VareseNews

Attacco informatico, ecco che cosa fare

Pubblicato: Giovedì 4 Febbraio 2016

L'articolo di ieri "Un hacker ha cancellato il mio passato, ho pagato per riaverlo" ha suscitato parecchio interesse tra i nostri lettori. C'è chi ci ha scritto di essere stato a sua volta vittima dell'attacco informatico e chi ci ha mandato suggerimenti per non incappare nella truffa.

Come ad esempio Federica che ci ha scritto sulla nostra pagina Facebook questo messaggio che vi giriamo:

Un mio collega mi ha fatto leggere questo articolo e l'ho trovato molto interessante. Ho visto che un lettore ha avuto, purtroppo, questa brutta sorpresa.
Magari diffondendo questo messaggio potremmo evitare altri episodi
In ogni caso, quello che noi consigliamo sempre ai nostri clienti è DI FARE BACKUP REGOLARI DEI DATI, IN HARD DISK ESTERNI, AL FINE DI NON PERDERLI!!

In fondo alla citazione ho lasciato il link dell'articolo.
"Attenzione, sabato 30 gennaio 2016 è stata lanciata una pesante campagna d'infezione tramite e-mail con ransomware TeslaCrypt 3.0 verso utenti italiani. I file vengono criptati aggiungendo in coda le estensioni ".XXX", ".TTT" e ".MICRO" e rispetto alle versioni di TeslaCrypt precedenti è cambiato il metodo con cui viene scambiata la chiave di cifratura. A differenza di alcune versioni di CryptoLocker e le vecchie versioni di TeslaCrypt, non sono al momento noti metodi per recuperare i propri documenti.

Alcune mail vettore contengono come oggetto il nome del mittente oppure la data d'invio e provengono da contatti noti. Non c'è testo nella mail, se non la data d'invio della mail riportata per esteso, talvolta identica a quella inserita nell'oggetto. Le mail hanno tutte un allegato, consistente in un archivio ZIP che contiene un file con estensione ".JS". ll file è no script in linguaggio javascript, il cui nome può essere del tipo "invoice_DjzkX0.js" o "invoice_scan_jWNWc3.js". Lo script, se aperto, causa il download del vero e proprio trojan TeslaCrypt. IL javascript infatti implementa la funzione di dropper, cioè un malware finalizzato a scaricare il vero e propriotrojan, chiamato payload, che infetterà il PC.

Il codice del dropper (il "programma" contenuto nell'allegato ZIP che spesso si presenta come una finta fattura o una nota di credito) non è offuscato e mostra chiaramente la fonte da cui attinge per scaricare il trojan TeslaCrpyt 3.0 sul PC della vittima, infettarla e criptare i documenti. Per quanto pericoloso, il codice viene eseguito soltanto se si apre l'archivio ZIP (in genere cliccandovi sopra con il mouse) e si clicca sul file il cui nome termina con ".JS" al suo interno.

Una volta criptati i documenti, il ransomware lascia un messaggio nelle cartelle dove risiedono i file codificati, chiamato "help_recover_instructions.BMP" e "help_recover_instructions.txt"

Il testo ove viene richiesto il riscatto in bitcoin è importante perché contiene il riferimento cui è legata la chiave privata necessaria per decriptare i documenti. Lo si trova all'interno dei file con le istruzioni lasciato dal ransomware sul PC

All'indirizzo segnalato dal ransomware si troverà una pagina che ricicla parte del codice e grafica CryptoWall e si presenta con uno sfondo blu e il solito testo che comunica l'indirizzo Bitcoin verso il quale eseguire il versamento e le condizioni di pagamento. Dalla stessa pagina, le vittime che pagano il

riscatto scaricheranno decryptor, il software per decriptare i propri documenti.

Il consiglio per le vittime è ovviamente di non pagare il riscatto, che viene richiesto in bitcoin per una cifra iniziale di 500 dollari che raddoppia dopo alcuni giorni.

Il consiglio per chi riceve email con allegati ZIP, anche da contatti noti, è come al solito quello di non aprirli ed eventualmente contattare il mittente.

L’articolo completo anche di immagini esplicative lo trovate qui

Redazione VareseNews
redazione@varesenews.it