Video rubati e venduti online, l'esperto di sicurezza informatica: «Gli hacker possono spiarvi anche attraverso l'aspirapolvere o lo spazzolino elettrico»

Oltre 2 mila video provenienti da abitazioni, palestre, centri estetici e persino ambulatori medici sono finiti in rete. Il docente dell'Università: «Persino l'aspirapolvere può essere spiato, io copro la webcam con il nastro adesivo»

(Fonte: https://corrieredelveneto.corriere.it/ 6 settembre 2025)

Nel riquadro, Mauro Conti, esperto di Sicurezza Informatica e docente

Un occhio elettronico che non si spegne mai, puntato su salotti, camere da letto e persino studi professionali, può trasformarsi in una vera «bomba» dal punto di vista della **privacy**. L'ultimo esempio è il caso portato alla luce in questi giorni da **Yarix**, il centro di competenza per la cybersecurity del gruppo Var di Treviso, che ha scovato migliaia di filmati rubati dalle telecamere di **videosorveglianza**, hackerate da pirati informatici e **rivenduti online** a pagamento. Un portale registrato alle Isole Tonga, raccoglie e organizza oltre 2 mila video provenienti da abitazioni, palestre, centri estetici e persino ambulatori medici. Sono già **150 i filmati italiani** identificati, tra cui tre provenienti da una sola abitazione di Verona. Per accedere al materiale basta collegarsi al portale o a un bot dedicato su Telegram e pagare una quota compresa tra 20 e 575 sterline.
Ma come ci si può difendere dalle nuove frontiere del cybercrimine? Lo abbiamo chiesto al professor **Mauro Conti,** esperto di Sicurezza Informatica e docente presso **l'Università degli Studi di Padova,** nonché capo del nodo di Padova del Laboratorio di Cybersicurezza Nazionale e del gruppo di hacker etici Spritz (Security and Privacy Research Group)

Professor Conti, com'è possibile che qualcuno sia in grado di spiarci nella privacy della nostra casa?

«Appena installiamo una telecamera nella nostra abitazione, soprattutto se si tratta di strumentazione a basso costo, senza adottare alcuni accorgimenti, **diventiamo potenziali prede di spioni** e malintenzionati esperti della rete. Spesso, infatti, chi installa una telecamera per sorvegliare le diverse stanze della propria casa, lascia le credenziali di accesso "user" e "password' di default, oppure password facilmente violabili. I cybercriminali utilizzano programmi automatizzati che scandagliano internet alla ricerca di dispositivi con credenziali non modificate. Una volta ottenuto l'accesso, deviano le immagini su server esterni e rivendono le credenziali in chat internazionali, permettendo a sconosciuti di spiare momenti intimi di ignare vittime. In Italia ci sono decine di migliaia di telecamere di sicurezza accessibili via internet, molte delle quali trasmettono immagini anche in diretta».

Ma dobbiamo preoccuparci anche quando andiamo dal medico o in un centro estetico?

«In queste tipologie di attività vengono generalmente installate telecamere più professionali, ma anche in questo caso le credenziali possono essere conservate da un installatore infedele della ditta che ha montato la telecamera e vendute successivamente. Oppure possono essere rubate attraverso attività di hacking ai danni dell'azienda. Cambiare periodicamente le credenziali di accesso diventa indispensabile».

Ma è possibile filmare un paziente o un cliente del camerino mentre si spoglia?

«La legge non permette di installare telecamere in bagni, spogliatoi, docce e aree di riposo, (salvo che per disposizioni dell'autorità giudiziaria). Tuttavia, probabilmente, a volte succede comunque. Oppure ci possono essere delle "spycam" ossia installate di nascosto, in questo caso l'unica arma è un controllo accurato della stanza».

Già nel 2016 era diventata virale una fotografia di Mark Zuckerberg mentre utilizzava il computer con webcam e microfono coperti da un nastro adesivo. Ma davvero ci possono spiare anche da lì?

«Certo. Anch'io utilizzo lo stesso accorgimento. Per violare una webcam, i criminali informatici devono innanzitutto ottenere l'accesso al nostro PC, smartphone o tablet. Una volta entrati, possono controllare la webcam e, ad esempio, accenderla a piacimento. Per farlo, gli hacker utilizzano diversi metodi».

Attenzione anche a baby monitor, smart TV, router, robot per pulire i pavimenti, ma anche allo spazzolino da denti…

«Ogni dispositivo connesso a internet è un potenziale bersaglio. Faccio un esempio: i dati sull'utilizzo di uno spazzolino possono rivelare molte informazioni 'vendibili: Uber, se avesse questi

dati, potrebbe organizzare le tempistiche dei clienti che prenotano un taxi (in genere l'utente si lava i denti prima di uscire). L'aspirapolvere può dare informazioni utili sul perimetro della casa, in questo caso a un potenziale ladro...».

Come possiamo accorgerci di essere «spiati» a casa nostra?
«Non è sempre semplice, perché le cosiddette spie accese che ci potrebbero mettere in allerta possono ormai essere hackerate. Serve la lettura dei registri degli accessi. Il consiglio è di rivolgersi, in caso di dubbi, a un esperto o alla Polizia Postale».

Leggi anche

- **Video rubati in case e studi medici: scoperto il portale che li vende in retedi Roberta Polese**
- **Aziende sotto attacco hacker, dal finto fornitore alla «frode del Ceo»: aumentano le estorsioni sessuali**
- **Hacker e passaporti rubati, l'hotel di Venezia: «Siamo corsi ai ripari, denuncia anche al Garante per la privacy»**
- **Gli hacker attaccano gli hotel, documenti dei clienti in vendita sul dark web per 20mila euro: colpito un 4 stelle di Venezia**