Furti, ricatti, minacce: i big dell'industria sabotati dagli hacker

S

November 10, 2020

Da marzo in Italia 26 colpi, l'ultimo ai danni di Campari: bloccata da dieci giorni. Ciardi, capo della Polizia Postale: «E' un salto di qualità»

Gabriele De Stefani **Pubblicato il** 10 Novembre 2020 **Ultima modifica** 10 Novembre 2020 *10:11*

Da dieci giorni ostaggio degli hacker. Campari è alle prese con un attacco di Ragnar Locker, uno dei gruppi di pirati informatici più organizzati della rete, che, dopo essere entrato nella rete aziendale e aver rubato una mole pesantissima di dati riservati, chiede un riscatto di 15 milioni di dollari per sbloccare l'attività del gruppo. Il lavoro di ripristino dei tecnici procede più lento del previsto, così le conseguenze iniziano a farsi pesanti: «Questa situazione può generare qualche impatto temporaneo sulla performance finanziaria del gruppo - dice l'azienda -. Il nostro impegno è garantire la continuità operativa nel modo più esteso possibile per le nostre attività, nonché quelle dei nostri clienti e controparti di business».

Quello di Campari è il ventiseiesimo caso pesante sul tavolo della Polizia postale dall'inizio della pandemia: nei guai sono finite 13 grandi industrie (tra cui Enel, Luxottica e Carraro, con blocchi della produzione durati giorni), sei enti istituzionali e sette società di servizi. Il trasloco rapido di gran parte delle attività sulla rete, spesso senza sistemi di sicurezza adeguati, ha attirato i pirati informatici. «C'è stato un netto salto di qualità degli hacker. Ora hanno competenze molto

sofisticate e puntano i grandi gruppi per portare a casa cifre importanti - spiega Nunzia Ciardi, capo della Polizia Postale -. Sono in grado di operare per mesi nelle reti aziendali senza lasciare traccia, finché non riescono a copiare tutti i dati e a bloccare l'operatività delle loro vittime. Fatture, pagamenti, segreti industriali, software che regolano la produzione: tutto viene rubato o sabotato. Nel migliore dei casi, e resta gravissimo, si crea solo un problema di privacy o danno d'immagine. Più spesso si arriva a impedire di lavorare».

Quando sullo schermo appare la richiesta di riscatto, dall'altra parte c'è una rete molto strutturata, con basi nell'Est Europa o in Estremo Oriente: «Gli hacker vengono reclutati nel deep web da vere organizzazioni criminali, non sono semplici pirati con buone capacità informatiche - continua Ciardi -. Se chiedono riscatti milionari, significa che sanno come riciclarli. Di certo non bisogna pagare. È come per i sequestri di persona: non è detto che poi le richieste si fermino. E i gruppi criminali non vanno finanziati».

Alla polizia però arriva solo una parte dei casi. La maggior parte, presa dall'ansia di sbloccare l'attività, non denuncia. E spesso paga. «Poche aziende hanno difese adeguate - spiega Mirko Gatto, capo della digital security di Var Group, 200 addetti nella consulenza sulla cyber sicurezza -. Noi studiamo i gruppi hacker nel deep web per capire quanto le loro minacce siano credibili. Si muovono benissimo, ad esempio iniziano subito a pubblicare frammenti dei documenti sottratti per scatenare il panico. Purtroppo l'attacco è spesso così efficace che risulta difficile non pagare. A quel punto si tratta: noi abbiamo assunto negoziatori professionisti, per condurre trattative nel deep web per minimizzare il danno. Spesso gli hacker finiscono per accontentarsi di cifre molto inferiori alle altissime richieste iniziali. Ma il danno è sempre molto pesante: per qualunque azienda è difficile spiegare ai clienti che dati e informazioni riservate sono stati violati».