Truffe on line post Covid uno studio made in Molfetta


XIII | BARI PROVINCIA

Alga tossica a Molfetta
Guardia medica e farmacie prese d'assalto

IL DOSSIER

Truffe on line post Covid uno studio made in Molfetta

Gli esperti di Exprivia hanno indagato negli anfratti del web

L'EVENTO

Salta la sagra del calzone di cipolla?

Polemiche in agguato ad Acquaviva delle Fonti. Il sindaco Carlucci: «Potrebbe slittare al 2021»

LETTERE DAI LETTORI

«La Gazzetta, strumento di lavoro»

IL CAMPIONE Gli esperti dell'Arpa hanno effettuato controlli nelle acque di Prima Cala

NELLE PAGINE DELLA RETE La truffa sono all'ordine del giorno

IN AZIENDA Andriola a Nicol al lavoro

IL CASO

IL DOSSIER SECONDO RAPPORTO SULLE MINACCE INFORMATICHE NEL 2020 DELL' OSSERVATORIO SULLA CYBERSECURITY Gli esperti di Exprivia hanno indagato negli anfratti del web MOLFETTA. L' emergenza Covid-19 in Italia ha influito pesantemente sulla sicurezza informatica anche post emergenza. Stando a quanto risulta dal secondo rapporto sulle minacce informatiche nel 2020 in Italia elaborato dall' Os servatorio sulla Cybersecurity di Exprivia, giugno è stato il mese in cui dall' ini zio 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' in cremento 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' emer genza 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%). Sono stati proprio gli esperti dell' azienda molfettese specializzata nell' erogazione di servizi informatici a porre l' accento sull' ele vato rischio che stanno correndo i sistemi di videosorveglianza presi

di mira dagli hacker, che già nel primo trimestre hanno messo a punto un pericoloso at tacco con il malware MIRAI. «I n questo periodo diversi siti illegali - ha affermato Domenico Raguseo, direttore Cybersecurity Exprivia - hanno sfruttato termini come "Corona Antivirus" e simili per introdurre software malevoli nei computer delle vittime, compromettendone il funzionamento. Il cybercrime - aggiunge Raguseo - 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».