Nieuwsbrief 125 - Week 39-2020

Meeluisteren met telefoongesprekken en meelezen met berichten en niets in de gaten, zes jaar lang

Zou het mogelijk zijn om tweestapsverificatie codes te stelen en vervolgens mee te luisteren met je spraakomgeving? Of mee te lezen met wat je communiceert via Telegram? Onderzoekers van CheckPoint hebben onlangs bekendgemaakt dat Iraanse entiteiten zich jarenlang hebben gericht op Iraanse expats en demonstranten...

LEES MEER »

Amsterdams waterbedrijf 'Waternet' hacken, is kinderspel

Bij het Amsterdamse waterbedrijf Waternet is de digitale beveiliging niet op orde. Dat blijkt uit een onderzoek van Follow The Money (FTM), die zich baseren op interne documenten en gesprekken met medewerkers. Het waterbedrijf blijkt gebruik te maken van verouderde systemen en er worden regelmatig beveiligingsmaatregelen teruggedraaid, aldus enkele medewerkers...

LEES MEER »

'Veilige kluisrekening', daar trapt de Cybersecurity specialist niet in

Met gebruik van zogeheten 'spoofing'-techniek konden criminelen de afgelopen maanden het telefoonnummer van de bank gebruiken om tientallen klanten te bellen en hen met een babbeltruc overhalen om geld naar een andere rekening over te maken. Zo konden in totaal miljoenen euro’s worden buitgemaakt. Nu blijkt dat de Rabobank deze fraude vergoedt, terwijl klanten van ING en ABN AMRO zelf opdraaien voor de schade...

LEES MEER »

Malware golf met varianten van Remote Access Trojan (RAT) verwacht

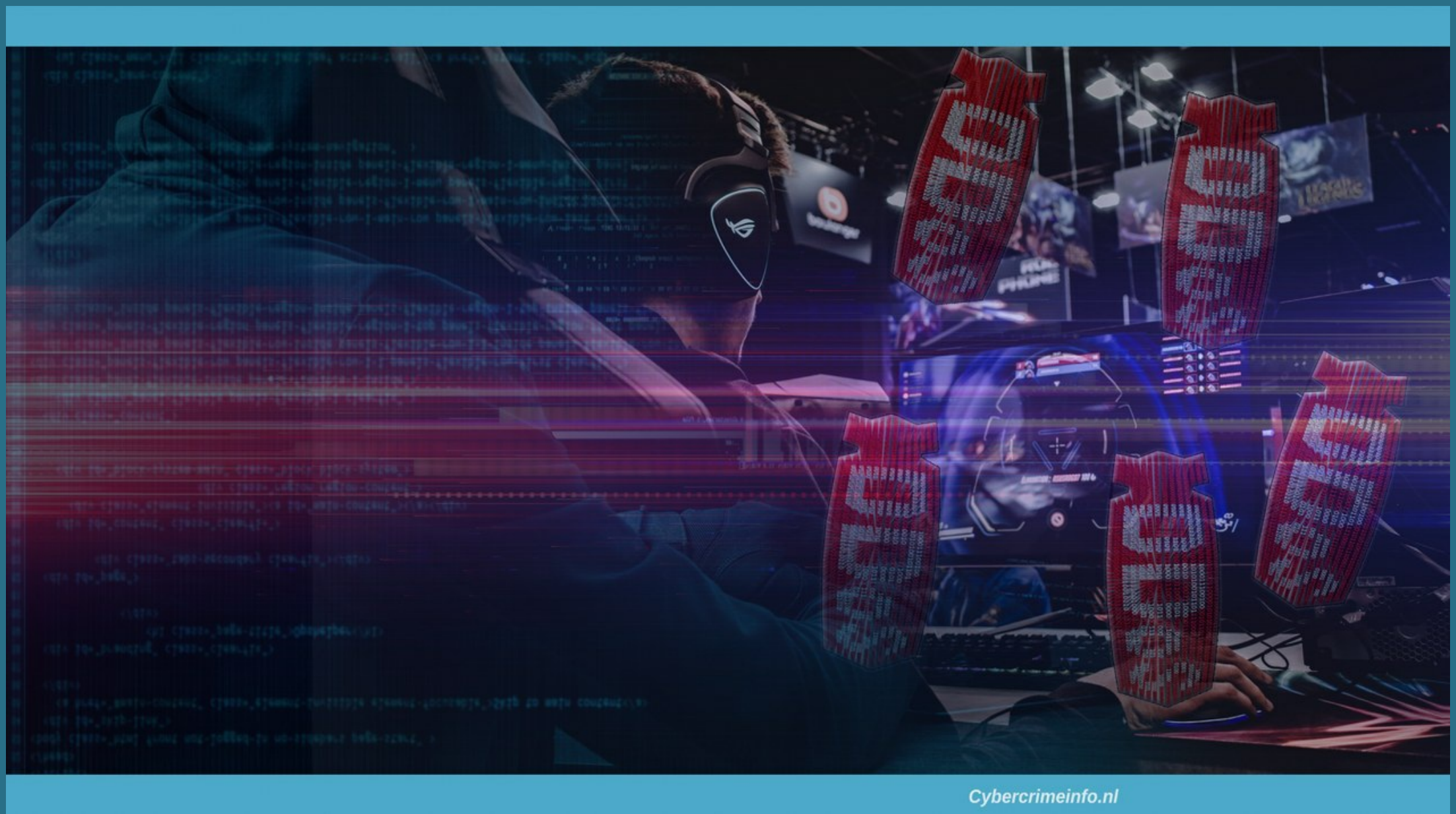
De volledige 'Cerberus-broncode' is gelekt op het darkweb en nu gratis beschikbaar voor cybercriminelen. Cerberus is een geavanceerde malware, gericht op online bankieren van Android. De bedoeling was dat de broncode van Cerberus online geveild zou worden. Door ‘een opeenstapeling van factoren’ besloot de maker om zijn programma gratis en voor niets aan te bieden op een Russisch platform dat voornamelijk bezocht wordt door hackers. Sindsdien zien beveiligingsspecialisten een toename in het aantal malafide applicaties voor smartphones....

LEES MEER »

Phishing, Smishing en Vishing populair als aanvalstechniek

De covid19 pandemie heeft wereldwijd honderdduizenden levens geëist, massale werkloosheid veroorzaakt en de manier waarop veel mensen hun leven leiden veranderd. Zelfs de economisch meest welvarende en stabiele economieën maken zich zorgen. Zullen bedrijven herstellen? Zullen we ons kunnen aanpassen aan deze nieuwe manier van leven? Het coronavirus is nog steeds erg onder ons, met regionale lockdowns waardoor de bewegingen van mensen worden beperkt. Natuurlijk heeft covid19 velen van ons gedwongen om meer tijd op internet door te brengen, goederen te kopen, werk te zoeken en het laatste nieuws over de pandemie te lezen...

LEES MEER »



De gaming-industrie behoort tot een van de zwaarst getroffen sectoren als het gaat om cyberaanvallen

Of het nu gaat om diamanten graven in een virtuele zandbak of de rol van een held spelen in een 'massively multiplayer online role-playing game' (MMORPG), of het zoeken naar de perfecte plek om een hinderlaag op te zetten in een 'first-person shooter (FPS)', gamen is voor velen aan het eind van de dag een beetje stoom afblazen. Of misschien midden op de dag wanneer er een lege ruimte in de agenda is, nu we allemaal vanuit huis werken. Vertel het maar niet aan mijn baas. ;-) De gaming-industrie behoort tot een van de zwaarst getroffen sectoren als het gaat om cyberaanvallen. Tussen juli 2018 en juni 2020 observeerde Akamai ruim 10 miljard aanvallen op webapplicaties verspreid over alle klanten van het bedrijf. Alleen voor de game-industrie waren dat in die periode 152 miljoen aanvallen...

LEES MEER »

Ransomware weekoverzicht week 38 - 2020

Nu de scholen over de hele wereld weer gestart zijn, blokkeren ransomware criminelen hen met cyberaanvallen die het begin van het schooljaar verstoren. In de afgelopen weken hebben we een gestaag spervuur van aanvallen gezien op basisscholen, hogescholen en universiteiten waar ransomware criminelen zich richten op slecht beveiligde externe desktopservers en de kwetsbaarheden van netwerkapparaten...

OVERZICHT »

Datalek nieuws en overzicht week 39-2020

Bij een 'datalek' gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens bij een organisatie. Of om vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens en verlies van (toegang tot) persoonsgegevens.

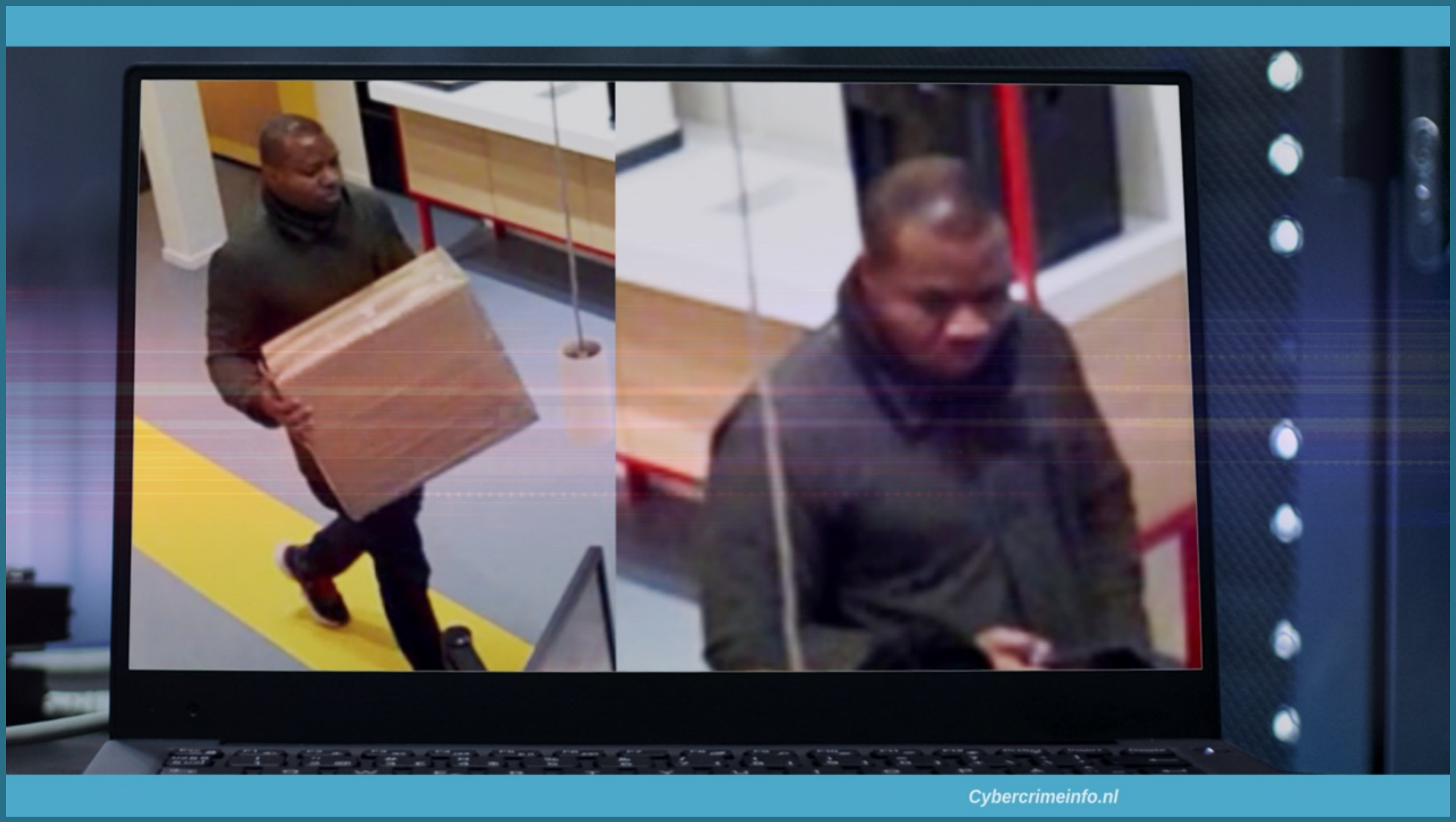
OVERZICHT »

Gedigitaliseerde oplichting / misdaad overzicht week 39-2020

Het melden van digitale oplichting pogingen is belangrijk, door het melden kunnen we andere potentiële slachtoffers behoeden voor het te laat is. Heb je een phishing mail, smishing bericht of werd je gebeld en vertrouw je het niet? Laat het ons, of onze collega's van Opgelicht?! of Fraudehelpdesk dan weten, want Samen bestrijden we cybercrime. Liever anoniem? Klik dan hier.

OVERZICHT »

Gezochte Personen



Amsterdam - Poging export grote hoeveelheid XTC-pillen

De politie is op zoek naar een man die ervan wordt verdacht op vrijdag 21 februari 2020 te hebben geprobeerd een grote hoeveelheid XTC-pillen naar het buitenland te versturen. De man bood die vrijdag omstreeks 18.50 uur een postpakket (doos) aan bij een servicepunt van DHL waar je post kan ophalen en verzenden op de Van Baerlestraat. In de doos zouden een aantal lampen moeten zitten...

LEES MEER »

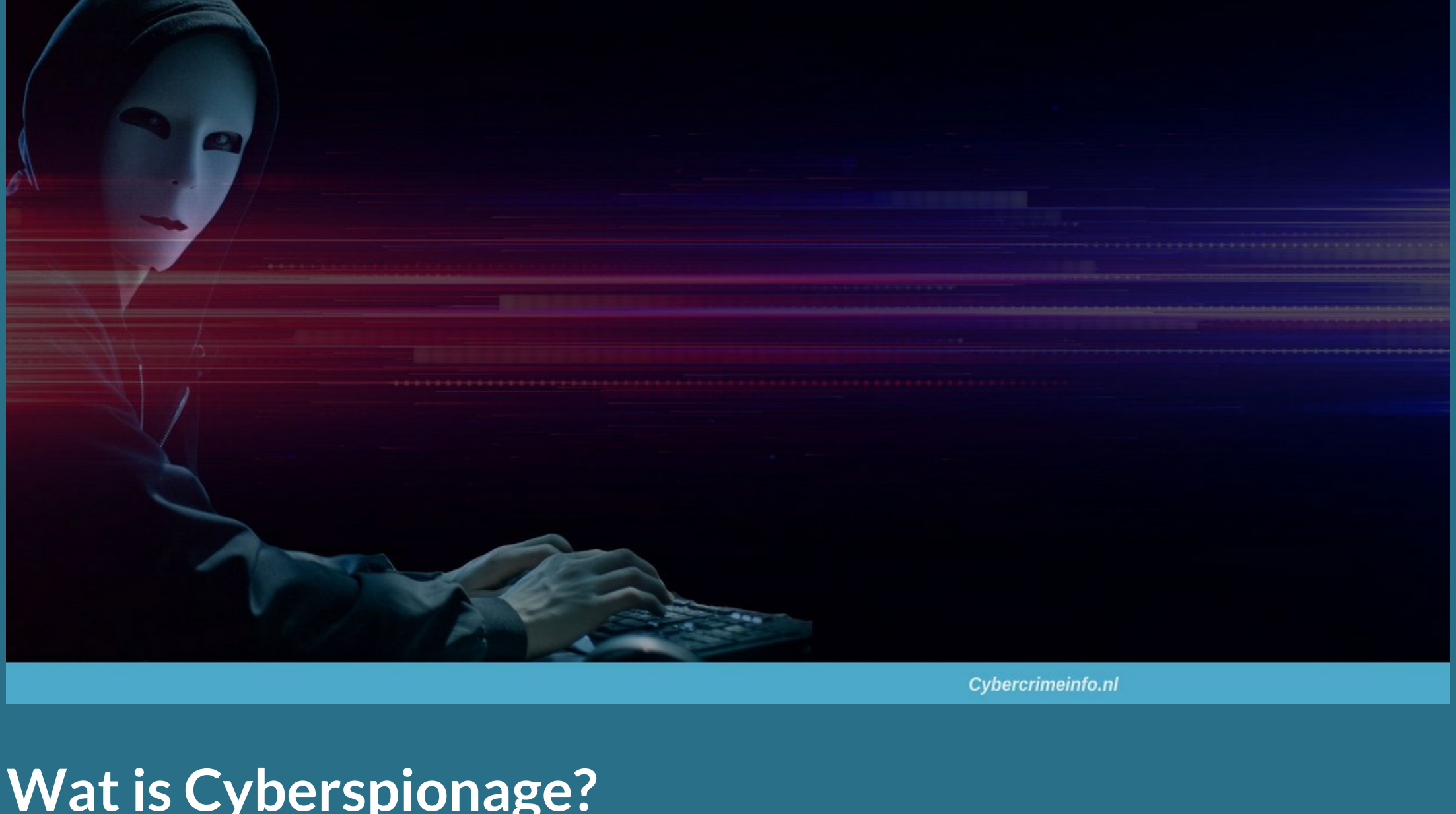
Dark Web

Operatie 'DisrupTor' op het darkweb leidt tot 179 aanhoudingen in 6 landen waaronder Nederland

Vandaag heeft een wereldwijd samenwerkingsverband van opsporingsdiensten de resultaten bekendgemaakt van een gezamenlijke operatie genaamd 'DisrupTor', die zich richtte op verkopers en kopers van illegale goederen op het darkweb. Deze operatie volgt op het offline halen van Wall Street Market in mei 2019, destijds de op een na grootste illegale online marktplaats op het darkweb. De criminelen achter deze marktplaats zijn vorig jaar geïdentificeerd en aangehouden door een internationaal opsporingsteam bestaande uit Duitse, Nederlandse en Amerikaanse rechercheurs. Deze actie leverde de opsporingsdiensten informatie op. Hiermee konden de verdachten geïdentificeerd worden die schuilgingen achter darkweb-accounts die gebruikt werden voor illegale activiteiten...

LEES MEER »

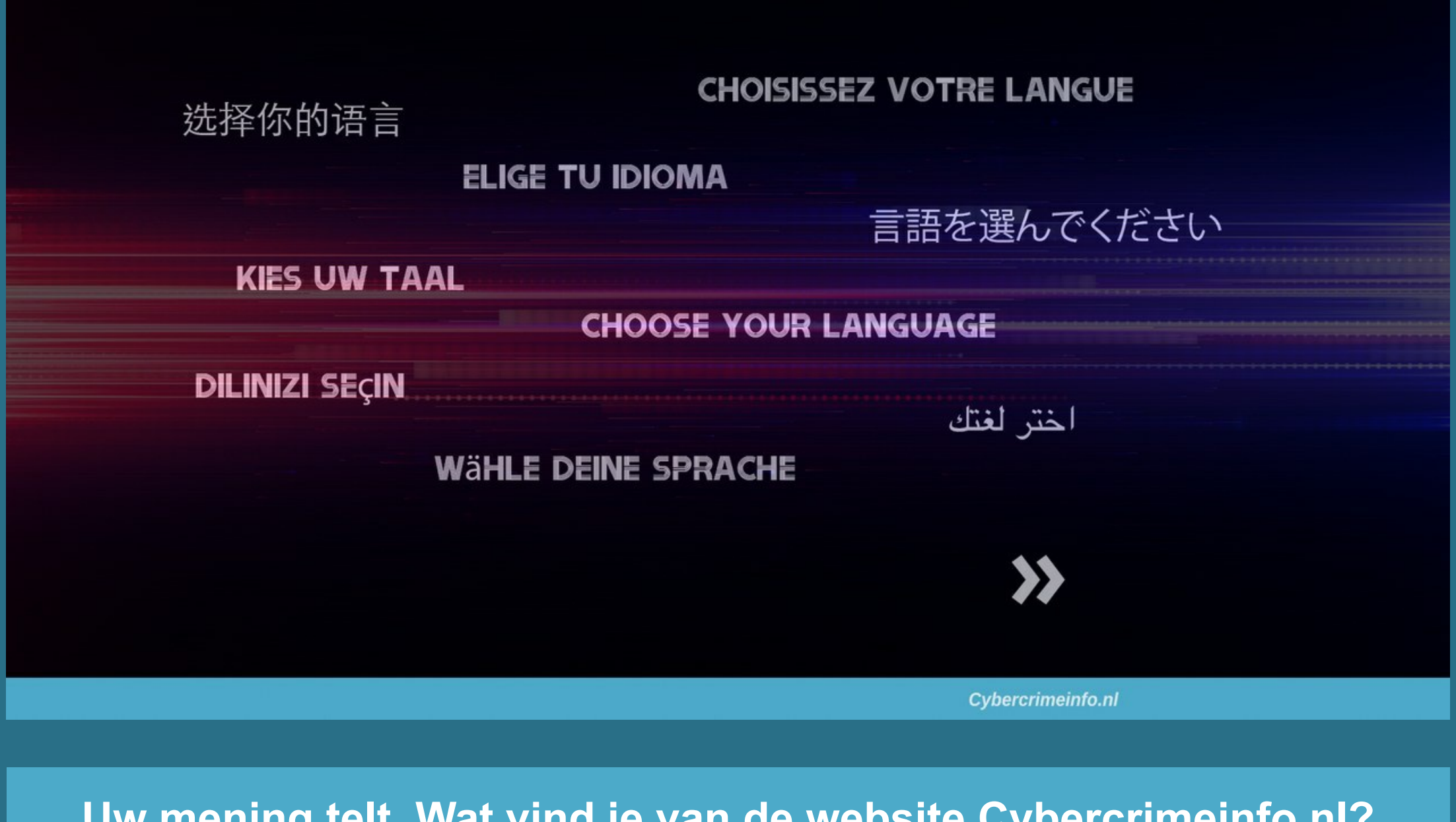
Wat is?



Wat is Cyberspionage?

Cyberspionage is wanneer inlichtingen verworven worden door gebruik te maken van digitale technologie. Deze inlichtingenverzameling richt zich grofweg op twee doelen. Staatsgeheimen, Economische geheimen...

LEES MEER »



Uw mening telt. Wat vind je van de website Cybercrimeinfo.nl?