Corriere del Mezzogiorno - Campania - Giovedì 3 Settembre 2026

Cyber "cavallo di ritorno"Guerra ibrida alle imprese«Dietro gruppi terroristici» Contro le Pmiil 73% degli assalti Firewall affidabiliEcco le difese Se arriva anchel'utilizzo dell'AI

Nel mirino numerose aziende campane. Gli inquirenti: una nuova ondata

napoli «Mi hanno paralizzato l'azienda, non mi è restato altro che mettere temporaneamente tutti i dipendenti a riposo». È il racconto di un imprenditore napoletano, uno dei diversi titolari di aziende, tra capoluogo e provincia, finiti negli ultimi mesi nel mirino degli hacker. Un attacco informatico che ha bloccato l'intera attività e trasformato computer, archivi e server in una prigione digitale. Poi è arrivata la richiesta: soldi per far tornare tutto come prima.

Una sorta di «cyber-cavallo di ritorno»; verosimilmente un atto di guerra ibrida alle aziende. Prima l'intrusione, quindi il blocco dei sistemi o la sottrazione dei dati. Infine, il ricatto: pagare per riavere ciò che fino a quel momento apparteneva alla vittima. L'imprenditore ha scelto di denunciare tutto alla Polizia postale. Altri, spiegano gli investigatori, preferiscono pagare. Perché quando un'azienda è ferma, ogni ora produce un danno e quando ad essere minacciati sono dati sensibili, clienti e informazioni riservate, alla perdita economica si aggiunge quella d'immagine.

«Si tratterebbe di una nuova ondata», riferiscono gli inquirenti. Ma il fenomeno non è nuovo. Il ransomware è noto da almeno 15 anni. Nel tempo, però, le tecniche di intrusione si sono affinate e quello che era un attacco informatico è diventato per i criminali un vero modello di finanziamento. «È una tecnica estremamente diffusa e può essere utilizzata anche da gruppi terroristici», spiegano gli specialisti. Il ransomware è un programma malevolo che infetta un dispositivo, dal computer allo smartphone, e impedisce di accedere ai contenuti. Può cifrare i file, rendendoli illeggibili, oppure bloccare direttamente il dispositivo. Sullo schermo compare quindi la richiesta di riscatto, accompagnata da una scadenza: poche ore o pochi giorni per pagare, altrimenti i dati resteranno inaccessibili o saranno pubblicati.

Oggi, però, il ricatto può essere ancora più pesante. È la cosiddetta «doppia estorsione»: gli hacker non si limitano a bloccare i sistemi, ma prima copiano i dati e poi minacciano di diffonderli. Così un'azienda non rischia soltanto di restare senza computer; può vedere finire online documenti, informazioni sui clienti, progetti e materiale riservato. «Di solito davanti a ogni pagamento gli hacker alzano il tiro», spiegano gli investigatori. Non c'è infatti alcuna certezza che, dopo il versamento, arrivi la "chiave" per sbloccare i file. I dati potrebbero non essere restituiti, i sistemi potrebbero rimanere infetti oppure essere stati manipolati. E la vittima può diventare nuovamente un bersaglio, con una seconda richiesta di denaro.

C'è poi un'altra faccia della stessa truffa, a un livello più basso e molto più personale. Nel mirino finiscono anche persone che conservano sui propri dispositivi video o immagini intime, realizzati autonomamente o recuperati dalla Rete. Gli aggressori entrano in possesso del materiale e minacciano di divulgarlo a familiari, amici, colleghi o sui social se non viene pagato un riscatto. Come entrano i pirati? Spesso dalla porta più facile da aprire: una mail, un Sms, un messaggio che sembra provenire da una persona o da un'azienda conosciuta. Un corriere, una banca, un gestore telefonico, una pubblica amministrazione. Oppure un collega. Dentro c'è un allegato da aprire con urgenza oppure un link da cliccare per verificare una pratica. Basta quel gesto per consentire al malware di entrare nel dispositivo.

Altri attacchi passano attraverso siti web compromessi, banner pubblicitari o social network. Esistono poi tecniche più sofisticate che consentono di assumere il controllo dei sistemi da remoto. Nel mirino finiscono soprattutto enti, infrastrutture e aziende che custodiscono grandi quantità di dati. Non solo i colossi: anche una piccola impresa può diventare un obiettivo se possiede informazioni interessanti e dispone di sistemi di protezione vulnerabili. Le difese, spiegano gli esperti, partono da regole elementari: backup periodici, meglio se su supporti scollegati dalla rete; aggiornamenti costanti dei sistemi; antivirus e firewall affidabili; attenzione a link

e allegati inattesi. E soprattutto una regola: non pagare il riscatto. Le forze dell'ordine lo sconsigliano perché non esiste alcuna garanzia di recuperare i dati e perché il denaro può alimentare nuove attività criminali.

Gli ultimi casi italiani raccontano la dimensione del fenomeno. Ad agosto è stato colpito l'operatore che gestisce la modulistica scolastica e la piattaforma ClasseViva. Secondo le informazioni sull'attacco, sarebbero stati sottratti 6,1 terabyte di dati relativi a oltre 3.000 scuole, con la minaccia di pubblicarli sul dark web se non fosse stato pagato il riscatto. Ad aprile era toccato agli Uffizi. Gli hacker non avrebbero sottratto soltanto dati, ma anche informazioni considerate particolarmente delicate per la sicurezza del museo: codici di accesso, planimetrie e indicazioni sulla posizione delle telecamere e dei sensori. A febbraio, invece, il ransomware Bablock aveva colpito i sistemi della Sapienza di Roma. Le indagini si erano concentrate anche sulla gang filorussa Femwar02.

E ora c'è l'intelligenza artificiale. Gli strumenti a disposizione dei criminali stanno diventando più veloci e sofisticati. Jadepuffer è stato indicato come il primo ransomware gestito in maniera autonoma dall'AI, capace, secondo quanto riferito, di individuare e aggirare le difese aziendali in appena trenta secondi.

© RIPRODUZIONE RISERVATA