diversi** (ad es. una su DVD e una su pendrive).

- **Cambiare sistema operativo**: il ransomware attacca solo i computer su cui gira Windows, quindi gli utenti Mac e Linux sono relativamente al sicuro, perlomeno non si conoscono varianti di questo malware che girano su sistemi operativi diversi da quelli Microsoft.

- **Passate parola**: diffondere la notizia tra colleghi e amici, magari condividendo questo stesso articolo.