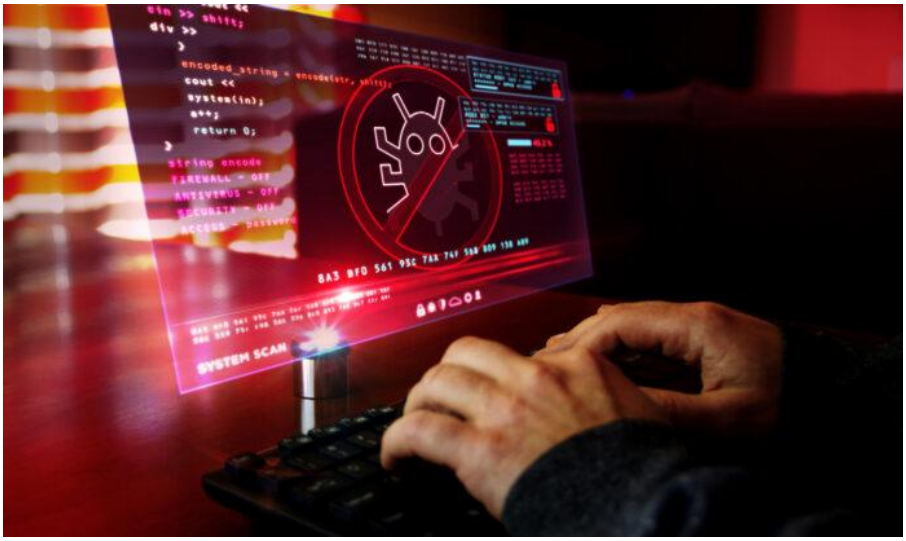
Windows-pc’s en Macs geïnfecteerd door EditPro, valse app die data steelt



Cybercriminelen zijn er al in geslaagd om heel wat Windows-pc’s en Macs te infecteren met een app die vermomd is als AI-toepassing. Het valse videobewerkingsprogramma ‘EditPro’ installeert schadelijke malware als Lumma Stealer en AMOS. Dat zijn twee zogenaamde ‘infostealers’. Lumma richt zich op Windows-gebruikers en kan gevoelige gegevens verzamelen, zoals inloggegevens, cryptoportefeuilles, cookies en browsergeschiedenis. AMOS is de tegenhanger voor macOS en voert vergelijkbare datadiefstal uit. De gestolen informatie wordt doorverkocht op het dark web of direct gebruikt voor verdere cyberaanvallen. Security-expert g0njxa ontdekte dat het programma ‘EditPro’ gebruikt wordt om de malware te verspreiden.

Misleiding via sociale media

De verspreiding van de malware is geraffineerd. Op sociale media zoals X (voorheen Twitter) verschijnen misleidende video’s waarin bekende figuren, zoals Joe Biden en Donald Trump, humoristisch worden afgebeeld. Bij de video’s staat een link naar de website van EditPro. Deze website oogt professioneel en bevat zelfs een cookiebanner, waardoor het vertrouwen wekt bij nietsvermoedende gebruikers. Na installatie van de app blijkt deze echter malware te bevatten.

EditPro geïnstalleerd: wat nu?

Heb je EditPro op je systeem staan, dan is directe actie noodzakelijk. Verwijder de software onmiddellijk en voer een grondige scan uit met een betrouwbaar antivirusprogramma. Wijzig alle wachtwoorden, zeker van accounts die gevoelige gegevens bevatten, zoals e-mail en banktoepassingen. Activeer daarnaast Multi-Factor Authenticatie (MFA) om je accounts beter te beveiligen. Houd je bankrekeningen en andere financiële informatie goed in de gaten voor verdachte activiteiten.

Blijf waakzaam

Om toekomstige infecties te vermijden, is het essentieel om software uitsluitend te downloaden van officiële bronnen, zoals erkende appstores. Controleer altijd reviews en beoordelingen voordat je een programma installeert. Wees daarnaast sceptisch over te mooi klinkende aanbiedingen, zoals gratis AI-tools met geavanceerde functionaliteiten.

Deze aanval laat opnieuw zien hoe belangrijk het is om voorzichtig om te gaan met populaire technologieën zoals AI-tools. Hackers blijven inspelen op trends en maken gebruik van misleidingstechnieken om slachtoffers te maken. Door alert te blijven en goede beveiligingsmaatregelen te nemen, kun je de risico's minimaliseren.

Bron: Clicks