COMUNICATO STAMPA

CYBERSECURITY: REPORT ANNUALE DI EXPRIVIA NEL 2023 ONDATA DI ATTACCHI INFORMATICI IN ITALIA

L'Osservatorio Cybersecurity di Exprivia nel 2023 registra 2.209 fenomeni legati al cybercrime. Gli hacker continuano a perfezionare le loro tattiche, causando incidenti informatici sempre più gravi e dannosi. Diminuiscono dell'8% i dispositivi IoT esposti in rete, ma il Sud Italia presenta ancora un rischio elevato rispetto al Centro-Nord.

07/03/2024 – Nuovo incremento degli attacchi informatici a scapito di aziende, organizzazioni e persone nel 2023 in Italia, con il settore finanziario che risulta tra i principali bersagli e la Pubblica Amministrazione sempre più colpita nel corso dell'anno. È quanto emerge dal nuovo **'Threat Intelligence Report'** **elaborato dall'Osservatorio Cybersecurity** di **Exprivia**, che prende in considerazione 145 fonti aperte tra siti di aziende colpite, siti pubblici di interesse nazionale, agenzie di stampa online, blog e social media.

Secondo il rapporto stilato dal gruppo ICT, lo scorso anno ha totalizzato **2.209** casi tra **attacchi, incidenti e violazioni della privacy**. Nello specifico, si sono verificati **1.635 attacchi** (+32% rispetto ai 1.236 del 2022), **518 incidenti** – **più che dimezzati** (-59%) **rispetto al 2022** quando gli incidenti di sicurezza erano stati 1.236 - e **56 violazioni della privacy** (-46% rispetto ai 103 fenomeni dell'anno precedente).

"Nel contesto della guerra informatica, valutare i danni con precisione è un processo simile a quello che riguarda le guerre convenzionali, possibile generalmente solo dopo la cessazione del conflitto – **commenta Domenico Raguseo, direttore Cybersecurity di Exprivia.** *Nel cybercrime non sempre un attacco si traduce immediatamente in un incidente, che può essere anche il risultato di un'azione avviata mesi prima. Il forte aumento degli attacchi in Italia si è verificato in modo particolare nel secondo trimestre del 2023, mentre gli incidenti, complessivamente più che dimezzati, mostrano comunque una curva in ascesa nel corso dell'anno. Nel 2023* – **prosegue Raguseo**, *è emersa anche l'importanza della sicurezza dell'intera catena di servizio. La digitalizzazione è così pervasiva che è irrealistico pensare che la sicurezza di un individuo possa essere indipendente da quella di tutti gli elementi che contribuiscono a fornire o utilizzare un servizio. La consapevolezza, sia a livello individuale sia organizzativo, e la valutazione del rischio della catena di approvvigionamento, diventano quindi elementi imprescindibili".*

Da quanto emerge nel nuovo report di Exprivia il settore maggiormente preso di mira dagli attaccanti risulta essere **'Finance'**, che include aziende finanziarie, istituti bancari o piattaforme di criptovalute, con **969 casi** e picchi di rilevanza nel corso del 2023, rappresentando il 44% del totale dei fenomeni (in lieve aumento del 3% rispetto al 2022 quando si erano registrati 939 casi). Al secondo posto il comparto **'Software/Hardware'** (società ICT, di servizi digitali, piattaforme di e-commerce, dispositivi e sistemi operativi), maggiormente colpito nel primo periodo del 2023 e che totalizza **380** casi (circa l'11% dei casi in più rispetto all'anno precedente). In terza posizione, con **335 fenomeni**, il settore della **'Pubblica Amministrazione'** mostra variazioni nell'andamento annuale, crescendo in particolare nei mesi di marzo e dicembre. Chiude la classifica il settore **'Retail'** (attività commerciali che forniscono beni e servizi direttamente ai consumatori, sia tramite negozi fisici che online), passando da 172 casi nel 2022 a **183** nel 2023 e confermandosi tra i settori più vulnerabili.

Nel 2023, sui 2.209 casi registrati, il **furto di dati** continua a prevalere come nel 2022, rappresentando il **59%** del totale. Il furto dei dati consiste nell'archiviazione o nel trasferimento illegale di informazioni personali, finanziarie o proprietarie come password, codici software, algoritmi e processi causando gravi conseguenze per le persone o le organizzazioni colpite. A seguire, la richiesta di **denaro**, con il **29%** dei fenomeni, e **l'interruzione di servizio** (l'arresto del normale funzionamento della rete, di un'applicazione o di un servizio software) **che rappresenta l'11%** dei fenomeni complessivi.

È sempre il **phishing/social engineering**, ovvero l'adescamento in rete o via mail di utenti distratti o poco consapevoli, la principale tipologia di attacco del 2023, con il **49% dei casi totali** (1.088, in calo del 4% circa rispetto ai 1.133 dell'anno precedente). Questa tecnica è utilizzata soprattutto nella fase di ricognizione per ottenere informazioni su un sistema, rete o organizzazione, e di accesso iniziale, quando gli attaccanti cercano di entrare nella rete o nel sistema bersaglio per adescare le vittime. Seguono gli attacchi tramite **malware** (software dannosi che compromettono o interrompono l'utilizzo di dispositivi) con **749 casi**, ovvero il **34% del totale**. In particolare, il malware RAT (Remote Access Trojan) segna 239 casi ed è la tipologia di malware più diffusa: il RAT presenta elevate capacità di evadere gli strumenti di rilevamento e, prendendo il controllo del sistema, può eseguire, ad esempio, attacchi Distributed Denial of Service (DDoS), volti a sovraccaricare o rendere inaccessibile un servizio, un sito web o una rete, oppure a rubare informazioni riservate.

Gli esperti dell'Osservatorio Cybersecurity di Exprivia hanno rilevato che il **cybercrime** si conferma la principale minaccia per la sicurezza in rete in Italia nel 2023, con oltre il **90%** dei fenomeni (2.015). A notevole distanza l'**hacktivism** (attività criminali al fine di promuovere una causa politica o sociale)

con circa il **5%** dei casi (122), mentre il **data breach** (violazioni di sicurezza che comportano distruzione, perdita, modifica, accesso o divulgazione non autorizzata dei dati personali) riguarda il **3%** degli eventi rilevati (66).

Rispetto al 2022, nel 2023 si è registrata una **diminuzione dell'8% dei dispositivi IoT esposti in rete**. Questo dato, emerso da uno studio condotto dall'Osservatorio Cybersecurity di Exprivia su scala nazionale, indica un progresso significativo nella sicurezza delle infrastrutture digitali nel paese. Un aspetto rilevante dell'analisi è l'identificazione delle aree geografiche in cui i dispositivi risultano più a rischio, con particolare attenzione al **Sud Italia**, dove i **dispositivi IoT** si sono dimostrati essere **maggiormente esposti rispetto al Centro-Nord**. Parallelamente, l'Investment Index (II), che valuta il livello di investimenti in diversi settori economici, si è mantenuto generalmente costante durante l'anno. Tuttavia, si rileva un lieve miglioramento nel settore Retail, indicando una maggiore fiducia in questo specifico ambito.

COMUNICATO STAMPA

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.

www.exprivia.com

Contatti

Donato Dalbis
donato.dalbis@exprivia.com
T. + 39 0803382070 - F. +39 0803382077

Press office

Sec and Partners
T. +39 06/3222712
Martina Trecca
martina.trecca@secnewgate.it - Cell. +39 334/1019671
Andrea Lijoi
andrea.lijoi@secnewgate.it - Cell. +39 329/2605000