CORRIERE DELLA SERA

LA RICERCA

Ransomware, in Italia colpito il 93% delle piccole e medie imprese

I dati dell'italiana Achab raccontano la diffusione nel Paese del malware che «rapisce» gli hard-disk e chiede un riscatto per liberarli. Un fenomeno da un miliardo di dollari a livello globale

di Federico Cella

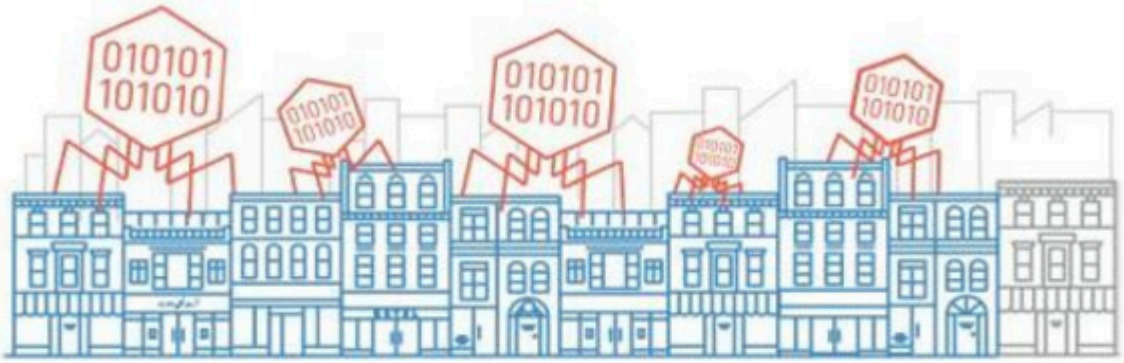
1. Molti attacchi, poche denunce

Scheda 1 di 3
AVANTI

Secondo l'ultimo rapporto del Clusit, l'Associazione italiana per la sicurezza informatica, non solo il 2016 è stato l'anno peggiore per gli attacchi subiti dai sistemi IT a livello mondiale, ma per la prima volta l'Italia rientra nella top 10 degli attacchi più gravi e per numero di vittime. L'attacco subito dalla Farnesina è stato l'elemento di punta, ma in generale il Paese è salito nelle classifiche per quantità di realtà che hanno subito una qualche attività di cyber-crimine. A febbraio il Cisr (Comitato Interministeriale per la Sicurezza della Repubblica) ha dato vita a un nuovo decreto per dare vita un programma nazionale per la cybersecurity che aggiorni e sostituisca quello del gennaio 2013. Sull'Italia secondo il Clusit in particolare saltano agli occhi gli attacchi di ransomware, file malevoli che di fatto prendono possesso degli hard disk di un'azienda, anche pubblica, o di un privato e che chiedono un riscatto per sbloccarli. Un fenomeno di cui abbiamo già parlato e che risulta forte nel nostro Paese. I motivi sono legati alla forte impreparazione tecnica di molte Pmi e al fatto che mancano i processi alternativi al pagamento per affrontare l'emergenza. La realtà è che i ransomware, in un 2016 che ha visto una media di 2500 attacchi al secondo nel mondo, hanno registrato un aumento a livello globale. Trend Micro ne ha registrati 247 tipologie alla fine dell'anno, partendo dai 29 a gennaio 2016. Attacchi che hanno portato nelle casse dei criminali una cifra intorno al miliardo di dollari.

IL RANSOMWARE È UN PROBLEMA DIFFUSO

Il rischio di subire attacchi ransomware è quasi una certezza
9 fornitori di servizi IT su 10 negli ultimi 12 mesi
hanno eseguito interventi a causa di infezioni da cryptovirus



datto WEBROOT

ACHAB

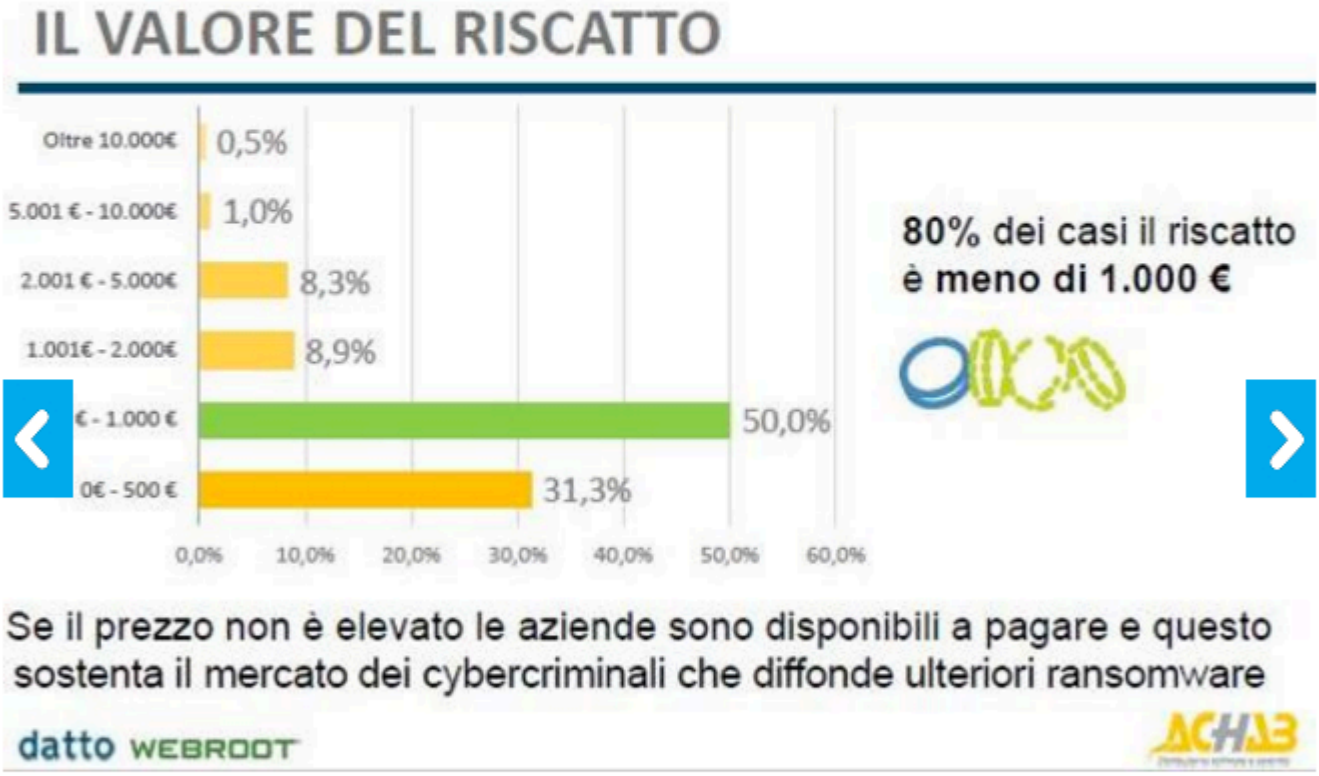
Su questo tipo di attacchi, il distributore italiano di software per le imprese Achab ha svolto una ricerca per capire la reale entità del fenomeno. Che sembra essere un vero flagello per le piccole e medie imprese italiane: secondo Achab, sui duecento fornitori di IT intervistati, il 93% negli ultimi 12 mesi ha effettuato interventi tecnici a causa di ransomware che hanno colpito le aziende a cui forniscono i servizi. Più di 9 realtà su 10, dunque, a fronte di meno del 25% degli attacchi criminali che sono stati denunciati alle autorità e del 37% che ha deciso di pagare un riscatto per tornare in possesso dei dati bloccati. La ricerca, anticipata al *Corriere*, verrà raccontata dagli esperti di Achab in occasione del Ransomware Day organizzato a Milano il prossimo 4 aprile.

Non è un problema solo italiano

27 marzo 2017 | 17:13

2. Non è un problema solo italiano

Serve ripetere che se il fenomeno da noi è molto forte, il tipo di attacco ha una diffusione mondiale non indifferente proprio per la sua tipologia che lo rende molto difficile da evitare – mancano vere soluzione software di prevenzione -, e ha dalla sua la "forza" di basarsi sui grandi numeri. Il riscatto richiesto solitamente è molto basso, dunque si sceglie di pagarlo (e non denunciarlo, come visto) per poter ripartire senza troppi fastidi. Se non procurarsi dei Bitcoin per il pagamento. Questo sistema diffuso su milioni di attacchi porta alla cifra raccontata prima. Infatti se i dati mondiali non arrivano al 90% raccontato da Achab per l'Italia, l'americana Osterman Research riporta come sempre lo scorso anno almeno il 50% delle aziende intervistate aveva subito un attacco finalizzato al pagamento di un riscatto. Ricordiamo per esempio il clamoroso attacco all'azienda dei trasporti pubblici di San Francisco dello scorso novembre.



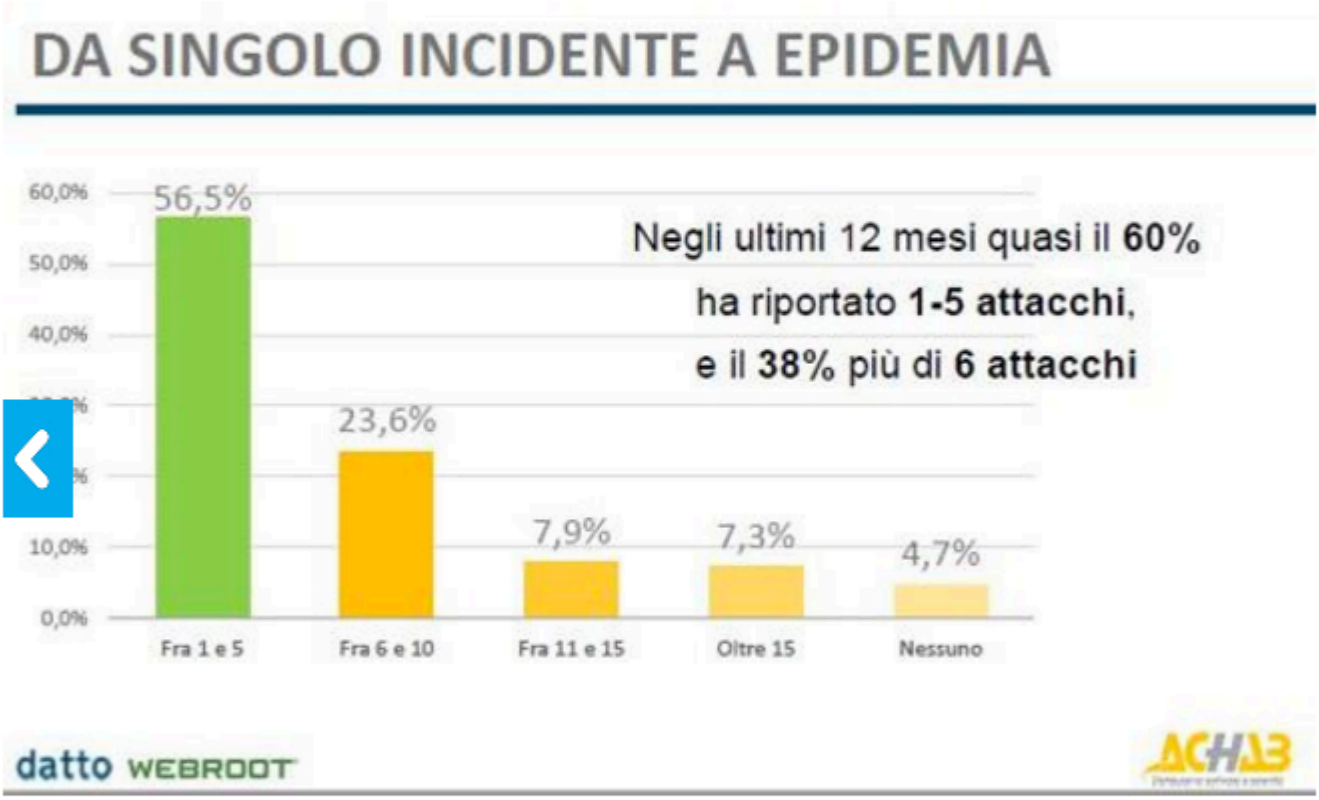
In quel caso la cifra richiesta era di 70 mila dollari. Nel survey, Achab ha registrato come nell'81% dei casi la cifra richiesta non superi i mille euro, ossia un esborso che anche una piccola impresa può pensare di affrontare per tornare rapidamente al lavoro.

Molti attacchi, poche denunce
Non bisogna pagare

27 marzo 2017 | 17:13

3. Non bisogna pagare

Bisogna dire che in un terzo dei casi raccontati dal service italiano anche chi ha pagato il riscatto non è tornato in possesso dei proprio dati. Pagare dunque, oltre a dare sostengo all'attività criminale, non è un sistema sicuro. Mentre in alcuni Paesi, come l'Olanda, esistono task force di intervento su casi di attività cyber-criminali, in Italia spesso ci si riduce a pagare. Per evitare questo serve una maggiore preparazione sul lato tecnico delle aziende, come sempre attenzione allo spam di email e a siti ingannevoli – i luoghi dove si annida il malware – e quindi un sistema software che permetta all'azienda di recuperare il prima possibile le attività a seguito di un attacco. Mancando la reale possibilità di prevenire, la cura rapida è la soluzione migliore.



Questo anche perché un attacco può essere il sintomo- soprattutto se va a buon fine – di una serie di altre richieste di pagamento. L'ultima slide di Achab che raccontiamo è proprio sulle frequenza dei ransomware denunciati da chi fornisce servizi IT alle aziende: quasi il 40% è sulla cifra di 6-10 attacchi nell'arco di un anno.

Non è un problema solo italiano

27 marzo 2017 | 17:13