COMUNICATO STAMPA

CYBERSECURITY: DIMINUISCONO I FENOMENI DI CYBERCRIME IN ITALIA MA PEGGIORA LA SICUREZZA DEI DISPOSITIVI MEDICALI

- *Secondo l'ultimo rapporto dell'Osservatorio Cybersecurity di Exprivia "Threat Intelligence" nel primo trimestre 2024 gli attacchi informatici sono diminuiti dell'11% rispetto alla fine dello scorso anno, ma risultano in aumento di oltre il 50% nello stesso periodo di riferimento (1Q) nel 2022 e nel 2023, rivelando una preoccupante escalation delle minacce*
- *Preoccupa il livello di sicurezza di dispositivi medicali connessi come apparecchi per radiografie, risonanze e microscopi, oltre a dispositivi indossabili per la telemedicina*
- *Nonostante il calo generale, il settore finanziario resta il più colpito (-16%). Frenano anche gli attacchi ai danni della Pubblica Amministrazione (-29%) e del Retail (-30%), mentre il settore ICT (+53%) e le infrastrutture critiche (+54%) vedono un aumento significativo*
- *Il furto dei dati torna al primo posto tra i danni causati dagli hacker*

Molfetta, 10 luglio 2024 – Nei primi mesi del 2024 si è registrata una complessiva diminuzione delle minacce informatiche rispetto al trimestre precedente, mentre i dispositivi connessi in rete sono aumentati e sono risultati poco protetti, in particolare quelli utilizzati in ambito medico.

È il quadro che emerge dal nuovo ***"Threat Intelligence Report"*** elaborato dall'Osservatorio Cybersecurity di **Exprivia**, che ha preso in considerazione 159 fonti aperte tra siti di aziende colpite, siti pubblici di interesse nazionale, agenzie di stampa online, blog e social media.

In particolare, secondo il rapporto stilato dal gruppo ICT pugliese, tra gennaio e marzo i fenomeni di cybercrime sono diminuiti dell'11%, con 559 casi rispetto ai 626 dell'ultimo trimestre del 2023. Il mese di febbraio ha registrato quasi la metà dei casi totali (230). Tuttavia, rispetto allo stesso periodo del 2023, gli attacchi informatici sono aumentati del 128%, mentre gli incidenti (attacchi andati a buon fine) sono calati del 7% e le violazioni della privacy sono aumentate del 117%. Nello specifico, nei primi tre mesi del 2024, si sono verificati 437 attacchi, 96 incidenti e 26 violazioni della privacy.

Aumentano i dispositivi IoT, preoccupa la sicurezza dei dispositivi medici intelligenti

Il rapporto evidenzia inoltre che il numero di dispositivi IoT connessi in rete in Italia è aumentato del 3% rispetto all'ultimo trimestre del 2023, raggiungendo quasi otto milioni di device. Tuttavia, la sicurezza dei dispositivi medicali intelligenti, come apparecchiature per radiografie e risonanze, microscopi e dispositivi cardiologici per la telemedicina indossabili e connessi, è peggiorata. Al contrario, il livello di sicurezza dei servizi esposti in rete è migliorato nel trimestre analizzato, un dato positivo che rende più difficile per gli attaccanti comprometterne la reperibilità o la disponibilità, evitando così inefficienze nei sistemi.

Il settore finanziario rimane il più colpito, aumenti preoccupanti per ICT e Infrastrutture Critiche, migliora la PA

Nel periodo analizzato, il settore finanziario è stato il più colpito dagli attacchi informatici, con 236 casi, sebbene in calo del 16% rispetto all'ultimo trimestre del 2023 (281 casi). Il settore Software/Hardware ha registrato un incremento del 53%, passando da 66 a 101 attacchi, posizionandosi al secondo posto tra i settori più bersagliati. La Pubblica Amministrazione ha visto un calo del 29%, con 69 casi rispetto ai 97 del periodo

ottobre-dicembre dello scorso anno. Il settore Retail ha registrato 57 attacchi, in diminuzione rispetto agli 81 del trimestre precedente (-30%). Le Infrastrutture Critiche, invece, hanno visto un aumento degli attacchi, passando da 13 a 20 casi (+54%).

Categorie di danno: il furto dei dati è in testa, seguono le richieste di riscatto e le interruzioni di servizio

Il furto di dati sensibili si riconferma al primo posto tra le principali tipologie di danni causati dagli hacker, rappresentando circa il 56% dei casi totali (311 su 559), sebbene in calo del 14% rispetto alla rilevazione precedente (363 casi). Al secondo posto si trova il pagamento di un riscatto (cd. ransomware), che rappresenta circa il 27% dei casi totali, con una tendenza positiva evidenziata da una flessione del 30% rispetto al trimestre precedente. La terza categoria di danno più comune è stata l'interruzione di servizio, ovvero l'arresto del normale funzionamento della rete, di un'applicazione o di un servizio software, che rappresenta oltre il 7% dei casi.

Calano phishing e malware, crescono Hacktivism e le violazioni della privacy

Primeggia il **phishing/social engineering**, ovvero l'adescamento in rete o via mail di utenti distratti o poco consapevoli, che ha subito una riduzione di quasi il 9% rispetto al trimestre precedente (233 fenomeni rispetto a 255), Calano anche gli attacchi tramite **malware**, al secondo posto con 214 casi rispetto ai 252 di quelli registrati tra ottobre e dicembre 2023. Il **cybercrime** si conferma la principale minaccia per la sicurezza in rete in Italia, con oltre l'80% dei casi (484) rispetto al totale dei fenomeni. A notevole distanza l'**hacktivism** (attività criminali al fine di promuovere una causa politica o sociale) con circa il 7% (37 casi), e il **privacy breacher** (violazioni di sicurezza che comportano distruzione, perdita, modifica, accesso o divulgazione non autorizzata dei dati personali) che segna il 5% degli eventi rilevati.

"Il numero di attacchi e incidenti è sostanzialmente costante dagli ultimi mesi del 2023 e sembra non risentire della contingenza sociale ed economica, così la motivazione principale degli attaccanti resta sempre focalizzata sul furto dei dati e di denaro - **commenta Domenico Raguseo, direttore Cybersecurity di Exprivia** - *È importante osservare il quadro complessivo dell'andamento tra il vecchio e il nuovo anno e non solo, con la preoccupante crescita - del 50% circa - dei fenomeni complessivi, se paragoniamo l'ultimo trimestre dello scorso anno e i primi tre mesi del 2024 con lo stesso periodo tra fine 2022 e inizio 2023".*

Exprivia

Il Gruppo Exprivia, specializzato in Information and Communication Technology, è tra i principali protagonisti della trasformazione digitale. Forte di un bagaglio di competenze maturate in oltre 30 anni di presenza costante sul mercato nazionale e internazionale, Exprivia impiega circa 2.400 persone in sei Paesi nel mondo avvalendosi di un team di esperti in diversi ambiti della tecnologia e della digitalizzazione: dall'Intelligenza Artificiale alla Cybersecurity, dai Big Data, al Cloud, dall'IoT al BPO, dal Mobile al Networking e alla Collaboration, presidiando interamente il mondo SAP. Quotata in Borsa Italiana dal 2000 nel mercato Euronext (XPR), Exprivia supporta i propri clienti nei settori Banking, Finance&Insurance, Aerospace&Defence, Energy&Utilities, Healthcare e Public Sector, Manufacturing&Distribution, Telco&Media. La capacità progettuale del gruppo è arricchita da una solida rete di partner, soluzioni proprietarie, servizi di design, ingegneria e consulenza personalizzata. La società è soggetta alla direzione e coordinamento di Abaco Innovazione S.p.A.
Maggiori informazioni al sito www.exprivia.com

COMUNICATO STAMPA

Contatti

Exprivia SpA
Luca Vittorio Mario Ferraris
marketing.exprivia@exprivia.com
T. + 39 0803382070
F. +39 0803382077

SEC Newgate – Ufficio Stampa Exprivia
Martina Trecca
martina.trecca@secnewgate.it
M: +39 334 1019671

Alessio Costa
alessio.costa@secnewgate.it
M: +39 340 3442329

Teresa Marmo
teresa.marmo@secnewgate.it
M: +39 335 6718211