Digital Security
Progress. Protected.

REDLINE/META

Er is een infostealer gedetecteerd

We begrijpen dat het verwarrend kan zijn om te weten wat je precies moet doen om jezelf te beschermen. Daarom hebben we dit eenvoudige document gemaakt, die hopelijk wat meer handvaten biedt bij de stappen die je kunt ondernemen.

Stap 1: Voer een volledige scan uit

Als je een korte scan (Quick Scan) hebt gedaan en die heeft malware (een virus of een gevaarlijk programma) gevonden, adviseren we je om je hele apparaat grondig laten controleren. Dit heet een "volledige scan".

Welke stappen kun je nemen?

- Open de Redline/META scanner en kies voor de optie "Volledige systeemscan".
- Laat het programma alles controleren. Dit kan enkele ogenblikken duren.

Stap 2: Verander je wachtwoorden

Als blijkt dat je geïnfecteerd bent, is ons advies om al je wachtwoorden te veranderen. Dit is belangrijk, omdat de malware mogelijk je wachtwoorden heeft gezien of opgeslagen, waardoor iemand anders nu toegang heeft tot je accounts.

Welke stappen kun je nemen?

- Verander wachtwoorden van belangrijke accounts zoals je e-mail, bank, Facebook of Instagram, en werkaccounts.
- Doe dit vanaf een ander apparaat, bijvoorbeeld je telefoon of tablet, die niet geïnfecteerd is. Je wilt niet dat je nieuwe wachtwoorden weer worden gestolen.
- Gebruik geen eenvoudige en korte wachtwoorden. Kies voor wachtzinnen die veiliger en makkelijker te onthouden zijn. Gebruik ook verschillende wachtwoorden voor elk account.

Stap 3: Controleer je bank- en persoonlijke accounts

De malware kan geprobeerd hebben om je bankgegevens of creditcardinformatie te stelen. Het is daarom belangrijk om te controleren of er geen rare of onbekende betalingen zijn gedaan.

Welke stappen kun je nemen?

- Log in op je bankrekening en bekijk je laatste transacties.
- Zoek naar betalingen of bedragen die je niet herkent.
- Als je iets verdachts ziet, bel dan meteen je bank en meld dit.
- Heb je je creditcard of inloggegevens voor werk of andere belangrijke accounts ingevoerd terwijl je apparaat geïnfecteerd was? Meld dit dan ook bij de betrokken bedrijven zodat ze stappen kunnen nemen om je te beschermen.

Stap 4: Update je apparaat en beveiligingssoftware

Soms vinden criminelen manieren om in je apparaat te komen door gebruik te maken van "gaten" in verouderde software. Door je software bij te werken (te updaten), sluit je die gaten. Zie het als het vervangen van je slot, bij het verliezen van je sleutel.

Welke stappen kun je nemen?

- Update je besturingssysteem (zoals Windows of Mac).
- Update je beveiligingsprogramma's en zorg ervoor dat ze altijd de nieuwste versie hebben. Dit betekent vaak dat ze je beter kunnen beschermen.
- Overweeg om een firewall aan te zetten (dit is als een soort onzichtbare muur die slechte dingen buiten houdt) en gebruik een VPN als je vaak openbare wifi gebruikt (zoals in een café of op school).

Stap 5: Blijf je accounts in de gaten houden

Ook nadat de malware is verwijderd door de volledige scan, moet je nog steeds alert blijven. Soms kan iemand je gegevens gebruiken, zelfs nadat je denkt dat alles veilig is.

Welke stappen kun je nemen?

- Controleer regelmatig je e-mail, bank, en sociale media op rare activiteiten, zoals vreemde berichten of transacties.
- Gebruik een wachtwoordmanager om sterke wachtwoorden te maken en op te slaan. Hierdoor hoef je niet elke keer een nieuw wachtwoord te bedenken en te onthouden, en kun je makkelijk sterke wachtwoorden gebruiken.

Stap 6: Schakel een expert in

Als je niet zeker weet of alles goed verwijderd is of als je gevoelige informatie hebt (zoals bedrijfsgegevens), kan het slim zijn om een expert in te schakelen. Die kan ervoor zorgen dat alles veilig is en dat er geen verborgen problemen zijn.

Welke stappen kun je nemen?

- Zoek online naar een betrouwbare IT-expert of een bedrijf dat gespecialiseerd is in het verwijderen van malware.
- Vraag hen om je systeem te controleren en te beveiligen.