Trenitalia è ancora alle prese con i danni dell’attacco informatico

A due settimane dall’attacco informatico che ha danneggiato i sistemi di Trenitalia, i problemi che hanno riguardato le biglietterie non sono stati risolti del tutto. In molte stazioni, soprattutto nelle città medio-piccole, la vendita nelle biglietterie non è stata ancora ripristinata e al momento i biglietti si possono acquistare attraverso i portali online o l’app di Trenitalia. Nelle principali stazioni, invece, la vendita in biglietteria è ripresa già da qualche giorno. I notevoli disservizi sono stati causati da un attacco compiuto contro il gruppo Ferrovie dello Stato, di cui fa parte Trenitalia, colpito mercoledì 23 marzo da un *cryptolocker*, un tipo di attacco informatico che prevede l’oscuramento di alcuni dati e successivamente la richiesta di un riscatto per rilasciarli.

Ferrovie dello Stato non è la prima grande azienda italiana colpita da un attacco di questo tipo: le aggressioni contro le aziende e la pubblica amministrazione sono sempre più frequenti, sempre più gravi, con conseguenze significative per moltissime persone.

Le prime segnalazioni di disservizi erano arrivate poco dopo le dieci di mercoledì 23 marzo. Il gruppo Ferrovie dello Stato era stato costretto a disattivare alcuni servizi informatici di Trenitalia e Rete ferroviaria italiana (Rfi) dopo aver scoperto l’attacco. Tra questi, il più importante era la rete di emissione dei biglietti, la cui disattivazione aveva causato la chiusura delle biglietterie, comprese quelle automatiche.

In un comunicato stampa diffuso nel pomeriggio, Ferrovie dello

Stato aveva detto di aver rilevato «elementi che potrebbero ricondurre a fenomeni legati a un'infezione da *cryptolocker*».

Un *cryptolocker* è un virus che appartiene alla famiglia dei *ransomware*, software che consentono di rubare dati e tenerli bloccati con l'obiettivo di chiedere un riscatto. Si può diffondere dall'esterno, caricato su uno dei computer che fanno parte della stessa rete, oppure attraverso il cosiddetto phishing via email: i criminali utilizzano un indirizzo email ingannevole (per esempio con un nome simile a quello di banche e servizi postali) per inviare una email a persone che lavorano nell'azienda da colpire. Nel testo dell'email c'è un link che se cliccato dà avvio all'installazione del *cryptolocker* nel sistema, bloccandolo. Il *cryptolocker* può impedire l'accesso al computer attraverso un'immagine a schermo intero o una pagina web da cui non si può uscire, in questo caso si definisce *lock screen*, oppure attraverso una crittografia che blocca i documenti presenti nel computer con una password, rendendoli inaccessibili.

Al momento non sono state diffuse molte informazioni tecniche sull'attacco: non si sa da dove sia entrato il virus, quali dati siano stati compromessi, se oltre alla chiusura delle biglietterie ci siano stati altri danni.

La procura di Roma ha aperto un'indagine. Del caso si sta occupando anche il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (Cnaipic) della Polizia postale. Già poco dopo l'attacco, però, è stato chiaro che il gruppo Ferrovie dello Stato non era stato aggredito con motivazioni politiche o legate alla guerra in Ucraina. «Qui c'è una matrice criminale come altrove», ha detto Roberto Baldoni, direttore dell'Agenzia nazionale per la cybersicurezza.

Il gruppo Ferrovie dello Stato si è affidato ai tecnici dell'Agenzia per la Cybersicurezza Nazionale, intervenuti poche ore dopo l'attacco insieme ai colleghi del reparto di

sicurezza informatica di Trenitalia per individuare le parti compromesse della rete e far ripartire i servizi.

La bonifica dei sistemi è un'operazione lunga e complessa perché consiste nel verificare la sicurezza di ogni singolo computer connesso alla rete delle biglietterie di Trenitalia. Nelle grandi stazioni il servizio è stato ripristinato in pochi giorni, così come la vendita attraverso le biglietterie self service, mentre nelle stazioni medio-piccole ci sono ancora problemi: gli sportelli sono operativi al 50 per cento.

(ANSA/DANIEL DAL ZENNARO)

È molto difficile capire quali siano le conseguenze economiche dell'attacco, principalmente perché non si sa quanti siano i ricavi di Trenitalia dai biglietti venduti agli sportelli: si tratta comunque di una percentuale piuttosto bassa sul totale delle vendite e la possibilità di acquistare il biglietto a bordo del treno senza sovrapprezzo ha comunque limitato le perdite. I disservizi più gravi, piuttosto, sembrano aver coinvolto le persone che dovevano gestire un abbonamento o

cambi di prenotazioni.

Il gruppo Ferrovie dello Stato ha detto di non aver ricevuto richieste di riscatto. Secondo molte ricostruzioni fatte da siti specializzati in sicurezza informatica, l'aggressione sarebbe stata compiuta dal gruppo di criminali chiamato Hive, che in passato aveva attaccato diverse aziende pubbliche e private tra cui MediaMarkt, un grande rivenditore di elettronica e elettrodomestici noto in Italia come Mediaworld. Nelle chat di negoziazione pubblicate da diversi siti, i criminali avrebbero chiesto un riscatto di 5 milioni di euro da pagare in Bitcoin.

Sempre nelle presunte chat di negoziazione di Hive, a cui dovrebbe poter accedere soltanto l'azienda aggredita, sono comparsi messaggi scritti da intrusi che erano riusciti a recuperare login e password. Secondo il sito *Redhotcyber*, le credenziali erano state diffuse in un gruppo Telegram italiano. A negoziazione ormai saltata, i criminali avrebbero alzato la richiesta di riscatto, da 5 a 10 milioni di euro in Bitcoin, ma fonti di Ferrovie dello Stato dicono che l'azienda non aveva ricevuto una richiesta di riscatto, né iniziato una trattativa con il gruppo Hive.

L'aggressione alle Ferrovie dello Stato, un gruppo enorme e – si suppone – con un elevato livello di protezione, è un caso piuttosto emblematico perché mostra la grande vulnerabilità delle aziende e i rischi legati a strategie criminali sempre più sofisticate.

Negli ultimi anni gli attacchi sono aumentati in quantità e qualità: secondo dati rilevati dal centro di sicurezza informatica (Security Operations Center) di Fastweb diffusi dal rapporto Clusit 2022, realizzato ogni anno dall'Associazione Italiana per la Sicurezza Informatica, nel 2021 in Italia sono stati segnalati 42 milioni di "eventi di sicurezza", in aumento del 16 per cento rispetto al 2020.

Fino al 2018 un attacco *ransomware* veniva lanciato prevalentemente via email, attraverso lo spam, e colpiva singole persone a cui veniva chiesto di pagare 500 euro in criptovalute per riavere accesso al computer. All'epoca il ritorno economico per i criminali era molto limitato.

«Dal 2018 iniziarono gli attacchi alle aziende, con risultati più efficaci e rapidi che contribuirono alla crescita del *ransomware*», dice Alberto Pelliccione, amministratore delegato di ReaQta, azienda che si occupa di sicurezza informatica. «I gruppi iniziarono a finanziare aggressioni sempre più complesse con i proventi degli attacchi. Di fatto, hanno reinvestito i proventi dei riscatti in strumenti e persone: oggi alcuni gruppi hanno la struttura delle grandi aziende. I compiti sono distribuiti e la filiera è molto articolata: c'è chi si occupa esclusivamente di scrivere il *ransomware*, chi compie materialmente l'attacco, chi gestisce i dati in attesa del riscatto una volta acquisiti».

Uno degli aspetti più preoccupanti è proprio la gravità degli attacchi, in forte crescita. Il ricorso ai *ransomware*, infatti, causa danni significativi a moltissime persone, come è accaduto con Trenitalia.

Il meccanismo estorsivo è piuttosto semplice: più i servizi sono pubblici ed essenziali, più è alta la necessità di ripristinarli nel più breve tempo possibile e più c'è la possibilità che le aziende aggredite acconsentano a pagare il riscatto. Non è un caso che tra le strutture più colpite ci siano aziende sanitarie, ospedali, centri diagnostici e ambulatori pubblici: custodiscono dati essenziali per curare le persone e non possono permettersi di bloccare i servizi per molto tempo.

— Leggi anche: Perché la sanità è così vulnerabile agli attacchi informatici

Contrastare questi crimini è complicato, per diversi motivi:

oltre alla maggiore preparazione dei criminali, le aziende e la pubblica amministrazione devono fare i conti con reti informatiche estese, quindi più vulnerabili, e soprattutto con l'impreparazione culturale dei dipendenti a cui raramente viene chiesto di applicare misure di sicurezza e accorgimenti minimi, per esempio nella gestione delle password. Nessuno può essere totalmente al sicuro.

«Magari tra 20 anni sarà possibile evitare qualsiasi tipo di attacco, oggi non è così», continua Pelliccione. «Il modo migliore per affrontare questa minaccia è prepararsi a una possibile aggressione, sviluppando sistemi per ridurre il più possibile i tempi di identificazione degli "attaccanti" e i tempi di mitigazione, cioè il ripristino dei servizi».

Read More