COMUNICATO STAMPA

NUOVO REPORT CYBERSECURITY DI EXPRIVIA: PAUSA ESTIVA PER IL CYBERCRIME, TRA LUGLIO E SETTEMBRE CALANO LE MINACCE INFORMATICHE IN ITALIA

Il report redatto dall'Osservatorio Cybersecurity del gruppo ICT ha evidenziato però che, nonostante il calo estivo, la situazione risulta peggiore rispetto al 2021. Migliora al Sud l'indice sulla sicurezza informatica dei dispositivi IoT.

28 ottobre 2022. Il cybercrime si concede una pausa. Diminuiscono nel periodo estivo gli attacchi e gli incidenti informatici e si riapre leggermente la forbice tra i primi e i secondi: segnali che evidenziano come il crimine informatico viaggi in parallello con l'attività economica.

È quanto emerge dal nuovo report **'Threat Intelligence Report'** dell'**Osservatorio Cybersecurity di Exprivia sulle minacce informatiche in Italia** che, tra luglio e settembre **2022, registra 251 attacchi, 203 incidenti** – ovvero attacchi andati a buon fine – e **27 violazioni della privacy**.

Netta la diminuzione dei fenomeni osservati (481 in totale) rispetto ai 766 del trimestre precedente, con un calo del 34% degli attacchi e del 43% degli incidenti, mentre per le violazioni della privacy non emerge una variazione significativa.

Il rapporto stilato dal gruppo ICT pugliese – che prende in considerazioni 113 fonti aperte (siti di aziende colpite, siti pubblici di interesse nazionale, agenzie di stampa online, blog e social media) – rileva che **l'87% dei fenomeni** è attribuibile ad attività legate al **crimine informatico**, ormai da sette trimestri in cima alle motivazioni degli attaccanti. A netta distanza hacktivism – ovvero azioni di disobbedienza civile in rete – (8% circa), e data breach (6% circa). Crolla vertiginosamente il cyber warfare (guerra cibernetica) che, con lo scoppio del conflitto tra Russia e Ucraina, si era aggiunto alla lista delle motivazioni degli hacker registrando un'impennata nel secondo trimestre del 2022, fino a quasi scomparire nel terzo (-96%).

Se tra i pretesti usati dagli attaccanti primeggia il **banking on line**, compare anche il **security alert** – una vera e propria trappola per trarre in inganno gli utenti indotti, ad esempio, a fornire informazioni riservate – seguito dagli **aquisti virtuali**.

"Dopo un periodo in cui le minacce informatiche sono cresciute continuamente, nei mesi estivi si è verificato un considerevole ridimensionamento dei casi e un allargamento della forbice tra attacchi e incidenti – **commenta Domenico Raguseo, direttore Cybersecurity di Exprivia**. *Paragonando, però, il terzo trimestre del 2022 allo stesso periodo dell'anno precedente, si nota un sensibile peggioramento della situazione, e riteniamo il dato del trimestre più correlato a una "pausa" estiva*

che a una migliorata capacità difensiva dell'ecosistema. Temiamo, infatti, che i primi mesi del 2023 possano riservare molte insidie".

Nonostante la riduzione dei casi rispetto ai mesi precedenti, infatti, il terzo trimestre dell'anno **risulta sensibilmente peggiore rispetto allo stesso periodo del 2021 (con una crescita del 76%), quando i fenomeni registrati erano stati 273**.

Secondo l'Osservatorio di Exprivia il settore **Finance** – che comprende dagli istituti bancari alle assicurazioni, alle piattaforme di criptovalute – pur registrando un trend in diminuzione rispetto al trimestre precedente, rimane quello maggiormente bersagliato dagli attaccanti, con 177 casi rilevati tra luglio e settembre. Al secondo posto il settore **Software/Hardware**, quindi società ICT, di servizi digitali, piattaforme di e-commerce, dispositivi e sistemi operativi, con 71 casi contro i 130 del trimestre precedente. Questo settore conferma un incremento a settembre, in concomitanza con la ripresa delle attività economiche e commerciali.
Il settore **Industria** si conferma al terzo posto con 55 casi, mentre la **Pubblica Amministrazione** resta in linea con il trimestre precedente (48 casi) segnando un significativo trend al ribasso nell'andamento dei fenomeni, mentre primeggiava durante la fase più acuta della pandemia di Covid-19.

Tra luglio e settembre torna al primo posto tra le tecniche di attacco il **phishing/social engineering** con 248 casi, confermando però un trend discendente nel corso dell'anno. Seguono i **malware**, ossia vettori di attacco volti a sottrarre informazioni sensibili (172 casi, in diminuzione del 45% rispetto al trimestre precedente) mentre gli **attacchi DDOS** (malfunzionamento o interruzione dei servizi informatici) passano dai 112 casi del secondo trimestre a un solo caso registrato nei mesi estivi.

Dal report di Exprivia emerge, inoltre, che in Italia i dispositivi IoT sono cresciuti del 6% e i nuovi indici elaborati dall'Osservatorio evidenziano un forte recupero del Sud nel rapporto tra dispositivi sicuri e non. Migliora anche il rapporto tra servizi digitali analizzati e vulnerabilità identificate su tutto il territorio nazionale, con maggiore intensità al Nord, che mantiene comunque un ritardo rispetto al Centro-Sud poiché i servizi digitali a disposizione del cittadino continuano a essere maggiormente presi di mira dagli hacker.

Ai dispositivi analizzati (come telecamere di video sorveglianza o stampanti), **si aggiungono all'analisi dell'Osservatorio quelli medicali**, dei quali solo l'8,6% è vulnerabile, **risultando quindi meno a rischio rispetto agli altri.**

"Nell'ultimo trimestre si riscontra una maggiore consapevolezza del Sud sui danni che può provocare una inefficace gestione della sicurezza dei dispositivi IoT – **prosegue Domenico Raguseo** – *rispetto a quanto evidenziato in precedenza. Questo ci fa ben sperare anche sul lavoro dell'Osservatorio, che mira proprio a sensibilizzare su temi legati alla cultura della sicurezza informatica, non solo delle imprese ma anche degli ecosistemi individuali".*

Exprivia, che recentemente ha ottenuto la certificazione Cybersecurity Made in Europe assegnata dal Comitato Nazionale per la Ricerca in Cybersecurity e promossa dall'European Security Organization (ECSO), ha presentato il report nell'ambito dell''Apulia Cybersecurity Forum', quattro giorni di eventi organizzati dal gruppo ICT sul tema della sicurezza informatica.

Exprivia

Exprivia è a capo di un gruppo internazionale specializzato in Information and Communication Technology in grado di indirizzare i driver di cambiamento del business dei propri clienti grazie alle tecnologie digitali.

Con un consolidato know-how e una lunga esperienza data dalla presenza costante sul mercato, il gruppo dispone di un team di esperti specializzati nei diversi ambiti tecnologici e di dominio, dal Capital Market, Credit & Risk Management all'IT Governance, dal BPO alla Cybersecurity, dai Big Data al Cloud, dall'IoT al Mobile, dal networking alla collaborazione aziendale sino al mondo SAP. Il gruppo affianca i propri clienti nei settori Banking&Finance, Telco&Media, Energy&Utilities, Aerospace&Defence, Manufacturing&Distribution, Healthcare e Public Sector. L'offerta comprende soluzioni composte da prodotti propri e di terzi, servizi di ingegneria e consulenza.

Oggi il gruppo conta circa 2.400 professionisti distribuiti in 7 paesi nel mondo.

Exprivia S.p.A. è quotata in Borsa Italiana nel mercato Euronext Milan (XPR).

La società è soggetta alla direzione e coordinamento di Abaco Innovazione S.p.A.

www.exprivia.it

COMUNICATO STAMPA

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
marmo@secnewgate.it - Cell. +39 335/6718211
Gianluigi Conese
conese@secnewgate.it - Cell. +39 335/7846403

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