CORRIERE DELLA SERA
CorrierEconomia

Virus Il fenomeno del «ransomware» colpisce soprattutto l'Italia. Attenzione all'oggetto della mail

Sicurezza I pirati della Rete vogliono il riscatto: non pagate

«Paga o distruggiamo i tuoi dati». La prima regola è non cedere

DI **UMBERTO TORELLI**

Quando arriva nella casella di posta elettronica, sembra una comune email di avviso pagamento. In cui, ad esempio, si comunica che nel bimestre abbiamo consumato più energia elettrica. Oppure viene chiesta conferma di una transazione online, o una precisazione dall'Agenzia delle Entrate.

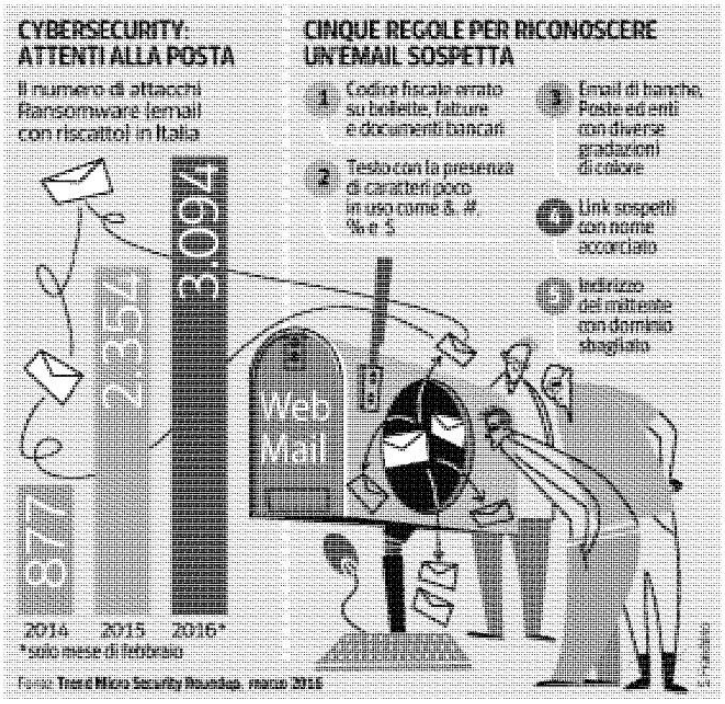
Ma una volta aperta, con il semplice clic del mouse, l'email contiene un «ransomware» (dall'inglese ransom, riscatto). È uno dei più temibili virus messi in circolazione dai cybercriminali negli ultimi anni.

Non lascia scampo a chi ne viene colpito, a meno che non paghi il riscatto economico richiesto, entro poche ore.

Il primato nazionale

Si va da qualche centinaia di euro a parecchie migliaia. Pena la cancellazione di tutti i dati del computer. A lanciare l'allarme in Italia è Trend Micro, azienda giapponese specializzata in sicurezza informatica. I numeri parlano chiaro. Lo scorso anno il nostro Paese è stato colpito da 2.384 ransomware.

«Ebbene, nel solo mese di febbraio 2016 gli attacchi messi a segno con questo sistema sono stati 3.094 — dice Gastone Nencini, responsabile italiano di Trend Micro —. È più di tutti quelli del 2015 e corrisponde al 24,6% del totale mondiale».



In pratica, ha colpito l'Italia un attacco su quattro nel mondo, fra tutti gli atti di pirateria con la richiesta di riscatto. Nella maggioranza dei casi si tratta di crypto-ransomware, cioè *malware* che crittografano i documenti, rendendoli inaccessibili.

Gli attacchi sono basati su quello che gli addetti ai lavori chiamano *social engineer* (ingegneria sociale). In pratica, i pirati informatici cattu-rano l'identità digitale dell'utente. Poi fanno leva sulle attitudini delle vittime per persuaderle ad aprire allegati e cliccare a link correlati.

Ad esempio, dopo una visita in albergo chiedono conferma dei pagamenti. Oppure inviano domande e presunte informazioni su biglietti turistici acquistati online, spedizioni di merci, conferma di fatture e operazioni bancarie.

«In Trend Micro consigliamo di non pagare il riscatto — continua Nencini — perchè non esiste certezza della restituzione dei dati».

Il pericolo è restare intrappolati in una spirale senza fine di riscatti. «Con il rischio di finire nella rete di una sorta di "pizzo" elettronico», avverte l'esperto.

In Italia è capitato a privati cittadini e professionisti, ma anche a istituzioni: che con il back-up (il salvataggio dei dati) hanno però potuto, secondo Trend Micro, recuperare le informazioni cancellate o rese inservibili. «Fare prevenzione è perciò essenziale — raccomanda Nencini — Va eseguita con continuità l'archiviazione, su hard-disk esterno e sul cloud». Poi, in caso di attacco, bisogna riformattare da zero i computer e installare un sistema di protezione completo.

Le cautele

Ad analizzare l'assedio quotidiano delle nostre caselle di posta elettronica (mailbox) da comunicazioni indesiderate è Libraesva. Una società informatica di Lecco, specializzata nello sviluppo di software per email sicure. «Allo spam quotidiano si aggiungono sempre più spesso gli attacchi pericolosi come phishing e randsomware — dice Paolo Frizzi, amministratore delegato —. Per i ricatti informatici uno degli errori più frequenti commessi dai pirati è la scrittura errata del codice fiscale, anche nel numero dei caratteri».

La raccomandazione resta quella di non usare un'unica password e cambiarla con regolarità.

Inoltre bisogna verificare con cura i messaggi in arrivo, guardando per prima cosa l'oggetto della email. Se contiene simboli poco usati come &, #, % e $ deve scattare il campanello d'allarme. Nel dubbio, non aprite quell'email.

@utorelli