del 20 Ottobre 2014 CORRIERE DELLA SERA

La mail pirata attacca i Comu
E il riscatto va pagato in bitc

Parte dalla Russia e beffa gli antivirus, decine di amministrazioni

MILANO L'anagrafe non può più rilasciare i certificati, la contabilità non riesce a pagare, il protocollo è fermo perché anche lì i documenti sono bloccati: sono gli effetti del virus informatico di ultima generazione che sta infestando i pc di decine di Comuni in tutta Italia. Per eliminarlo si deve pagare un riscatto: 400 euro, ovviamente in bitcoin, il doppio se lo si fa dopo tre giorni.

Arriva da San Pietroburgo (Russia) l'ultimo «ransomware» (dall'inglese *ransom*: riscatto) che da mercoledì si sta diffondendo a macchia d'olio attraverso le reti informatiche dei Comuni. Solo alcuni antivirus hanno già fatto in tempo ad aggiornarsi e a bloccarlo. Dopo aver rubato la rubrica di posta elettronica di un qualche ufficio in una qualunque città, che spesso contiene gli indirizzi di altri Comuni, il virus spedisce a nome dello stesso ufficio il file «Compenso.Pdf» seguito da una lunga linea continua.

Provenendo da un indirizzo insospettabile e facendo pensare a un qualche pagamento, molti impiegati lo aprono senza rendersi conto che alla fine della linea continua, nascosto oltre la schermata, c'è la pericolosissima estensione «.exe». Non è un documento, ma un programma che immediatamente cripta nei pc e nei server i file documenti pfd, word o excel, ma anche le foto, rendendoli inutilizzabili. «Una cosa inimmaginabile che ci ha bloccati per tre giorni. Avevamo l'antivirus, ma non è bastato» racconta Maria Cristina Di.Fo.B., lo studio di consulenza informatica forense che collabora con le Procure in molte inchieste, come quelle sull'Expo a Milano, sulla Concordia a Grosseto e sul Mose a Venezia e che sta fornendo assistenza a molti dei Comuni infettati. «Solo chi ha una copia di riserva dei documenti si salva, gli altri devono pagare i criminali» aggiunge il collega Giuseppe Dezzani. In che modo? Sullo schermo appare un messaggio che invita ad acquistare un «software di decodifica» per 400 euro in bitcoin, spiegando anche come fare. «Purtroppo — dice Dal Checco — il sistema bitcoin prevede che le transazioni e gli indirizzi su cui vengono fatte, una sorta di Iban, siano pubblici, ma non c'è modo di attribuire un indirizzo a un nome». Monitorando due di questi indirizzi, la Di.Fo.B. ha scoperto che i cybercriminali in soli 5 giorni «hanno incassato circa 100 mila dollari».

Dopo averle provate tutte, mercoledì a Bussoleno hanno deciso di mettere mano al portafoglio. «Abbiamo fatto una colletta tra noi in attesa di capire come giustificare la spesa. Dopo che abbiamo pagato hanno anche avuto la spudoratezza di invitarci a contattarli nel caso avessimo altri problemi», racconta Mazzolari che sta preparando una denuncia alla Procura di Torino. «Fare attenzione — avverte Dezzani — alle mail, anche quelle di amici questa mattina, quando gli uffici dei Comuni riapriranno dopo il fine settimana. C'è il rischio che il fenomeno prenda