COMUNICATO STAMPA

CYBERSECURITY: RECORD ASSOLUTO DI ATTACCHI TRA APRILE E GIUGNO
LA PA MIGLIORA IN SICUREZZA INFORMATICA

Il report trimestrale di Exprivia registra quasi il doppio dei fenomeni di cybercrime rispetto ai primi mesi dell'anno. Il settore Finance tra i più colpiti dagli hacker. Trend inverso per la PA, frutto di investimenti in politiche di protezione. A rischio di attacchi l'industria dell'Intrattenimento.

26 luglio 2023 – Record assoluto di attacchi nel secondo trimestre dell'anno in Italia, con una sostanziale ripresa della sicurezza nel settore della Pubblica Amministrazione che migliora i suoi sistemi di difesa dagli hacker. È quanto emerge dal nuovo **'Threat Intelligence Report' elaborato dall'Osservatorio Cybersecurity** di **Exprivia** che prende in considerazione 129 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 pugliese, tra aprile e giugno si registra un **aumento costante dei fenomeni di cybercrime**, con **672** casi complessivi, quasi il doppio rispetto ai **308** del trimestre precedente. Nello specifico, si sono verificati **569 attacchi** (+196% rispetto ai 192 del trimestre precedente) **- un numero mai raggiunto da quando l'Osservatorio Cybersecurity di Exprivia ha avviato per la prima volta l'analisi dei dati (gennaio 2020) -, 82 incidenti** - ovvero attacchi andati a buon fine - in calo del 21% rispetto ai 104 precedenti, e **21 violazioni della privacy** (+75% rispetto alle 12 dello scorso trimestre).

"Siamo di fronte a uno scenario di crescita costante dei fenomeni di cybercrime, anche se a fronte di un record di attacchi, rileviamo un valore minimo di incidenti, ossia attacchi andati a buon fine **- commenta Domenico Raguseo, direttore Cybersecurity di Exprivia.** *Una lettura ottimista potrebbe suggerire una maggiore efficacia dei sistemi di difesa, così come dimostrano i dati nel settore della Pubblica Amministrazione. Non è da escludere, però, che gli incidenti si possano registrare nei prossimi due mesi, così come evidenziato da dinamiche passate. Pertanto, è necessario attendere l'autunno per avere certezza di quanto gli hacker siano riusciti a portare a segno i loro colpi".*

Per gli esperti dell'Osservatorio Cybersecurity di Exprivia, impegnata nel promuovere la cultura sulla sicurezza informatica anche attraverso corsi di formazione, il settore maggiormente preso di mira dagli attaccanti nel secondo trimestre torna a essere quello **'Finance'** (aziende finanziarie, istituti bancari o piattaforme di criptovalute), con il **56% dei casi** (**377**) e un raddoppio da aprile a giugno.

Al secondo posto il comparto **'Software/Hardware'** (società ICT, di servizi digitali, piattaforme di e-commerce, dispositivi e sistemi operativi) che passa da 99 fenomeni del primo trimestre a **105**. Al terzo posto il **'Retail'**, ovvero quel mercato che comprende le attività di vendita da parte di un'azienda al consumatore finale, che dai 14 casi registrati nei primi tre mesi dell'anno ne segna **40** tra aprile e giugno. Il settore della **'Pubblica Amministrazione'** scende invece **da 89 a 65 casi**, per effetto di investimenti in politiche di protezione dei dati e frutto di una maggiore consapevolezza sulla sicurezza informatica negli enti pubblici. Chiude la classifica il settore **'Industria'** con 19 fenomeni.

Mantiene il primato tra le principali tipologie di danni causati dagli hacker il **furto dei dati** con il **63% dei casi totali** (423), in leggera flessione rispetto al 65% del trimestre precedente. 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. Al secondo posto, la richiesta di **denaro**, con un **incremento percentuale di circa il 362%** rispetto al trimestre precedente. A seguire, l'**interruzione di servizio** (l'arresto del normale funzionamento della rete, di un'applicazione o di un servizio software) con il **5% dei casi**, in netto calo rispetto al 15% del trimestre precedente; mentre la **violazione della privacy**, ossia la divulgazione di dati da parte di soggetti terzi senza il consenso dell'interessato, si attesta al **4%**.

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, con il **60% dei casi totali** (406 fenomeni rispetto ai 145 del trimestre precedente e **un incremento del 180%**); aumentano anche gli attacchi tramite **malware** (software dannosi che compromettono o interrompono l'utilizzo di dispositivi), al secondo posto con **173 casi** rispetto agli 104 registrati tra gennaio e marzo 2023. In particolare, si registra un aumento esponenziale dei malware RAT (Remote Access Trojan), che hanno elevate capacità di evadere gli strumenti di rilevamento e, prendendo il controllo del sistema, possono eseguire, ad esempio, attacchi DDoS o rubare informazioni riservate.
Secondo il rapporto di Exprivia, il **cybercrime** si conferma la principale minaccia per la sicurezza in rete in Italia, con **617** fenomeni e un rialzo del 142% rispetto al trimestre precedente. A notevole distanza il **data breach** (violazioni di sicurezza che comportano distruzione, perdita, modifica, accesso o divulgazione non autorizzata dei dati personali) con 28 casi e l'**hacktivism** (attività criminali al fine di promuovere una causa politica o sociale) che ne riporta 22.

Il numero dei **dispositivi IoT connessi in rete (circa otto milioni)** subisce una lieve diminuzione (-2%) e, secondo gli indici di valutazione elaborati dall'Osservatorio di Exprivia, a maggior rischio

sicurezza sono le telecamere, mentre il settore più esposto ad attacchi - quindi dove si registrano meno investimenti in ambito cybersecurity - è quello dell'Entertainment (Industria del cinema, tv, sport, parchi tematici, ecc). Un dato che potrebbe essere fortemente influenzato dalla velocità con cui le aziende di questo ambito affrontano il progresso tecnologico e che non sempre va di pari passo con la protezione delle nuove soluzioni introdotte.

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

Exprivia SpA

Investor Relations
Gianni Sebastiano
gianni.sebastiano@exprivia.it
T. + 39 0803382070 - F. +39 0803382077

Ufficio Stampa

Sec Mediterranea
T. +39 080/5289670
Teresa Marmo
teresa.marmo@secnewgate.it - Cell. +39 335/6718211
Gianluigi Conese
gianluigi.conese@secnewgate.it - Cell. +39 335/7846403

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