Italiani sotto assedio informatico: da dove arrivano gli attacchi più pericolosi

di Pierpaolo Molinengo

Pubblicato il 21 Giugno 2024

L'utilizzo di internet e dei device informatici è sempre più pericoloso: le minacce si nascondono quasi ovunque e mettono a rischio la privacy ed i dati anche di professionisti e aziende. Strumenti come VPN e blocco dei tracker possono migliorare la sicurezza.

Quali sono le principali minacce che impattano sui dipendenti che si collegano ad Internet per lavorare? Da dove arrivano gli attacchi alla sicurezza e alla privacy dei device aziendali? A rispondere a questa domanda di ha pensato una ricerca di NordVPN, che ha messo in evidenza che i maggiori problemi arrivano dai contenuti per adulti, dai siti di video hosting gratuiti e da quelli che si spacciano per popolari ed affidabili brand. Anche quella che può sembrare come una normale attività online, può nascondere delle insidie, che possono arrecare ingenti danni ai dati protetti dell'azienda. Se non vengono adottate degli accurati sistemi di sicurezza.

> *"Ogni giorno affrontiamo minacce informatiche senza nemmeno accorgercene - spiega Adrianus Warmenhoven, consulente per la sicurezza informatica di NordVPN -. Anche se non vediamo malware o tracker a occhio nudo, o riusciamo a gestire l'irritazione causata dagli annunci invadenti, ciò non ci salva da gravi problemi di privacy e sicurezza informatica. Dobbiamo migliorare le nostre conoscenze e utilizzare strumenti tecnologici affidabili per evitare queste minacce. La maggior parte delle funzioni anti-malware integrate nelle VPN più diffuse si limita solitamente a un semplice filtro DNS. Lo strumento di protezione digitale di NordVPN, aggiornato a Threat Protection Pro, aiuta gli utenti a evitare hacking, tracciamento, phishing, truffe, malware, annunci e cookie fastidiosi".*

Riproduzione riservata © www.commercialistatelematico.com
Documento riservato alla consultazione da parte di: N/D

Dove si nascondono i malware più insidiosi?

Una delle principali minacce per i device è il malware, un software dannoso che include virus, trojan, ransomware e spyware. Strumenti informatici progettati per danneggiare i dispositivi degli utenti connessi alla rete. Sono in grado di rubare dei dati sensibili, crittografare file importanti e, in alcuni casi, sono addirittura in grado di assumere il controllo dei dispositivi. Questo permette ai criminali informatici di avere pieno accesso alle informazioni più sensibili degli utenti. Sicuramente il metodo più comune per danneggiare i propri dispositivi è quello di visitare i siti più pericolosi. Ma non solo. I criminali informatici iniziano ad essere sempre più subdoli, arrivando ad adottare dei nomi di brand famosi, ma con degli errori ortografici ingannevoli, in modo da indurre gli utenti a cliccare su un link di phishing e scaricare dei file infetti. Almeno il 99% di tutti gli attacchi di phishing (negli ultimi avvisi del Fisco italiano si segnala il phishing per le criptovalute) utilizzano 300 brand famosi per commettere le loro frodi. Tra i marchi che vengono sfruttati di più per insidiare ed ingannare gli utenti - e per diffondere malware - ci sono:

- Office365: 86.000 URL falsi scoperti;
- Gazprom: 60.000;
- AT&T: 28.000;
- Facebook: 19.000;
- Bet365: 15.000.

> *“In questo i brand non hanno alcuna colpa: falsi come questi danneggiano anche la loro reputazione, costringendo le aziende a dare loro attivamente la caccia - spiega Warmenhoven -. Ma l'elevata popolarità del marchio può indurre le vittime a sentirsi al sicuro e quindi ad abbassare la guardia”.*

Un dispositivo subisce 75 attacchi al mese

Il malware agisce indisturbato a livello globale, anche se con percentuali diverse in base al paese di residenza. Le differenze potrebbero essere condizionate dai diversi livelli di connettività, di sviluppo economico e di consapevolezza della sicurezza informatica nei vari paesi. La ricerca NordVPN ha censito almeno 4,3 milioni di tentativi di infezione in Italia nei primi cinque mesi dell’anno. Mediamente un utente italiano è esposto a 75 incidenti legati a malware ogni mese. L’Ucraina è il paese più colpito: 786 tentativi di infezione da malware su dispositivo al mese.

Riproduzione riservata © www.commercialistatelematico.com
Documento riservato alla consultazione da parte di: N/D

I tracker invasivi dominano nei siti di video hosting gratuiti, compromettendo la privacy

> *"I tracker web costituiscono una vasta categoria di strumenti che minano la privacy e monitorano l'attività degli utenti - viene riportato nella ricerca NordVPN -. Solitamente, si presentano sotto forma di script speciali, cookie del browser o pixel di tracciamento. Purtroppo, in caso di violazione dei dati, le informazioni raccolte dai tracker potrebbero finire nelle mani sbagliate".*

Gli utenti dovrebbero prestare la massima attenzione nel momento in cui utilizzano dei siti di video hosting gratuiti, che rappresentano il 28% di tutti i tracker bloccati. Massima attenzione deve essere prestata, inoltre, allo storage online (13%) ed ai motori di ricerca (13%), i quali risultano essere i principali responsabili nel tracciamento delle attività degli utenti online.

> *"I siti web spesso condividono o vendono a terzi i dati raccolti dai tracker - conclude Warmenhoven -. Ma chi vuole proteggere la propria privacy può utilizzare diversi strumenti per diventare meno rintracciabile. Ad esempio, la VPN, che cambia l'indirizzo IP reale e la posizione virtuale, il blocco dei tracker o i browser per la privacy".*

NdR: potrebbe interessarti anche...Phishing: una subdola insidia che colpisce un italiano su due

Pierpaolo Molinengo venerdì 21 Giugno 2024

Riproduzione riservata © www.commercialistatelematico.com
Documento riservato alla consultazione da parte di: N/D