Libero
QUOTIDIANO: MILANO

Guido Mondelli, ad di Assiteca Sicurezza Informatica

«Il vero punto debole è il settore pubblico non a norma»

FRANCESCO RIGATELLI

Ma quale *ransonware*, si tratta di un banale *worm*, sostiene Guido Mondelli, 57 anni, ad di Assiteca Sicurezza Informatica, società di consulenza che vanta tra i suoi clienti le maggiori aziende del settore bancario, assicurativo, petrolifero e della grande distribuzione.

«La differenza - spiega - è che questo virus parte da solo, non ha bisogno dell'intervento umano, insomma del nostro clic. La falla ormai nota è quella dei server Microsoft non aggiornati da alcune aziende. Chi all'interno di esse ha ricevuto l'email infetta e l'ha aperta ha propagato il virus all'infinito. Il primo allarme lo ha dato l'altra mattina la società spagnola Telefonica. Quando si toccano aziende così grandi, come pure Renault in Francia, l'effetto è immediato. Tutti i file nei pc degli infettati diventavano criptati e arrivava la minaccia di pagare 300 dollari in bitcoin, la moneta elettronica, entro il 15 maggio per vederli ricomparire».

Il primo consiglio del supertecnico è «mai pagare, è reato e le grandi aziende salvano sempre copia di tutto. Tanto è vero che lunedì la Renault riparte senza problemi». Dietrologia vuole che l'attacco venga dalla Cina, ma è vero? «Un hacker utilizza tecniche per nascondere il vero indirizzo ip. In questo caso si tratta di un'organizzazione criminale che può essere ovunque. Un modo per rintracciarla è seguire il denaro, scoprire dove si appoggiano i conti dei bitcoin, ma si arriverebbe a Paesi poco trasparenti sulle banche».

In Italia non ci sono stati danni, «anche perché molte aziende usano un sistema operativo diverso da Microsoft. Attacchi come questo ci sono di continuo, solo che stavolta sono stati bravi a trovare la finestra giusta dell'aggiornamento mancato. Hanno spedito ovunque tramite email di spam il *worm* o forse hanno attaccato direttamente alcuni server non aggiornati. Tra quindici giorni mi aspetto un episodio simile, perché molte aziende non aggiorneranno nulla. Farlo significa infatti non riuscire a usare più tanti programmi. Per questo servono società come la nostra che suggeriscono come mettersi al sicuro. Le banche hanno intere strutture dedicate al tema, così le maggiori aziende e anche alcune società pubbliche, ma in generale si è agli albori e il vero punto debole resta il settore pubblico dove pochi sono a norma rispetto alla circolare di un anno fa dell'Agenzia per il digitale». Senza contare i privati, presto ancora più esposti all'internet degli oggetti: «Ci cambierà la vita, ma ci sono già stati dei ritiri di prodotti facilmente hackerabili».

Di hackeraggi ce ne sono di tanti tipi. Partiamo da quelli nei confronti delle aziende: «Il più frequente è di chi spara nel mucchio con una richiesta economica, come nel caso del *worm*. Ci sono poi quelli mirati, per esempio diretti a intercettare un bonifico specifico. E quelli riguardanti documenti, non solo politici ma pensiamo anche ai disegni industriali di prodotti nuovi. Senza dimenticare sabotaggi e persecuzioni».

Cosa può fare un'azienda? «Usare il buon senso, non cadere nel panico e adottare una strategia. Vanno decisi i documenti a rischio, tolti dal server quelli non necessari e crittografati gli altri. Occorrono procedure, regole, formazione, autorizzazioni specifiche per l'accesso e istruzioni per l'uso». E un privato cosa può fare? «Anche per lui valgono le buone vecchie regole della realtà. Buon senso e non fidarsi. Insomma, non accettare le caramelle dagli sconosciuti. Non aprire e non cliccare sul contenuto di email dal mittente incerto, verificare cosa si installa su pc e cellulare. Nel dubbio, non rispondere. Diffidare delle mode come Whatsapp: un sms è molto più sicuro. E attenzione a mettere la propria vita sui social, ad oggi il modo migliore per comunicare ai ladri di essere fuori casa. Perché su internet, come nei classici gialli, il colpevole è l'insospettabile più vicino. Basti pensare che il 70 per cento degli attacchi informatici viene da dipendenti infedeli».


Ci voleva un ragazzo inglese per fermare gli hacker globali