LegnanoNews
Le news di Legnano e dell'Alto Milanese

“Non aprite quella mail”

Valeria Arini · Tuesday, February 2nd, 2016

Stanno circolando in questi giorni una serie di mail contenenti pericolosi virus per i software dei computer. Si tratta di una nuova ondata di ransomware Teslacrypt 3.0. Si tratta di un tipo di malware che limita l'accesso del dispositivo che infetta, **richiedendo un riscatto** (ransom in Inglese) da pagare per rimuovere la limitazione. Questa forma di ransomware, in particolare, blocca il sistema e intima l'utente a pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro.

Come riportato sul sito ransomware.it sabato 30 gennaio 2016 è stata lanciata una pesante campagna d’infezione tramite email 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. BloodDolly,** lo sviluppatore che ha prodotto un decryptor per le versioni precedenti di Teslacrypt, **sta lavorando alla ricerca di un antidoto anche per questa.**

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 uno 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 proprio trojan, 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. La semplice apertura e visualizzazione del testo della mail – in questo caso – non causa l’infezione del PC.

Il consiglio, come spiegano i professionisti della società legnanese Wom, per chi riceve email con allegati ZIP, anche da contatti noti, è quello di non aprirli ed eventualmente contattare il mittente.

E' buona abitudine, inoltre, effettuare un backup periodico dei dati del proprio computer su un supporto esterno rimovibile (Hard Disk o "chiavetta" USB). Fate attenzione però a non collegare questi dispositivi al computer ancora infetto, potrebbero essere resi anch'essi irrecuperabili.

This entry was posted on Tuesday, February 2nd, 2016 at 2:02 pm and is filed under Cronaca, Legnano
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.