Cybersecurity: dal Covid al conflitto Russia-Ucraina crescono le minacce informatiche nel 2022

Di **Redazione Data Manager Online** - 5 Maggio 2022

Secondo l'Osservatorio Cybersecurity di Exprivia, in Italia, nel primo trimestre dell'anno, peggiorano i dati rispetto al 2021. A marzo picco dei danni collegati alla crisi internazionale: fake news sul conflitto e campagne di aiuto umanitario nuovi ganci per le attività criminali

Dalla pandemia al conflitto bellico, nuovo e allarmante balzo dei fenomeni di crimini perpetrati sul web nel primo trimestre del 2022, il peggiore degli ultimi due anni. È quanto emerge dall'ultimo Report sulle minacce informatiche **dell'Osservatorio Cybersecurity di Exprivia** che, tra gennaio e marzo, registra in **Italia 806 casi tra attacchi, incidenti e violazioni della privacy**, in forte aumento rispetto alla media dei trimestri precedenti.

Nello specifico, si rileva circa **il 78% di casi in più rispetto all'ultimo trimestre del 2021** (quando si verificarono 454 fenomeni), con 213 eventi nel mese di gennaio, 207 a febbraio e 386 a marzo, il mese di maggior impatto in cui i criminali hanno sfruttato la situazione di instabilità internazionale

Cybersecurity: dal Covid al conflitto Russia-Ucraina crescono le minacce informatiche nel 2022

Secondo l'Osservatorio Cybersecurity di Exprivia, in Italia, nel primo trimestre dell'anno, peggiorano i dati rispetto al 2021. A marzo picco dei danni collegati alla crisi internazionale: fake news sul conflitto e campagne di aiuto umanitario nuovi ganci per le attività criminali

Dalla pandemia al conflitto bellico, nuovo e allarmante balzo dei fenomeni di crimini perpetrati sul web nel primo trimestre del 2022, il peggiore degli ultimi due anni. È quanto emerge dall'ultimo Report sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia che, tra gennaio e marzo, registra in Italia 806 casi tra attacchi, incidenti e violazioni della privacy, in forte aumento rispetto alla media dei trimestri precedenti.
Nello specifico, si rileva circa il 78% di casi in più rispetto all'ultimo trimestre del 2021 (quando si verificarono 454 fenomeni), con 213 eventi nel mese di gennaio, 207 a febbraio e 386 a marzo, il mese di maggior impatto in cui i criminali hanno sfruttato la situazione di instabilità internazionale legata soprattutto alla guerra tra Russia e Ucraina. Secondo l'Osservatorio Exprivia, che prende in considerazione 113 fonti pubbliche, in questi primi mesi del 2022, oltre al banking on line e agli acquisti virtuali, che mantengono il primato, tra i pretesti per colpire le vittime emerge la guerra russo-ucraina, con frequenti inganni che si nascondono dietro fake news sul conflitto o false campagne di aiuti umanitari.

Dal Report risulta che tra gennaio e marzo si sono verificati 408 attacchi, 379 incidenti di sicurezza cioè attacchi andati a buon fine, e 19 violazioni della privacy. Continua, quindi, a crescere velocemente il rapporto tra incidenti e attacchi informatici, alimentando la percezione che, malgrado gli investimenti degli ultimi anni nella sicurezza, gli hacker aumentano e sono sempre più efficaci, provocando danni legati pricipalmente al furto dei dati e di denaro.

Leggi anche: Genetec pubblica l'indagine sullo Stato della Sicurezza Fisica
"Negli ultimi due anni, gli eventi ad alto impatto politico ed economico e le relative tensioni sociali hanno concesso ai criminali di sfruttare occasioni come il Covid o, recentemente, il conflitto tra Russia e Ucraina per ingannare le vittime, nella maggior parte dei casi a scopo di lucro – commenta Domenico Raguseo, direttore Cybersecurity di Exprivia. Nello sconfinato ecosistema digitale in cui viviamo non è semplice attribuire cause e origini geografiche dei crimini informatici; se un attacco viene sviluppato per una vittima designata, potrebbe colpire anche altri soggetti e, se un malware viene utilizzato per uno scopo specifico, presto potrebbe diventare patrimonio di altri criminali che lo utilizzeranno per fini differenti. Quindi, al momento stiamo toccando con mano i primi danni provocati dal conflitto bellico anche in rete, e nei prossimi mesi le conseguenze

potrebbero essere ancora più severe”.

Secondo l’Osservatorio Exprivia, nel primo trimestre del 2022 il settore Finance – che comprende dagli istituti bancari alle assicurazioni, alle piattaforme di criptovalute – è quello che ha registrato il maggior numero di fenomeni criminali (286, oltre un terzo del totale), con un picco di 161 casi solo nel mese di marzo, tra furto dei dati di carte di credito, accesso a conti bancari e richieste di denaro. A seguire la Pubblica Amministrazione, con 109 casi tra attacchi, incidenti e violazioni della privacy, più che triplicati rispetto a quelli registrati nell’ultimo trimestre del 2021. Al terzo posto, con 91 casi, il settore del Software/ Hardware, quindi società ICT, di servizi digitali, piattaforme di e-commerce, dispositivi e sistemi operativi, che principalmente subiscono il furto di dati, come credenziali di accesso o informazioni sensibili; dal rapporto emerge un balzo dei casi a marzo, con un numero piu che doppio rispetto a quello di gennaio e febbraio.

Leggi anche: Check Point Software presenta in Italia la prima edizione della Check Point SecureAcademy

“È sempre più in crescita il resoconto dei crimini informatici sulle fonti analizzate dal nostro Report, anche in conseguenza dell’aumentata criticità dei servizi digitali da cui dipendiamo. Maggiori sono l’impatto e la durata di un incidente o semplicemente di un attacco, minore è la probabilità che la cosa passi inosservata – osserva Raguseo. Anche sui mass-media, ormai la visibilità e la rilevanza del cybercrime aumentano di pari passo con le nuove vulnerabilità sfruttate dai criminali”.

Tra le tecniche più utilizzate dai criminali informatici c’è il phishing, modalità di adescamento tramite e-mail ingannevoli o social network, con 389 fenomeni e un aumento dell’80% rispetto agli ultimi tre mesi del 2021. D’altro canto si riscontra un incremento esponenziale (+102% rispetto all’ultimo trimestre dello scorso anno) nell’utilizzo dei malware – con 372 casi – come vettore di attacco per sottrarre informazioni sensibili, principalmente mediante lo spionaggio delle attività bancarie degli utenti. Da non sottovalutare anche i malware che stanno provocando gravi danni di reputazione ed economici, criptando i dati di varie organizzazioni e aziende per chiedere riscatti in denaro.