DIGITAL4TRADE

SURVEY ESCLUSIVE

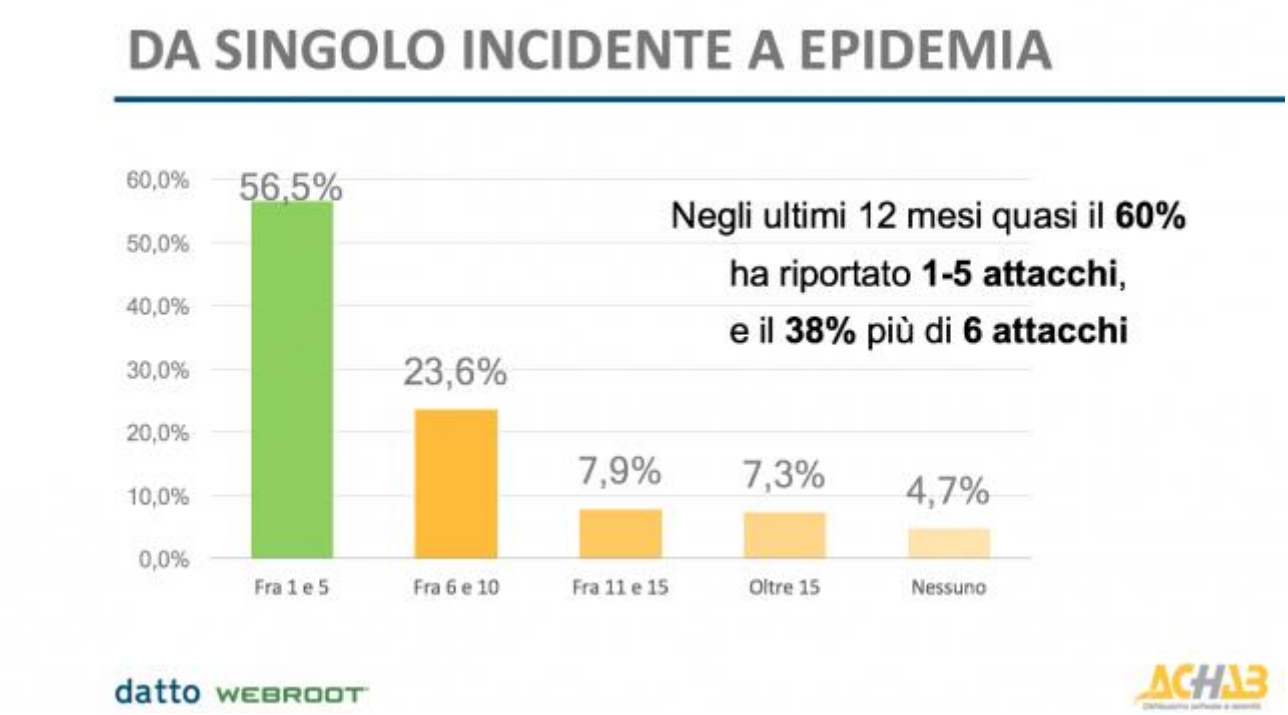
Cosi i Ransomware bloccano l'Italia: il 93% di Reseller IT ha effettuato almeno un intervento. Cryptolocker il più diffuso

di Marco Maria Lorusso

29 Mar 2017

I dati allarmanti di una ricerca esclusiva condotta da Achab in collaborazione con Digital4Trade. Intervistati oltre 200 fornitori di servizi IT dichiarando le loro esperienze in merito agli attacchi ransomware. Meno di un incidente su 4 viene denunciato alle autorità

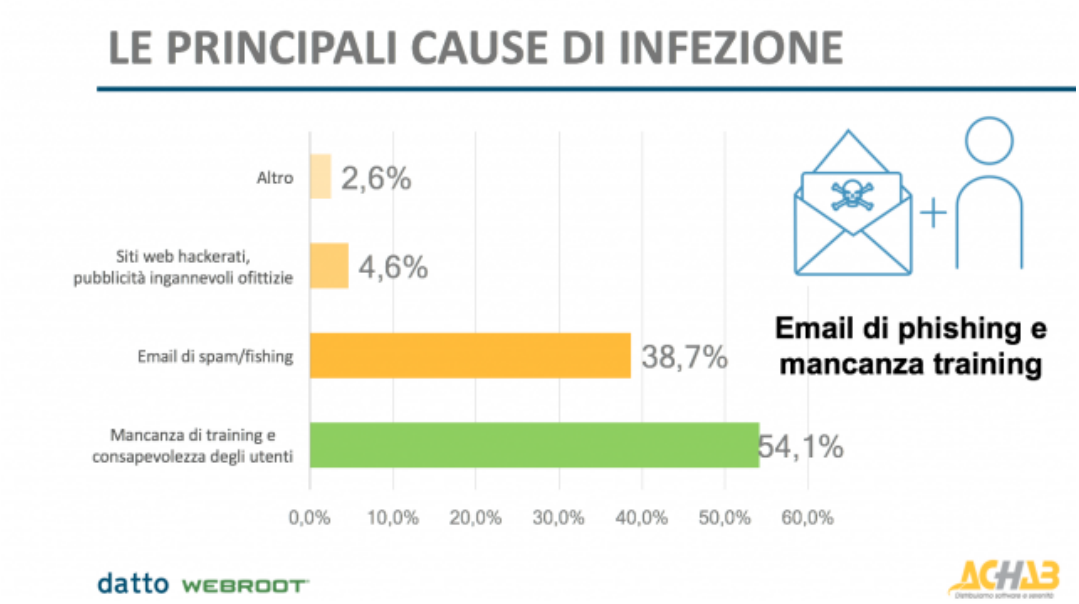
Il 93% dei fornitori di servizi IT negli ultimi 12 mesi ha effettuato interventi tecnici a causa del ransomware, un fenomeno destinato a crescere nei prossimi due anni.
Meno di un incidente su 4 viene denunciato alle autorità. La scarsa consapevolezza degli utenti, la mancanza di training e le email di phishing e spam sono le principali cause di infezione. Il 93% di chi ha subito attacchi ha accusato downtime e/o perdita di dati. Pizzo digitale, ransomware, Cryptolocker… chiamatelo un po' come volete ma, nei numeri e nei fatti questa è una piaga che continua a fare male, e molto, alle imprese italiane e non solo. Una piaga che emerge nitida come non mai, in una ricerca, esclusiva, sviluppata da un distributore IT come Achab in collaborazione con Digital4Trade. Una survey che ha chiamato in causa oltre 200 fornitori di servizi IT e che sarà mostrata e discussa il prossimo 4 aprile nel corso dell'atteso Ransomware Day di Milano. Un evento che si propone di mettere un punto chiaro sul fenomeno IT più doloroso degli ultimi anni con interventi e discussioni concrete e di alto valore.



I numeri della piaga

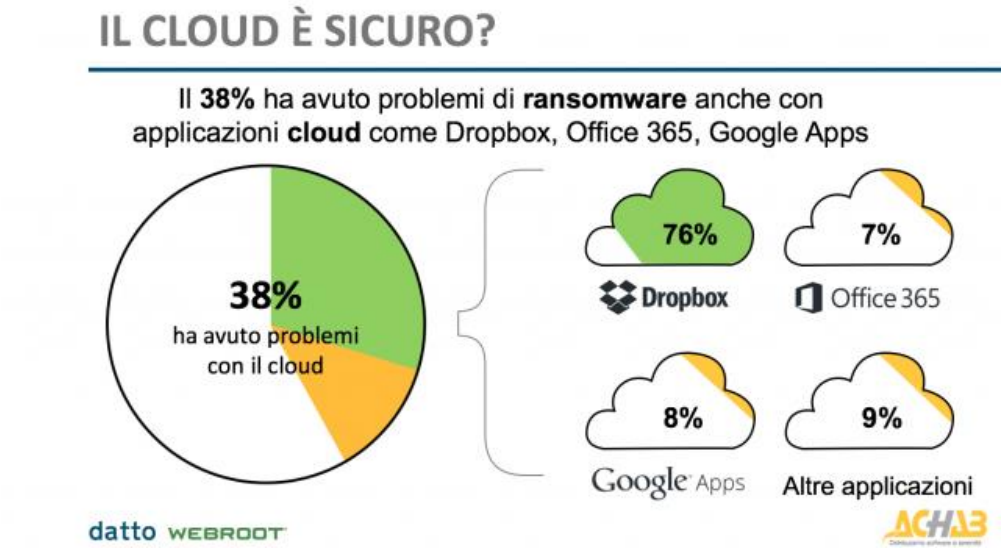
Ma tornando ai numeri della survey, che mostriamo qui in anteprima, «Per come i dati oggi vengono trattati in azienda e per la centralità del dato in ogni tipo di attività, il ransomware ha la capacità di distruggere aziende, anche grandi, nel giro di pochi minuti – raccontano Andrea Veca e Claudio Panerai, rispettivamente CEO e CTO che hanno ideato e spinto la survey e il progetto dell'evento -. E benché alcune aziende inizino a utilizzare sistemi antivirus di nuova generazione e soluzioni di business continuity, la verità è che la maggior parte delle imprese non sono preparate per attacchi di questo tipo.
E questo è maggiormente vero nel mercato delle piccole e medie imprese dove spesso non c'è un informatico dedicato a gestire l'IT e dove spesso si utilizzano sistemi informatici «vecchi». La verità è che queste realtà fanno affidamento ai propri dati per lavorare né più né meno delle multinazionali, ma a differenza di queste ultime non hanno gli strumenti, la protezione e la preparazione per difendersi e reagire ad attacchi di ransomware. I cybercriminali oggi sono consapevoli di questa situazione e ne approfittano guadagnando miliardi di dollari. Sì, miliardi!. Nasce così l'idea e la pratica di una survey e un evento dedicati a coloro che hanno il compito, cruciale, di portare innovazione digitale nelle imprese, ai manager e nelle nostre case, il canale, i reseller, i provider di servizi IT da cui, oggi più che mai, passa la possibile svolta o la condanna allo scacco

costante di fronte ad attacchi che, come raccontano i numeri, puntano forte proprio sul bassissimo livello delle competenze di chi con gli strumenti IT ci lavora.



La consapevolezza

A questo proposito, la ricerca è chiara, c'è una grande differenza di consapevolezza sui rischi del ransomware fra chi si occupa di IT e i clienti: solo il 24% dei clienti è consapevole dei rischi. Cryptolocker è di gran lunga il ransomware più diffuso.
Altro tema chiave è quello legato al riscatto, chiave di volta del funzionamento della trappola cryptolocker.
«Il pagamento del riscatto – racconta Panerai – non garantisce il recupero dei dati: il 37% dei fornitori di servizi IT ha pagato il riscatto almeno una volta e di questi in 1 caso su 3 è successo di non riavere i dati anche dopo aver pagato. Le richieste di riscatto per l'81% dei casi non supera i 1.000 €, ma si sono verificati casi in cui le richieste abbiano superato i 10.000 €. Va detto comunque che in generale, benché il tipico riscatto non sia generalmente una somma elevata da prosciugare il conto in banca, il costo del downtime e della perdita di dati conseguente a un attacco ransomware è il danno maggiore da sostenere».



Ma il cloud è sicuro?

Inevitabilmente una parte della ricerca è stata dedicata al cloud. Paradigma che trasforma l'IT in servizio e che, proprio in tema di privacy, gestione dei dati critici e sicurezza in generale è da tempo al centro del mirino come raccontano i dati dell'Osservatorio Cloud & ICT as a service del Politecnico di Milano.
«Il cloud – spiega Veca – non è al riparo dal ransomware: il 38% dei fornitori di servizi IT ha visto infezioni anche su diffuse applicazioni cloud come Dropbox (76%), Office 365 (7%), Google Apps (8%)…»

Come provare a difendersi dunque?

«Le soluzioni di sicurezza tradizionali non sono in grado di arginare gli attacchi di ransomware – concludono i manager . Una sintesi abbastanza chiara ed evidente che è tutta nei numeri di questa survey e in quello che ci raccontano fonti autorevoli come il Clusit per esempio. Sul fronte tecnologico la risposta migliore, oltre a un sistematico aggiornamento di sistemi, applicazioni e antivirus, è l'adozione di un sistema di Disaster Recovery e Business Continuity».

Attacchi, numeri, sistemi di difesa, strade possibili e impossibili, errori da evitare, tutti i numeri completi della survey e gli interventi dei massimi esperti italiani in materia di sicurezza, sistemi di attacco, normative, sistemi di difesa… tutto insieme, tutto in un giorno sarà disponibile il prossimo 4 aprile a Milano nel corso del #RansomwareDay.