05/08/2020

federconsumatorivda.it

Argomento: Exprivia: si parla di noi

EAV: € 110
Utenti unici: 333

Link alla pagina web

Coronavirus e crimini informatici, più 250% nel secondo trimestre dell'anno.

I crimini informatici viaggiano insieme al coronavirus. Nel secondo trimestre del 2020 i crimini informatici sono aumentati di oltre il 250% rispetto al primo trimestre. Picchi di attacchi informatici ci sono stati a giugno. Il 60% degli attacchi porta a furto dei dati: questi sono aumentati del 361% rispetto al primo trimestre. Sono cresciuti del 300% i casi di phishing. E per il futuro non ci sono buone prospettive. È facile attendersi che i crimini informatici continueranno ad avere ingenti numeri. A rischio saranno soprattutto i sistemi di videosorveglianza e i dispositivi IoT, Internet of Things, non adeguatamente protetti. I numeri vengono dall'Osservatorio Cybersecurity di Exprivia che anche nel secondo trimestre dell'anno ha collegato al coronavirus la maggior parte dei fenomeni segnalati. Il rapporto sulle minacce informatiche nel 2020 in Italia, al secondo numero, dice che giugno è stato il mese in cui dall'inizio dell'anno ci sono stati il maggior numero di attacchi, incidenti e violazioni della privacy a danno di aziende, privati e pubblica amministrazione. Attacchi e crimini informatici sono passati dai 47 del primo trimestre dell'anno ai 171 del secondo trimestre: più 250% di aumento, con un picco nel mese di giugno che ha contato 86 attacchi «complici l'incremento dello smart working, una maggiore connessione ai social network durante l'emergenza e la riapertura delle industrie subito dopo il lockdown», dicono da Exprivia. La maggior parte degli attacchi , sono da mettere in relazione all'emergenza Coronavirus e oltre il 60% degli episodi ha provocato come danno il furto dei dati con una crescita a tripla cifra rispetto al primo trimestre (+ 361%), superando di gran lunga sia le violazioni della privacy (11% dei casi) che le perdite di denaro (7%). Per gli esperti di Exprivia sono ad alto rischio i sistemi di videosorveglianza. Nel secondo trimestre 2020 sono inoltre aumentati del 700% gli attacchi di matrice 'hacktivistica', ossia

pratiche di azione digitale in stile hacker, un fenomeno emergente spesso collegato a campagne internazionali su temi di grande attualità. In questo periodo diversi siti illegali hanno sfruttato termini come 'Corona Antivirus' e simili per introdurre software malevoli nei computer delle vittime, compromettendone il funzionamento. Il cybercrime ha trovato terreno fertile soprattutto a causa di una diffusa mancanza di cultura digitale, anche nei singoli cittadini, e dell'inadeguatezza con cui aziende ed enti pubblici proteggono dati sensibili e sistemi informatici. Si prevede che nei prossimi mesi corrano un rischio elevato di attacchi anche i sistemi di videosorveglianza e i dispositivi IoT collegati a Internet che non vengono protetti adeguatamente, facilitando accessi illegittimi. Quadruplicano le truffe tramite tecniche di phishing e social engineering (+307% rispetto al primo trimestre, oltre il 37% dei casi), che ingannano l'utente facendo leva su messaggi "esca" via e-mail o su tecniche subdole tramite social network per carpire dati finanziari, come il numero di conto corrente o della carta di credito, oppure rubare i codici di accesso ai servizi a cui la persona è abbonata. Il 17% degli attacchi, invece, è avvenuto tramite malware (software o programmi informatici malevoli) che hanno sfruttato il Coronavirus per attirare l'attenzione degli utenti. Tra questi il programma "Corona Antivirus" o "Covid 9 Antivirus", un malware -spiegano dall'Osservatorio – che permette ai criminali informatici di connettersi al computer delle vittime e spiarne il contenuto, rubare informazioni o utilizzarlo come vettore per ulteriori attacchi. C'è poi "CovidLock", un ransomware (tipologia di malware che rende un sistema inutilizzabile esigendo il pagamento di un riscatto per ripristinarlo) che prende di mira gli smartphone Android quando si cerca di scaricare un'app di aggiornamenti sulla diffusione del Coronavirus. Oltre a una quota di campagne criminali indirizzate verso settori non classificabili, fra gli ambiti più attaccati ci sono la Pubblica amministrazione e il cloud. Fra i settori più vulnerabili ci sono Finanza ed Educazione (scuole e università impegnate con gli esami), e a giugno anche il settore Industria.