# PIÙ TRAPPOLE SUL WEB L' ALTRO VIRUS


Innovazione

35

I PIRATI DEL COVID-19

L'Economia

PIÙ TRAPPOLE SUL WEB
L'ALTRO VIRUS

Dai videogiochi fake alle false app Immuni: come evitare i nuovi attacchi informatici

di Chiara Sottocorona

Le tecniche

Gli obiettivi

Pit Spot
WindTre riparte con Fiorello (per le vacanze)

a cura di Aldo Grasso

Metropolis

Il guanto sensibile traduce la lingua dei segni

Mantello magico

Dai videogiochi fake alle false app Immuni: come evitare i nuovi attacchi informatici Il Covid-19 è stata una ghiotta occasione per gli hacker. «Da febbraio a maggio l' intero panorama del cybercrime è cambiato», avvertono i Kaspersky Lab. Una doppia pandemia: sanitaria e informatica. «Il numero di attacchi lanciati sfruttando il Coronavirus è così ampio da coprire tutti i tipi di crimini informatici - dice Giampaolo Dedola, ricercatore del Global Research and Analysis team di Kaspersky -. Frodi attraverso false raccolte di fondi per gli ospedali, file malevoli mascherati nelle istruzioni per proteggersi dal virus, falsi comunicati dell' Oms che installavano trojan bancari o virus informatici per ottenere un riscatto (ransomware, ndr.), campagne di phishing per rubare le credenziali bancarie su siti che imitavano quelli di alcuni istituti italiani». Non si è salvata neanche l' app anticontagio: un pericoloso ransomware ne ha sfruttato il nome. «È stato veicolato tramite una mail che proponeva una versione potenziata di Immuni realizzata per pc, indicata con un link», dice Dedola. Un clic e si scarica Immuni.exe, il file malevolo, da un falso sito che replica i contenuti della Federazione ordini farmacisti italiani. Se installato fa apparire una falsa schermata sulla contaminazione da Covid, seguita da una vera richiesta di riscatto di 300 euro in Bitcoin, per liberare i dati cifrati. CovidLock è un altro ransomware che prende di mira gli smartphone Android. È stato scoperto sul sito «Coronavirusapp» che propone di scaricare un' app per gli aggiornamenti sulla diffusione dell' epidemia. È

facile cadere nell' inganno. I malcapitati si ritrovano con il telefonino bloccato e un messaggio sullo schermo che dice: «Hai 48 ore per pagare 100 dollari in bitcoin o tutto sarà cancellato». È uno dei casi segnalati nell' «Exprivia Threat Intelligence Report» rilasciato in giugno dall' Osservatorio italiano sulla Cybersecurity. Il rapporto avverte che i crimini informatici hanno toccato un record nel mese di aprile. Durante il lockdown gli attacchi di phishing e di ransomware sono aumentati entrambi del 27% e i trojan che spiano i dati del 30%, indica Bitdefender, società di cyber-sicurezza che ha svolto un' ampia indagine internazionale: «L' indelebile impatto di Covid-19 sulla Cybersecurity». L' 86% degli intervistati (oltre 6 mila e 700 professionisti dell' Information technology) ha ammesso un forte aumento del cybercrime durante la pandemia. «Abbiamo constatato la vulnerabilità del telelavoro: per gli hacker è più facile passare attraverso un router casalingo e attaccare l' individuo, più fragile fuori dall' ufficio. Il 38% delle violazioni sono state veicolate dallo Iot : oggetti come box Internet, smart-speaker, smart-Tv - dice Denis Cassineiro, direttore vendite in Italia di Bitdefender -. C' è stato anche un aumento costante del cyberwarfare: gli attacchi alle infrastrutture critiche del Paese, come la Sanità. Gli ospedali sono diventati un target importante per i furti di dati, poi rivenduti nel Dark web, o di informazioni sensibili su farmaci e ricerca. Gli hacker ottengono una doppia monetizzazione: con il riscatto attraverso il ransomware e con la vendita dei dati». Il 74% dei professionisti della sicurezza, secondo l' indagine di Bitdefender, pensa che in Italia la Sanità non sia adeguatamente protetta. E un terzo teme che l' uso di computer e mail personali sia veicolo di minacce per i sistemi aziendali. Mentre eravamo tutti a casa a lavorare, studiare, passare il tempo sui social o in videoconferenza, i cybercriminali si sono scatenati attraverso siti di gaming, di intrattenimento e social meeting. Il Kaspersky Security network ha rilevato un aumento del 54%, rispetto a gennaio, degli attacchi di phishing attraverso le principali piattaforme di gaming e oltre 200 minacce che sfruttavano i nomi delle applicazioni di videoconferenze più usate, da Zoom a Slack. «Il cybercrime usa i nomi delle piattaforme di gaming, come Steam e Fortnite, o di videogiochi come Minecraft, per attirare con promozioni su falsi siti che rubano password e credenziali bancarie - dice Dedola -. E nei giorni scorsi abbiamo segnalato un attacco su siti di ecommerce con la tecnica del Web Skimming, che cattura dati delle carte di credito». Come difendersi? «Va alzato il livello degli investimenti - dice Cassineiro -. Occorre passare da una sicurezza reattiva a una proattiva: monitoraggio costante per rilevare l' attacco prima che sia lanciato ».