Il Sole 24 ORE

30-MAR-2023
pagina 17 /
foglio 1

La battaglia contro gli hacker non si vince cedendo ai ricatti

Estorsione 2.0

Giovanni Paolo Accinni

È notizia dei giorni scorsi che la Ferrari è stata colpita da un attacco *hacker*: un attacco di tipo *ransomware*, ossia quello che si verifica sempre più frequentemente allorquando i criminali informatici accedono abusivamente alle reti informatiche bersaglio, ne criptano i dati rendendoli inservibili e (in taluni casi) li "esfiltrano" minacciandone la successiva divulgazione incontrollata. Per evitare i danni finanziari e reputazionali (talvolta di potenzialità letale) derivanti dalla pubblicazione di quanto illecitamente sottratto o per ottenere la chiave di cifratura dei dati criptati, i criminali informatici sono soliti domandare quindi un riscatto da corrispondersi in bitcoin o in altra valuta virtuale che garantisca l'anonimia della transazione. Sono estorsioni 2.0 la cui frequenza sta aumentando in maniera esponenziale e che lasciano talvolta attoniti, come quando la richiesta di riscatto viene formulata attraverso stampe di messaggi sinistri che appaiono all'improvviso dalle stampanti dell'ufficio; magari a distanza di giorni dall'attacco informatico. La risposta di Ferrari all'attacco è la sola consigliabile. Non è ammissibile (né utile) soddisfare gli estorsori: la sola cosa peggiore di praticare un ricatto si conferma essere il subirlo. Sottostare significherebbe perpetuare e ingigantire il fenomeno senza alcuna reale possibilità di evitare la pubblicazione di quanto trafugato o di ricevere le chiavi crittografiche per tornare a leggere i contenuti dei propri archivi. È l'esperienza empirica più recente a insegnarlo: il pagamento non frena i cybercriminali, né (tantomeno) li induce a decriptare i *file* o a non seguitare a minacciarne la pubblicazione illecita.
Quando solo utile è agire nella legalità con immediata efficacia. Denunciare subito l'attacco all'Autorità giudiziaria, avvalendosi di consulenti tecnici informatici che, monitorando massivamente i blog frequentati dai cybercriminali, riescano a comprendere l'origine soggettiva dell'attacco, a ottenere la chiave di decriptazione dei dati oppure a individuare in anticipo il *link* tramite cui gli *hacker* procederanno alla pubblicazione dei dati illecitamente esfiltrati. In questo caso, si dovrà poi depositare immediatamente un'istanza di sequestro preventivo (*recte*: di oscuramento) del *link* alla stessa Autorità inquirente. Si tratta senz'altro di una corsa a ostacoli, resa talvolta più difficile dal fatto che il *link* di pubblicazione venga diffuso tramite il cosiddetto *dark web*, che, non facendo capo ad alcun *internet service provider*, rende praticamente inattuabile qualunque ordine di oscuramento. È tuttavia chiaro che solo queste azioni valgano a tutelare la società bersaglio e la sua reputazione, i relativi *stakeholder* e – *a fortiori* – l'interesse collettivo. Sono tante battaglie di un'unica (costosa) guerra che si vince non cedendo al ricatto e alla paura.