“Cryptolocker”, “Cryptowall” o “CBT-locker”… attenzione agli allegati delle vostre email.

di Paolo Franzese

In questi giorni molti utenti ci segnalano di aver beccato un “bastardissimo” ransomware denominato “**Cryptolocker**” o “**Cryptowall**” o “**CBT-locker**” .

L’infezione si contrae da una mail con un allegato manipolato che aggira le sicurezze antivirus.

La sottile strategia utilizzata è dare agli allegati nomi come… F24, Fattura insoluta, Ricorso fallimento, etc…per indurre l’utente ad aprirlo
(in realtà l’utente autorizzerà l’esecuzione di un software) che “**CRIPTERÀ**” tutti i files (DOC, XLS, PDF, CAB, SCR, etc) presenti sul PC, rendendoli praticamente inutilizzabili.

Occorre quindi prestare scrupolosa attenzione ai msg di posta ed attuare le seguenti misure cautelative:
– Avere copia dei documenti e dei files importanti, nelle cartelle del server, che provvederà al backup giornaliero (*l’unica soluzione efficace al momento*);
– Anche se la curiosità è tentatrice, non aprire mail da mittenti sconosciuti o non attendibili;
– Fare attenzione al tipo di allegato alla mail, quindi verificare che non sia un eseguibile (*quelli con estensione EXE*);

Ovviamente queste regole sarà bene applicarle sempre… il 2015 sarà un anno difficile per l’ **hacking nel digitale**!!

Per chi vuole approfondire l’argomento questo è un link che vi chiarirà la pericolosità :
http://www.repubblica.it/tecnologia/2015/01/21/news/paga_o_il_virus_distrugger_il_pc_ora_gli_hacker_ch
105404305/

a cura di **Guido Damian** (IT Manager http://www.tecnodigi.it)

Da un articolo scritto da Paolo Franzese il 29 Gennaio 2015