Recentemente un virus sta facendo molto parlare molto di se. Si chiama Criptolocker. Appartiene ad una categoria di virus detti “ransomware“, ovvero che chiedono un riscatto per poter essere rimossi. Si diffonde per email e basta aprire un allegato per contrarre l’infezione.

CryptoLocker generalmente si diffonde come allegato di posta elettronica apparentemente lecito e inoffensivo che sembra provenire da istituzioni legittime, o viene caricato su un computer già facente parte di una botnet.

Un file ZIP allegato alla e-mail contiene un file eseguibile con una icona e una estensione pdf, avvalendosi del fatto che i recenti sistemi Windows non mostrano di default le estensioni dei file (un file chiamato nomefile.pdf.exe sarà mostrato come nomefile.pdf nonostante sia un eseguibile). Alcune varianti del malware possono invece contenere il Trojan Zeus che, a sua volta, installa CryptoLocker.

Come funziona il virus

Cryptolocker, come dice stesso il nome, cripta tutti i file disponibili sull’hard disk con una chiave RSA-2048. Documenti, PDF, immagini, file zip non possono essere più aperti, e vengono cancellati allo scadere del tempo indicato. Appena il virus viene installato, al riavvio del PC si nota subito lo sfondo differente ed un messaggio che indica la presenza del virus. I file non sono immediatamente più leggibili, infatti Windows non li riconosce perchè sono stati criptati. Per poter decriptare i file, il virus propone di pagare una certa somma di denaro. Ovviamente si sconsiglia di effettuare questo pagamento, anche perchè non è certo che successivamente i file vengano decriptati.

Come prevenire ed evitare Cryptolocker

Eliminando l’email sospetta, non avrai niente da temere. Se vuoi prevenire ed evitare

Cryptolocker, è possibile installare un programma chiamato “CryptoPrevent” disponibile cliccando qui: (https://www.foolishit.com/cryptoprevent-malware-prevention/). La versione gratuita si trova alla fine del sito indicato. Questo programma permette di attivare delle regole di restrizione su alcuni tipi di file, impedendo di eseguire dei software potenzialmente dannosi per il sistema. Anche in questo caso non si ha la totale garanzia di non contrarre il virus: gli inventori del virus possono sempre creare delle varianti per eludere queste restrizioni, ma è pur sempre una protezione in più.

Come rimuovere CryptoLocker

Per prima cosa il virus va rimosso, e per farlo c’è bisogno di uno strumento specifico che acceda al sistema a basso livello per controllare tutti i file e rimuovere quelli infetti. Il tool più adatto per questo tipo di operazioni è Norton Power Eraser , uno strumento gratuito distribuito da Symantec. Il suo utilizzo è davvero semplice: basta scaricarlo ed avviare l’installazione confermando le opzioni proposte, e al termine dell’installazione avviare il programma.

Dalla schermata principale clicca su Cerca Rischi e attendi la scansione del sistema. Una volta terminata la scansione i virus rilevati verranno eliminati e dopo aver riavviato il computer è ora il momento di ripristinare il file criptati.

Rielaborazione testo tratto da:
http://www.max89x.it/virus-cryptolocker-cose-come-evitarlo-e-decriptare-i-file/
https://www.giuseppefava.com/come-rimuovere-cryptolocker/
https://it.wikipedia.org/wiki/CryptoLocker