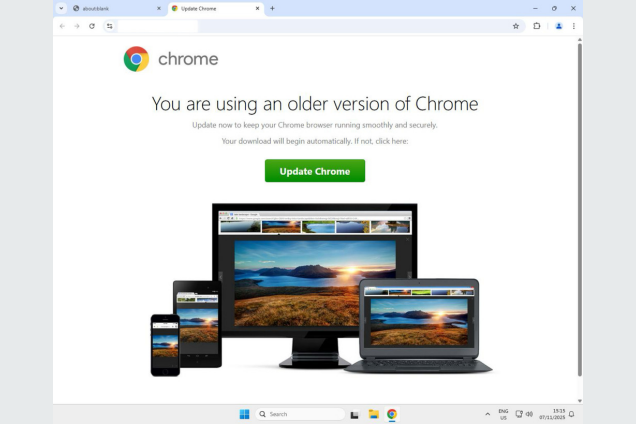
Beheert u een website die met WordPress is gemaakt?

Mogelijk is uw website gehackt, zonder dat u het weet. Criminelen hebben verschillende WordPress websites geïnfecteerd met SocGholish malware.

Voorkom verdere verspreiding. Neem maatregelen om uw WordPress website veilig te maken en te houden voor uw en de bezoekers van uw website.



Met deze malware kunnen bezoekers van de geïnfecteerde websites een fake update in hun scherm krijgen. Als bezoekers op de valse melding klikken, installeren zij geen officiële update, maar schadelijke software die criminelen toegang geeft tot hun (computer)systeem en gegevens.

Waar maakt SocGholish misbruik van?

1. De cybercrimineel logt in met uw gelekte wachtwoord en gebruikersnaam.
2. De cybercrimineel voegt malafide code (backdoor) toe aan de broncode van uw WordPress website.
3. De cybercrimineel maakt een eigen admin account aan met een eigen gebruikersnaam en wachtwoord.
4. De cybercrimineel logt in op de WordPress admin inlogpagina met uw gelekte gegevens, via de backdoor of via het extra account.

Wat kunt u nu zelf doen?

1. Verander uw wachtwoord en maak gebruik van de MFA (Multi-Factor Authentication)
2. Verwijder de malafide code (backdoor) van uw website. Ga naar www.NCSC.nl voor meer informatie
3. Verwijder accounts die onbekend zijn voor u of neem contact op met de websitebeheerder of uw hostingpartij om de accounts te verwijderen
4. Whitelist de IP-adressen van uw apparaten voor de /wp-admin inlogpagina

Meer informatie?

Ga naar politie.nl/actiebericht of www.NCSC.nl - de site van het Nationaal Cyber Security Centrum

Politie.nl/Endgame

POL-cu46cq8xoii-nl-NL-0626-1