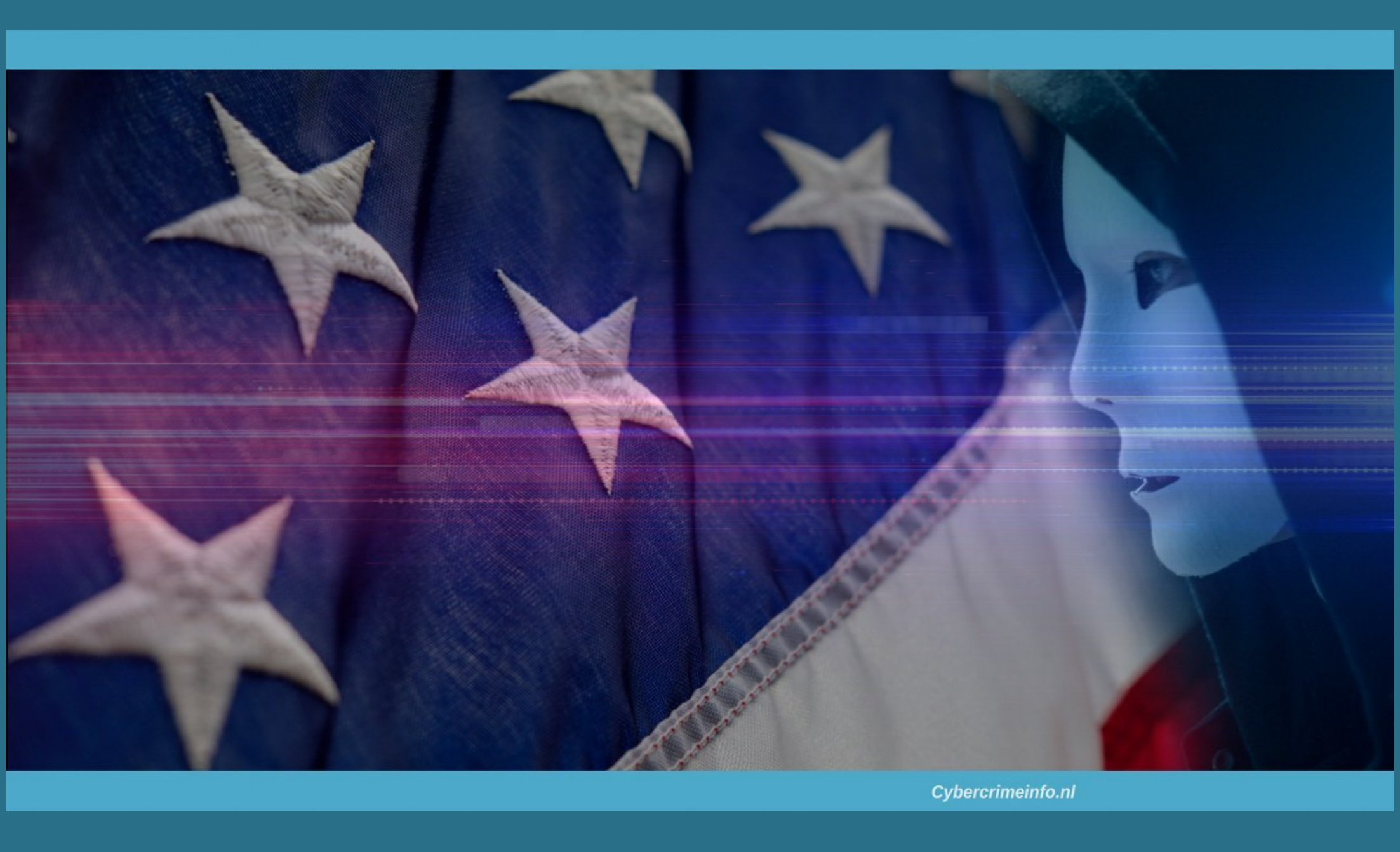
Nieuwsbrief 137 - Week 51-2020

Hackers zetten "achterdeurtje" open bij 'nieuwe update' van monitor en beheer software

Hackers zijn erin geslaagd om officiële software-updates van it-beheersoftware 'SolarWinds' van een backdoor te voorzien en zo overheden en bedrijven wereldwijd aan te vallen. Dat hebben SolarWinds, Microsoft, securitybedrijf FireEye en het Amerikaans CISA bekendgemaakt. De aanvallers wisten op deze manier ook bij FireEye binnen te dingen...

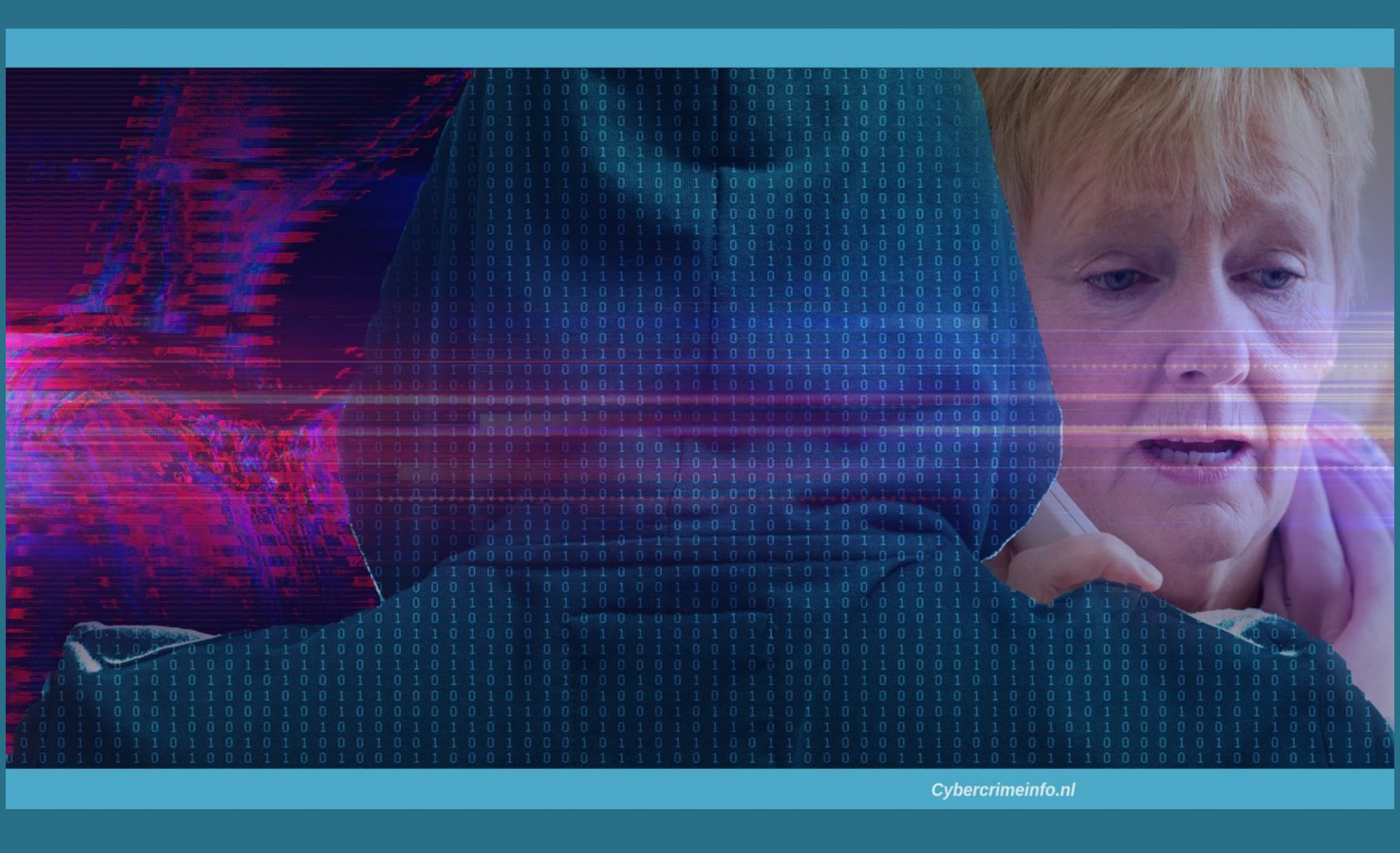
LEES MEER



Joe Biden geïnformeerd over de gevolgen van hack campagne die meerdere federale agentschappen heeft getroffen

Amerikaanse nationale veiligheidsfunctionarissen hebben het overgangsteam voor de verkozen president Joe Biden en Capitol Hill-assistenten geïnformeerd over de gevolgen van een vermoedelijke door de overheid gesteunde hack campagne die meerdere federale agentschappen heeft getroffen...

LEES MEER



Maatregelen tegen 'Spoofing' en 'Smishing'

Staatssecretaris Keijzer van Economische Zaken heeft maatregelen aangekondigd om telefoon spoofing en smishing tegen te gaan. Bij telefoon spoofing en smishing (sms-phishing) geven oplichters vaak een ander nummer door dan waarvandaan wordt gebeld of het bericht van afkomstig is. Slachtoffers kunnen daardoor denken dat het om een gesprek of bericht van de bank gaat...

LEES MEER

“Als een producent software heeft aangeboden die vervolgens niet voldoet aan de digitale veiligheidseisen, is hij mogelijk aansprakelijk op grond van wanprestatie”

Gebruikers kunnen de software-ontwikkelaar aansprakelijk stellen voor de schade die een hacker heeft toegebracht als blijkt dat de cybersecurity niet op orde is. Als het product niet voldoet aan de digitale veiligheidseisen, kan de fabrikant of verkoper van de software aangeklaagd worden op grond van wanprestatie. Er zijn echter wel de nodige juridische en economische barrières die het verhalen van de schade complex maken...

LEES MEER

Meer gepersonaliseerde aanvallen in 2021

Nu veel digitale initiatieven in een sneltreinvaart zijn gerealiseerd, zijn ook veel trends sneller dan verwacht ontwikkeld. Met die kennis in het achterhoofd hebben verschillende security-experts van 'CyberArk' zich toch gewaagd aan enkele voorspellingen in cybersecurity voor de komende periode...

LEES MEER

"De verdachte heeft zich schuldig gemaakt aan een geraffineerde vorm van fraude"

De rechtbank Den Haag heeft twee mannen van 24 en 27 jaar wegens qr-code fraude veroordeeld tot gevangenisstraffen van respectievelijk vier en vijf maanden. De mannen maakten meerdere slachtoffers in Den Haag en Tilburg. Het duo vroeg slachtoffers om hulp, bijvoorbeeld om een klein bedrag voor te schieten, zoals het betalen van een treinkaartje...

LEES MEER

Aanhoudingen na fraude met testen Covid-19

Een Gelders bedrijf in medische goederen is dit jaar slachtoffer geworden van internationale fraude. Het bedrijf dacht zaken te doen met hun vaste Koreaanse leverancier en had een grote hoeveelheid Covid-19 sneltesten besteld. Waarschijnlijk hebben criminelen toegang gekregen tot de mailwisselingen tussen de bedrijven...

LEES MEER

Ransomware weekoverzicht week 50-2020

De gemeente Hof van Twente is nog steeds aan het worstelen met het opstarten van de systemen na een ransomware aanval. Ransomware aanvallen richten zich op bedrijven, het onderwijs en de gezondheidszorg en leidde tot sluitingen van scholen. Hier het overzicht van nieuwe ransomware vormen en het nieuws van dag tot dag...

OVERZICHT

Digitale fraude, oplichting meldingen week 51-2020

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

Datalek nieuws en overzicht week 51-2020

Een datalek kan ernstige gevolgen hebben, soms worden levens totaal verwoest door dat er identiteit fraude mee gepleegd wordt.
Heb je een vermoeden van een datalek en is het nog niet gemeld of weet je niet als het gemeld is aan de 'Autoriteit persoons gegevens (AP)' laat het ons dan weten, want bij een datalek moet er snel gehandeld worden om mogelijke catastrofale gevolgen te voorkomen. O, ja, doe je dit liever anoniem dan kan dit hier

OVERZICHT

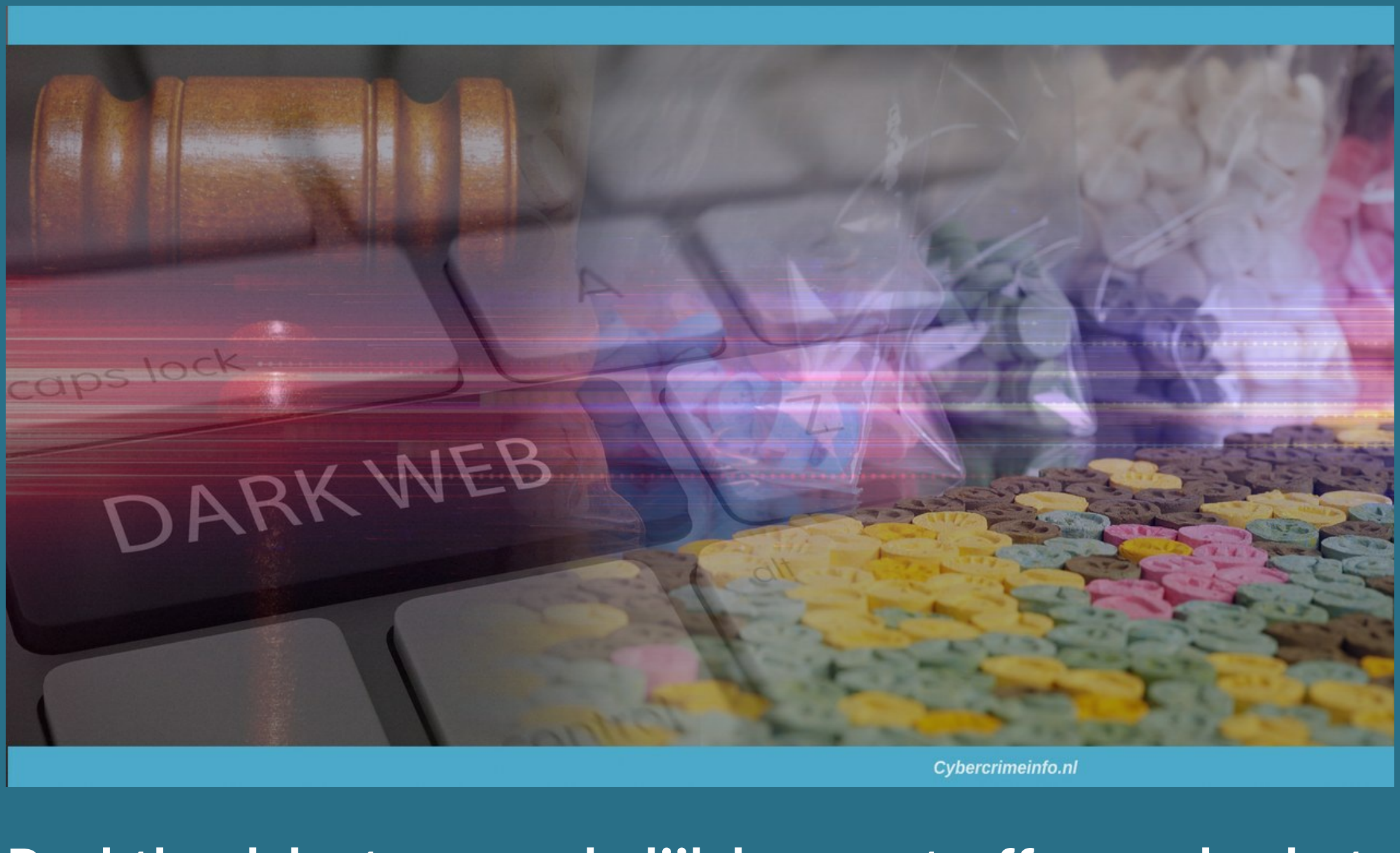
Gezochte Personen

Den Haag - Bankhelpdeskfraude

Op dinsdag 6 oktober werd het slachtoffer door een zogenaamde bankmedewerkster gebeld. Deze zogenaamde medewerkster vertelde dat de rekening van het slachtoffer werd geplunderd en dat ze haar geld moest overmaken naar zogenaamde 'veilige rekeningen'. In totaal heeft het slachtoffer onder valse voorwenselen voor ruim 16.000,- euro naar verschillende rekeningen overgemaakt...

LEES MEER

Dark Web

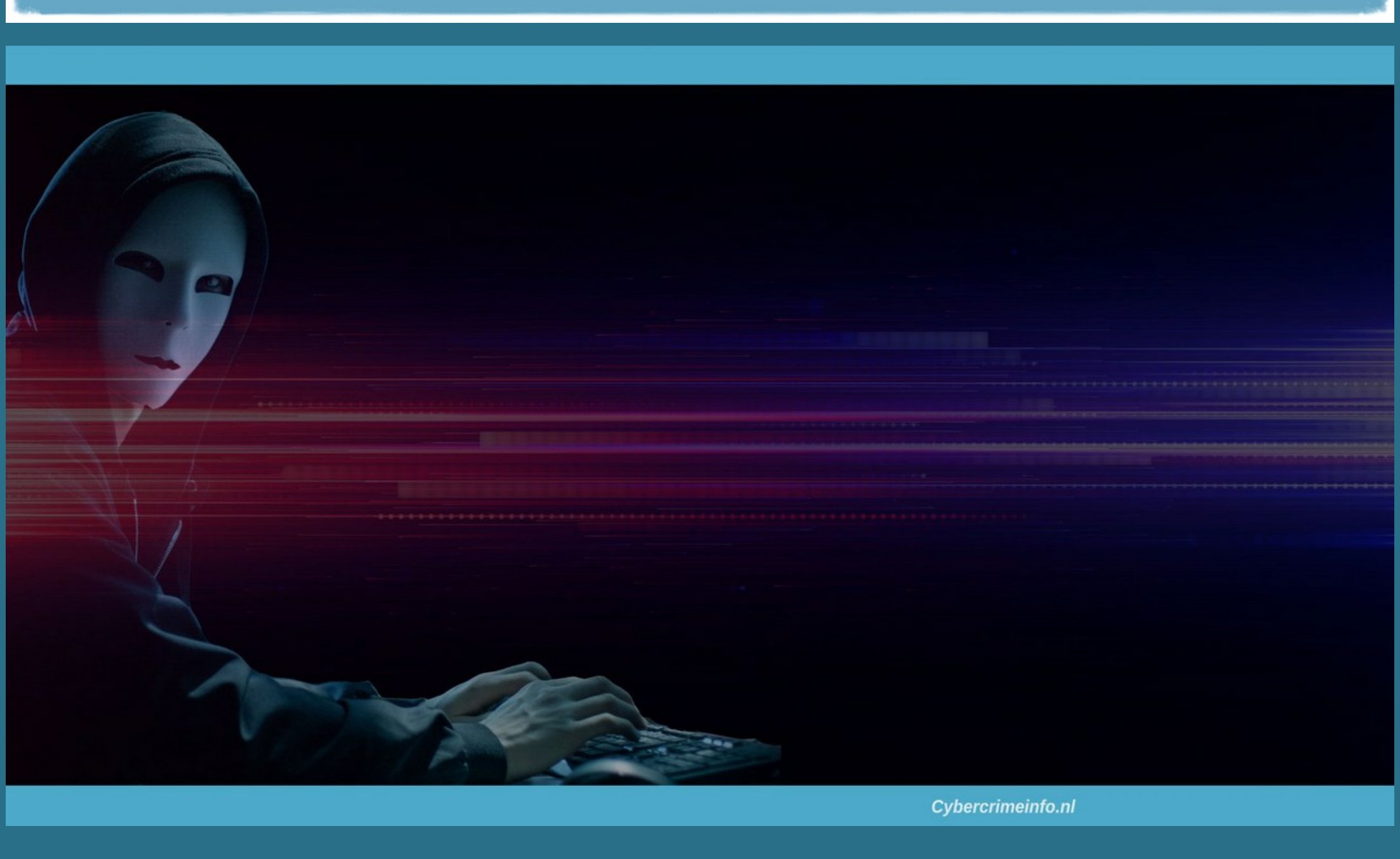


Rechtbank legt aanmerkelijk lagere straffen op dan het Openbaar Ministerie voor drugshandelaren op het Darkweb

De rechtbank in Rotterdam legt in een Boxtelse drugszaak aanmerkelijk lagere straffen op dan het Openbaar Ministerie had geëist. Hoofdverdachte Alex P. (33) krijgt 24 maanden cel, waarvan 14 maanden voorwaardelijk. Justitie had een straf van zeven jaar voor hem in petto...

LEES MEER

Wat is?



Wat is BEC fraude?

Business E-mail Compromise is een vorm van cybercrime die enigszins lijkt op phishing en focust op e-mailcontact binnen bedrijven. Zoals veel succesvolle vormen van fraude, focust BEC-fraude zich op het manipuleren van natuurlijk menselijk gedrag. We noemen dit ook wel ‘social engineering’. Criminelen spelen in op reacties die je als mens van nature hebt en buiten deze vervolgens uit. Hieronder beschrijven we twee populaire Business E-mail Compromise-methodes...

LEES MEER

De week in beeld