RANSOMWARE, ATTACCHI IN CRESCITA

di GIACOMO CORVI

AUMENTANO IN ITALIA LE IMPRESE VITTIMA DI INTRUSIONI INFORMATICHE: SERVIZI, MANIFATTURA E SANITÀ SI RIVELANO I SETTORI PIÙ COLPITI. TREND AL RIALZO ANCHE A LIVELLO GLOBALE. E A PAGARNE LE SPESE, SECONDO UN RECENTE REPORT DI SWASCAN, SONO SOPRATTUTTO LE SOCIETÀ DI MEDIE E PICCOLE DIMENSIONI

Hacker e criminali del web mettono nel mirino le piccole e medie imprese in Italia. Nel secondo trimestre del 2023, un totale di 35 aziende è rimasto vittima di un attacco ransomware. A pagarne le spese, come già accennato, sono state soprattutto le imprese di piccole e medie dimensioni: l'80% delle vittime conta al massimo 100 dipendenti e il 91% vanta un fatturato inferiore ai 250 milioni di euro. "Questo dato indica che i cybercriminali hanno indirizzato i loro attacchi principalmente verso le imprese più piccole, considerate più vulnerabili a questo tipo di minaccia a causa di risorse limitate e misure di sicurezza meno sviluppate", si legge nel rapporto stilato dal *security operation center* e dal team di *cyber threat intelligence* di **Swascan**, società di cyber security che nel 2020 è entrata a far parte del gruppo **Tinexta**.

Insomma, piccolo non è sempre bello quando si parla di sicurezza informatica. E le dimensioni, almeno a giudicare dai numeri del report, sembrano contare qualcosa quando si tratta di difendersi dalle incursioni di hacker e criminali del web: le imprese più grandi, quelle che possono contare più di mille dipendenti, non hanno subito alcun attacco ransomware nei tre mesi oggetto di analisi.

LE INDUSTRIE PIÙ VULNERABILI

Il settore dei servizi è quello che si è rivelato più vulnerabile a questo genere di attacco informatico: la maggioranza assoluta delle imprese colpite (54%) rientra proprio in questo comparto industriale. "La vasta gamma di aziende e organizzazioni presenti in questo settore offre agli aggressori un ampio campo di azione per cercare di ottenere vantaggi finanziari attraverso estorsioni", illustra il rapporto. Seguono poi il settore manifatturiero (11%) e quello dei servizi sanitari (9%), quest'ultimo con numeri praticamente raddoppiati nel giro di appena tre mesi. Più resilienti invece i comparti della finanza (3%), delle costruzioni (3%), dei trasporti (6%) e dei servizi finanziari (6%).

Complessivamente, il report arriva a contare in Italia circa 190mila dispositivi compromessi e registra una crescita del 34,6% nel numero di attacchi informatici rispetto ai tre mesi precedenti. L'organizzazione criminale più attiva in Italia è stata *Monti*, capace di mettere la propria firma sul 26% degli attacchi avvenuti nel nostro paese nel secondo trimestre dell'anno. Seguono quindi *LockBit3* (20%) e poi, molto più distanziata, la gang *Darkrace* (8%).

UNA MINACCIA GLOBALE

Il fenomeno, com'è noto, non riguarda tuttavia soltanto l'Italia. E assume giorno dopo giorno una portata sempre più globale: il rapporto, a tal proposito, evidenzia che nel trimestre considerato il numero di paesi colpiti da almeno un attacco ransomware si è attestato a quota 89, dieci in più rispetto ai tre mesi precedenti. Gli Stati Uniti si confermano la vittima principale di questo genere di attacco informatico, con 636 imprese colpite da episodi di ransomware. Alle sue spalle, a debita distanza, si piazzano invece Regno Unito (69), Canada (60), Germania (54), Francia (39), Brasile (38) e, come detto, Italia (35).

Complessivamente il rapporto arriva a contare 1.451 vittime, dato che registra un aumento del 62% sul trimestre precedente e del 105% su base annua. Il mese di maggio si è rivelato essere quello più prolifico per hacker e criminali del web: il numero di attacchi ransomware si è attestato a quota 575, in rialzo del 51% sul mese precedente e del 228% rispetto all'inizio dell'anno.

NESSUNO È IMMUNE

Il comparto dei servizi si conferma quello più vulnerabile anche a livello globale, con quasi la metà degli attacchi (47%) che ha riguardato questo specifico settore produttivo. Alle sue spalle, come avvenuto anche in Italia, si piazza l'industria manifatturiera (16%), mentre al terzo posto si colloca il comparto tecnologico (6%). "Il settore tecnologico, nonostante sia tradizionalmente più attento alla sicurezza informatica, ha registrato diverse aziende vittime di ransomware nel periodo considerato", si legge nel report. "Questo – prosegue il rapporto curato da Swascan – evidenzia la sofisticazione e la persistenza degli attacchi, che sono riusciti a superare le difese anche delle aziende considerate ipoteticamente più tecnologicamente avanzate".

Seguono quindi il settore sanitario (4%), il commercio al dettaglio (4%) e poi, a seguire, finanza (3%), costruzioni (3%) ed educazione. "Questi dati – rimarcano i curatori del report – dimostrano che nessun settore è immune dagli attacchi ransomware e sottolineano l'importanza di adottare misure di sicurezza per proteggere i dati aziendali e mitigare gli effetti negativi degli attacchi informatici".

© Zephyr18 - iStock

NUOVE STRATEGIE DI DIFESA

Quasi otto milioni di dispositivi informatici sono stati compromessi nel secondo trimestre del 2023 a livello globale, offrendo ad hacker e criminali di web la possibilità di esfiltrare informazioni personali, come chiavi di accesso a wallet di criptovalute e portali di home banking, che possono poi essere vendute illegalmente sui mercati del *deep web* e del *dark web*.

Il fenomeno del phishing emerge infine come una delle minacce sempre più diffuse, con quasi 160mila campagne che, almeno in Italia, hanno interessato principalmente il settore bancario e finanziario. "La convergenza tra diverse tipologie di minacce è una dimostrazione della complessità e dell'adattabilità del panorama degli attacchi: fenomeni come phishing, ransomware e malware stanno seguendo una curva di crescita che supera le spiegazioni legate a fenomeni casuali", ha commentato **Pierguido Iezzi**, cyber security director e ceo di Swascan. "Questa tendenza sottolinea l'urgenza di adottare strategie di difesa avanzate nell'era digitale per proteggere il patrimonio, l'economia e i cittadini. Ora più che mai – ha concluso Iezzi – è imperativo garantire la sicurezza della rete per salvaguardare aspetti che ci riguardano da vicino, come il prestigio del *Made in Italy*, oltre che proteggere le persone da minacce dirette e indirette".