ALLARME HACKER UN'ORA PER REAGIRE

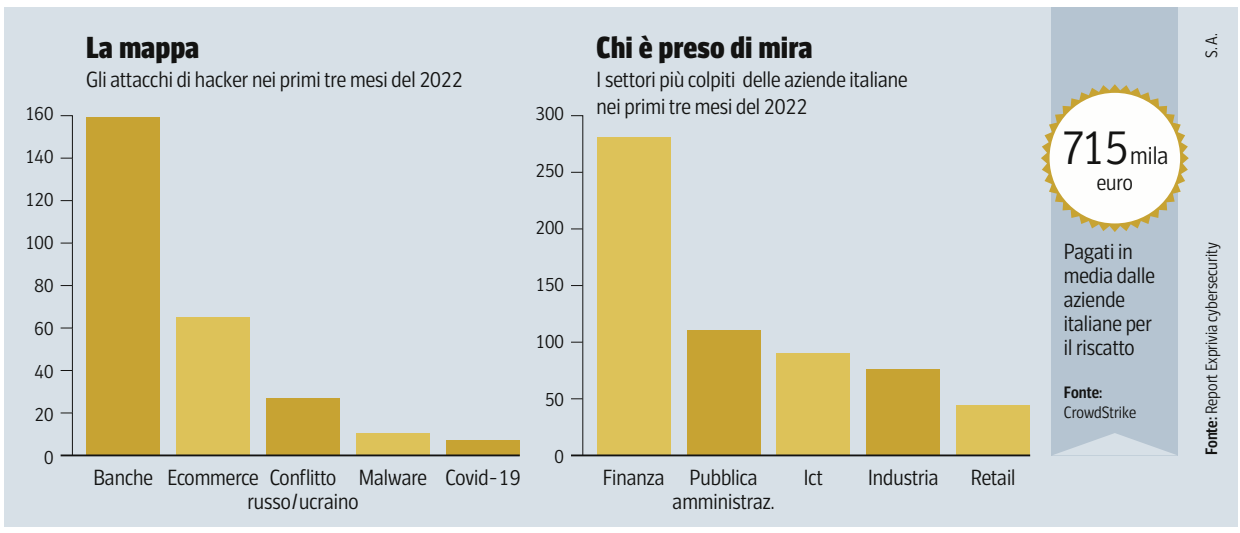
Gli attacchi informatici alle aziende in Italia si sono impennati nel primo trimestre rispetto alla fine del 2021

Il virus più diffuso è quello che ruba i dati per avere un riscatto. Fondamentale la risposta rapida per limitare i danni

di **Umberto Torelli**

Nel primo trimestre di quest'anno la coda della pandemia e il conflitto russo-ucraino hanno tatto balzare in avanti gli attacchi informatici. In particolare i ransomware, quelli con richiesta di riscatto. Settore finanziario, pubblica amministrazione e servizi digitali sono stati i settori i più colpiti. È quanto emerge dall'ultimo report sulle minacce informatiche dell'Osservatorio cybersecurity di Exprivia, azienda pugliese di sicurezza informatica. Tra gennaio e marzo, dice l'indagine, in Italia si sono registrati almeno 806 attacchi hacker, il 78% in più rispetto agli ultimi tre mesi del 2021.

L'azienda italiana, che impiega 2.400 esperti in sette Paesi del mondo, ha preso in esame i siti di 113 imprese e istituzioni pubbliche nazionali. «Negli ultimi due anni gli eventi ad alto impatto politico ed economico, con le relative tensioni sociali, hanno consentito ai criminali di ingannare le vittime, sfruttando il Covid e il recente conflitto tra Russia e Ucraina — dice Domenico Raguseo, direttore cybersecurity di Exprivia — . Nella maggiore parte dei casi, attacchi gravi e a scopo di lucro». Tra i casi, Trenitalia che il 23 marzo è stata colpita alle biglietterie fisiche e self service; il ministero della Transizione ecologica i cui servizi sono il primo aprile andati in blackout; e l'ospedale Fatebenefratelli Sacco di Milano, che il primo maggio ha dovuto chiudere i sistemi contabili.



Gli obiettivi

Secondo l'Osservatorio, nel primo trimestre il settore Finanza — dagli istituti bancari alle assicurazioni fino alle piattaforme per le criptovalute — ha registrato il maggior numero di cyberattacchi. In tutto 286, con un picco di 161 casi solo nel mese di marzo, tra furti di dati e carte di credito, accesso ai conti bancari e richieste di denaro. Segue la pubblica amministrazione con 109 casi tra attacchi, incidenti e violazioni della privacy: è più del triplo rispetto all'ultimo trimestre del 2021.

Al terzo posto, con 91 casi, il settore hardware e software delle aziende Ict. Inclusi servizi digitali, piattaforme di ecommerce, dispositivi e sistemi operativi. Qui a farla da padrone secondo gli esperti Exprivia sono la cattura delle credenziali di accesso a informazioni sensibili. Incluse quelle mediche. Tra le tecniche messe in atto troviamo il phishing, con modalità di adescamento tramite email ingannevoli e social network. Parliamo di 389 casi, in aumento dell'80% rispetto a tre mesi precedenti. Ma i principali attacchi hacker restano legati al ransomware: questo emerge dal report di CrowdStrike, società texana che ha intervistato 2.200 responsabili della sicurezza nel mondo, inclusa l'Italia.

Vi si legge un dato sconcertante: il 96% delle aziende colpite, dopo avere pagato un primo riscatto per poter accedere ai propri dati rubati, ha deciso di pagarne un secondo, per evitare che dati e informazioni venissero resi pubblici e venduti. Il calcolo è che per l'Italia il valore medio pagato dalle aziende per riscattare i dati rubati con il ransomware sia di 751 mila euro ciascuna. Ecco perché è essenziale la tempestività. Ogni minuto perso può costare decine di migliaia di euro.

CrowdStrike consiglia di adottare le formula uno-dieci-sessanta. Spiega Luca Nilo Livrieri, direttore tecnico Sud Europa: «Per essere efficaci bisogna rilevare la minaccia durante il primo minuto dall'intrusione, analizzarla nell'arco di dieci minuti e neutralizzarla entro un'ora». Oggi occorrono in media oltre cento ore.

L'ultimo report di Verizon, dei giorni scorsi, ha stimato un incremento del 13% degli attacchi ransomware nell'ultimo anno. Sono sotto attacco anche le strutture industriali. «Gli hacker trovano meno redditizio violare i sistemi di telefonia e i servizi digitali — dice Alessio Aceti, ceo di Sababa Security, azienda di cybersecurity — così stanno rivolgendo l'attenzione ai grandi complessi produttivi». Lo dimostra il massiccio attacco del 2021 alle linee di trasporto del petrolio Usa della Colonial Pipeline. E al sistema idrico Oldsmar in Florida, colpito con la minaccia d'inquinare le riserve d'acqua.

Ma già i pirati informatici pensano allo spazio. Siamo entrati nell'era del «crime as a service», un mercato globale dove i cyberattacchi si ordinano nel dark web con pagamento in criptovalute. Secondo i laboratori californiani Fortinet, le nuove minacce nel corso del 2022 prenderanno di mira le organizzazioni che usano i satelliti per supportare il business presso i clienti. Parliamo ad esempio dei giochi online, ma anche della fornitura dei servizi digitali a sedi remote, delle crociere e delle compagnie aeree.

@utorelli

Il 96% delle aziende colpite dal ransomware ha pagato una seconda volta, per evitare che i file rubati fossero resi pubblici o venduti

Glossario

I pericoli dalla A alla W

I virus informatici appartengono alla categoria dei malware, i programmi maligni creati dagli hacker. In genere contengono codici binari, che vengono introdotti nel computer o nel cellulare all'insaputa dell'utente. Saturano la memoria del dispositivo, rubano dati e informazioni personali. Per combatterli è buona norma installare uno dei tanti antivirus in commercio. Ma come per i virus fisici, non è certo che il vaccino li debelli sempre, perché ogni giorno escono nuove varianti. Ecco i programmi più diffusi.

Adware Veicolano messaggi pubblicitari in grande quantità. Presi singolarmente sono innocui, ma a lungo termine e messi assieme bloccano la memoria e le risorse del Pc.

DDoS Tra i malware di ultima generazione sono i più pericolosi. Gli hacker indirizzano attacchi di più computer verso uno stesso server, con lo scopo di mandarlo in tilt.

Ransomware Sono virus diffusi via email che catturano file e dati, da restituire dietro pagamento di un riscatto.

Spyware Sono programmi spia che rubano dati d'accesso senza che l'utente si accorga. Informazioni personali, mediche e bancarie rivendute sul web.

Trojan S'insediano invisibili nei programmi dell'utente, per scatenare attacchi malware successivamente.

Worm Sono i «vermi» informatici, si replicano da soli in memoria. Contengono codici maligni, capaci di propagarsi verso altri computer via Internet.

U. Tor.