30/07/2020

CORCOM
IL QUOTIDIANO ON LINE DELL'ECONOMIA DIGITALE E DELL'INNOVAZIONE

EAV: € 1.032
Utenti unici: 10.400

Argomento: Exprivia: si parla di noi

Link alla pagina web

L'Italia sempre più bersaglio degli hacker, a giugno il picco

Nel secondo trimestre 2020 in aumento del 250% i crimini informatici. Prese di mira soprattutto industria e PA con oltre il 60% degli episodi che ha provocato il furto dei dati. In pericolo i sistemi di videosorveglianza La pandemia da Covid-19 in Italia ha influito pesantemente sulla sicurezza informatica anche post emergenza. Stando al secondo Rapporto sulle minacce informatiche nel 2020 in Italia, elaborato dall'Osservatorio sulla Cybersecurity di Exprivia, giugno è stato il mese in cui dall'inizio dell'anno si sono verificati la maggior parte di attacchi, incidenti e violazioni della privacy a danno di aziende, privati e pubblica amministrazione.Analizzando 40 fonti di informazione pubbliche è risultato che tra il primo trimestre dell'anno (quando gli attacchi erano stati 47) e il secondo (ben 171) l'incremento è stato superiore al 250% con un picco nel mese di giugno (ben 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.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%). E gli esperti di Exprivia pongono l'accento sull'elevato rischio che stanno correndo i sistemi di videosorveglianza presi di mira dagli hacker, che già nel primo trimestre hanno messo a punto un pericoloso attacco con il malware Mirai."In questo periodo diversi siti illegali – spiega Domenico Raguseo, direttore Cybersecurity Exprivia – hanno sfruttato termini come 'Corona Antivirus' e simili per introdurre software malevoli nei computer delle vittime, compromettendone il

Riproduzione autorizzata Licenza Promopress ad uso esclusivo del destinatario Vietato qualsiasi altro uso

exprivia | ITALTEL

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. Prevediamo anche 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".Dal secondo report dell'Osservatorio di Exprivia si evince inoltre che nel secondo trimestre in Italia sono cresciuti 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 come "black-lives-matter" e "revenge-porn".Quadruplicano, inoltre, 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 (il numero di conto corrente o della carta di credito) oppure rubare i codici di accesso ai servizi a cui la persona è abbonata.Anche nel secondo trimestre dell'anno resta ancora sconosciuta la modalità di attacco informatico in oltre il 30% dei casi (53 attacchi in più nel secondo trimestre), evidenziando così l'impellente necessità di elaborare adeguati sistemi di protezione. 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 che permette ai criminali informatici di connettersi al computer delle vittime e spiarne il contenuto, rubare informazioni o utilizzarlo come vettore per ulteriori attacchi. E ancora "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.Nel secondo trimestre dell'anno il 26% delle campagne criminali sono state indirizzate verso settori non classificabili e ben il 18% ha riguardato settori multipli; a seguire, tra gli ambiti individuati che hanno ricevuto più attacchi, quello della Pubblica Amministrazione e del Cloud (circa il 10% ciascuno sul totale), le cui piattaforme, anche dopo il lockdown, continuano a risentire dello stress per il lavoro da remoto. I settori Finance ed Education rimangono ancora nella lista degli ambiti più vulnerabili (in particolare a giugno università e scuole impegnate con gli esami), ma si registra una new entry per il settore Industria che a giugno segna un picco di attacchi evidentemente collegato alle riaperture di molte fabbriche dopo il periodo di

Riproduzione autorizzata Licenza Promopress ad uso esclusivo del destinatario Vietato qualsiasi altro uso

emergenza.

Riproduzione autorizzata Licenza Promopress ad uso esclusivo del destinatario Vietato qualsiasi altro uso