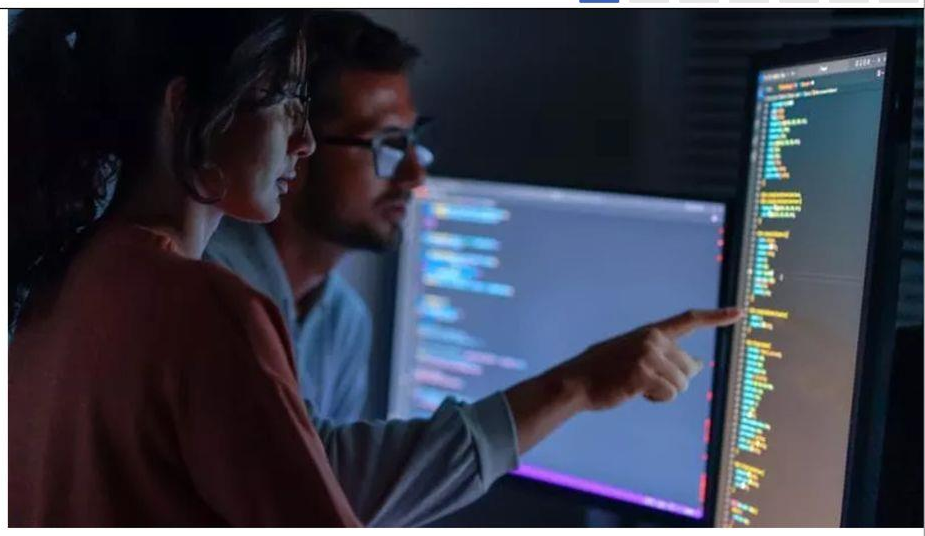
“Dalle app ai social, siamo tutti spiati. Ecco come accorgersene e come difendersi”

di Viola Giannoli



Intervista ad Alessio Aceti, ceo del provider Hwg Sababa e esperto di cybersicurezza

Ascolta l'articolo

07:16

28 OTTOBRE 2024 AGGIORNATO ALLE 20:59

3 MINUTI DI LETTURA

Se per diventare spioni ci vogliono abilità tecniche, manie di controllo, interessi dall’illecito o spregiudicatezza criminale, a finire tra gli spiati basta pochissimo. Perché moltissime informazioni le rendiamo pubbliche noi stessi, altre possono essere violate con software, trojan, app, sms, whatsapp, mail, chiamate. Esistono però anche scudi per difendersi. Lo spiega **Alessio Aceti**, ceo di Hwg Sababa, un provider di cybersecurity che offre consulenze e soluzioni contro le minacce informatiche.

Inchiesta hacker, Renzi si costituisce parte civile, il Pd: “Meloni riferisca in Parlamento”. La Russa: “Chi sono i mandanti?”

28 Ottobre 2024

Aceti, quanto è facile e frequente essere spiati?

“La risposta varia a seconda della criticità dei dati a cui si ha accesso. Tutti abbiamo una vita sui social e immettiamo dunque i nostri dati direttamente nel web: i nostri interessi, che scuola fanno i figli, i luoghi che visitiamo, le persone che frequentiamo. E più dati immettiamo più questi sono disponibili. C’è insomma una gran quantità di informazioni già pubbliche. Esiste poi un secondo livello che è quello delle informazioni non pubbliche. E quasi tutti noi siamo stati indirettamente vittime di furti di dati: basti pensare al caso Synlab quando 1,5 terabyte di documenti sanitari sono finiti nel dark web, anche le mie analisi del sangue. Il problema è che non dobbiamo più pensare a questi dati uno alla volta: chi vuole spiarci può prenderli tutti e unire i puntini, ricostruendo una mole notevole di informazioni private”.

In che modo si viene spiati?

“Si possono prendere Open data source, ovvero informazioni aperte, a cui chiunque può accedere, senza violazioni. Ci sono poi tool disponibili gratuitamente o per pochi euro che permettono di fare ricerche su una persona e di “bucare” ad esempio le app per la dieta, per il fitness, per la salute. Esistono software legittimi che consentono degli screening, utili ad esempio ad aziende che si occupano di Difesa per la scelta del

personale, che nelle mani sbagliate possono essere usati in maniera illegittima. Poi c'è il caso degli "impiegati infedeli" che hanno accesso ad esempio ai nostri conti bancari, li spiano e potrebbero anche venderli o diffonderli".

Enrico Pazzali, quel Tarzan in grisaglia che usava i partiti come liane. Tentò di sedurre anche Amazon

di Francesco Manacorda
28 Ottobre 2024

Password e conversazioni possono essere rubati anche attraverso mail o link sospetti.

"Certo, con il phishing, attraverso mail o messaggi whatsapp, si cercano di estorcere credenziali, password o informazioni spacciandosi come per un ente, una società o una persona affidabile. Oppure esistono dei link per scaricare App quasi identiche nella grafica e nel nome a quelle ufficiali ma che in realtà sono delle esche attraverso le quali un malintenzionato si introduce nel nostro telefono e legge messaggi in entrata e in uscita. Lo stesso può avvenire attraverso sms o chiamate. Si parla spesso di "Trojan", software legittimi che funzionano come il cavallo di Troia, appunto, e che una volta inseriti o scaricati su un dispositivo sono in grado di metterlo in comunicazione con un altro e da lì spiarne il contenuto".

La minaccia principale arriva dagli hacker o da dipendenti infedeli all'interno di aziende o pubbliche amministrazioni?

"Da entrambi. La criminalità organizzata agisce con comportamenti estorsivi. Ci sono poi alcune, per fortuna poche, società di consulenza che dovrebbero operare nella legalità e invece ne travalicano i confini. C'è poi l'attività degli insider, cioè dei dipendenti che violano i dati. Purtroppo c'è ancora poca attenzione e formazione sia da parte dei privati che da parte delle aziende".

C'è un modo per capire se si è spiati?

"Esistono pochi alert automatici. Però quando i dispositivi – cellulari, pc o tablet – sono compromessi si scaldano di più, la batteria si scarica più velocemente, si aprono di continuo dei pop up di verifica che chiedono più e più volte se procedere o meno con una operazione, vengono visualizzate schermate strane oppure si nota qualcosa di anomalo nei processi di autorizzazione a fornire ulteriori informazioni: nomi sbagliati, mail differenti da quelle ufficiali, estrema urgenza nella richiesta".

Cosa bisogna fare per proteggersi?

"Anzitutto mantenere i dispositivi aggiornati perché più un sistema operativo è aggiornato più è difficile che ci siano vulnerabilità e dunque tentativi di compromissione. Lo stesso vale per le singole applicazioni, soprattutto le più comuni: un attaccatore – così si chiamano coloro che voglio rubare dati – punterà infatti a quelle con più utenti per "bucare" più gente possibile con un solo investimento".

Bisogna cambiare password?

"Sì, costantemente, renderle complesse e una diversa dall'altra: ogni servizio deve avere una sua parola in codice. Le password non vanno salvate nei browser (tipo Google chrome) perché esistono moltissimi tool per rubarle. E' più opportuno acquistare un password manager commerciale (costano anche 20 euro l'anno) per conservarle tutte al sicuro. Nella scelta delle password non conviene utilizzare informazioni che ci riguardano troppo da vicino – il nome del papà, la data di nascita, la squadra del cuore -: meglio che siano facili per noi da ricordare ma assolutamente randomiche per un estraneo da indovinare. Un esempio: se avete un poster in camera degli anni 70 e accanto la foto di un gatto potreste usare postersiamese74".

Quali altri consigli?

Leggi anche

"Toga rossa Silvia Albano, spero che qualcuno ti spari". Minacce di morte alla giudice dei migranti

Ilaria Salis, l'Ungheria chiede la revoca dell'immunità. L'eurodeputata: "Il Parlamento difenda i diritti". Il portavoce di Orban: "Disgustosa"

Migranti, il Viminale ricorre in Cassazione contro il "no" ai trattenimenti. Un portavoce della Corte Ue: "Sentenza vincolante"

Raccomandati per te

Elezioni Usa, dai sondaggi ai meccanismi che determinano il vincitore: tutto quello che c'è da sapere

Il Fondo sovrano dell'Arabia Saudita taglia gli investimenti all'estero: -10%. "Focus sul nostro Paese"

Genova, il Comune verso nuove elezioni. E già si scalda il vice di Bucci

"Sugli account più critici come quelli di Google o dei social va attivata l'autenticazione a due fattori nelle impostazioni, altrimenti basta che qualcuno rubi la password per sapere ad esempio dove siamo stati e conoscere i nostri spostamenti nel tempo. E' bene stare attenti ai mittenti delle mail, ai numeri di provenienza di sms, whatsapp e chiamate e al loro contenuto, soprattutto se ci sono allegati e link. L'ultima frontiera della truffa è questa: con il deepfake potrebbe chiamarvi qualcuno che ha la voce del vostro capo e invece l'ha solo campionata utilizzando dei video. Se notate qualcosa di strano meglio diffidare e richiamare su numeri noti".

Cosa fare se ci si accorge di essere spiati?

"La cosa migliore è fare una segnalazione delle forze dell'ordine. E rivolgersi a un tecnico esperto in cybersecurity. Quando mi sono accorto che le mie analisi del sangue erano finite nel dark web ho fatto anche una segnalazione al Garante per la privacy".