Nieuwsbrief 196 - Week 06-2022

Cybercriminelen richten zich op zero-day kwetsbaarheden en supply chain netwerken voor maximale impact

Vorige week verscheen het 'Ransomware Spotlight Year End Report' van Ivanti. Het rapport identificeerde 32 nieuwe ransomwarefamilies in 2021, waarmee het totaal op 157 komt, een toename van 26 procent ten opzichte van het voorgaande jaar.

Lees verder

Stijging van ruim 47 procent met nieuwe malware

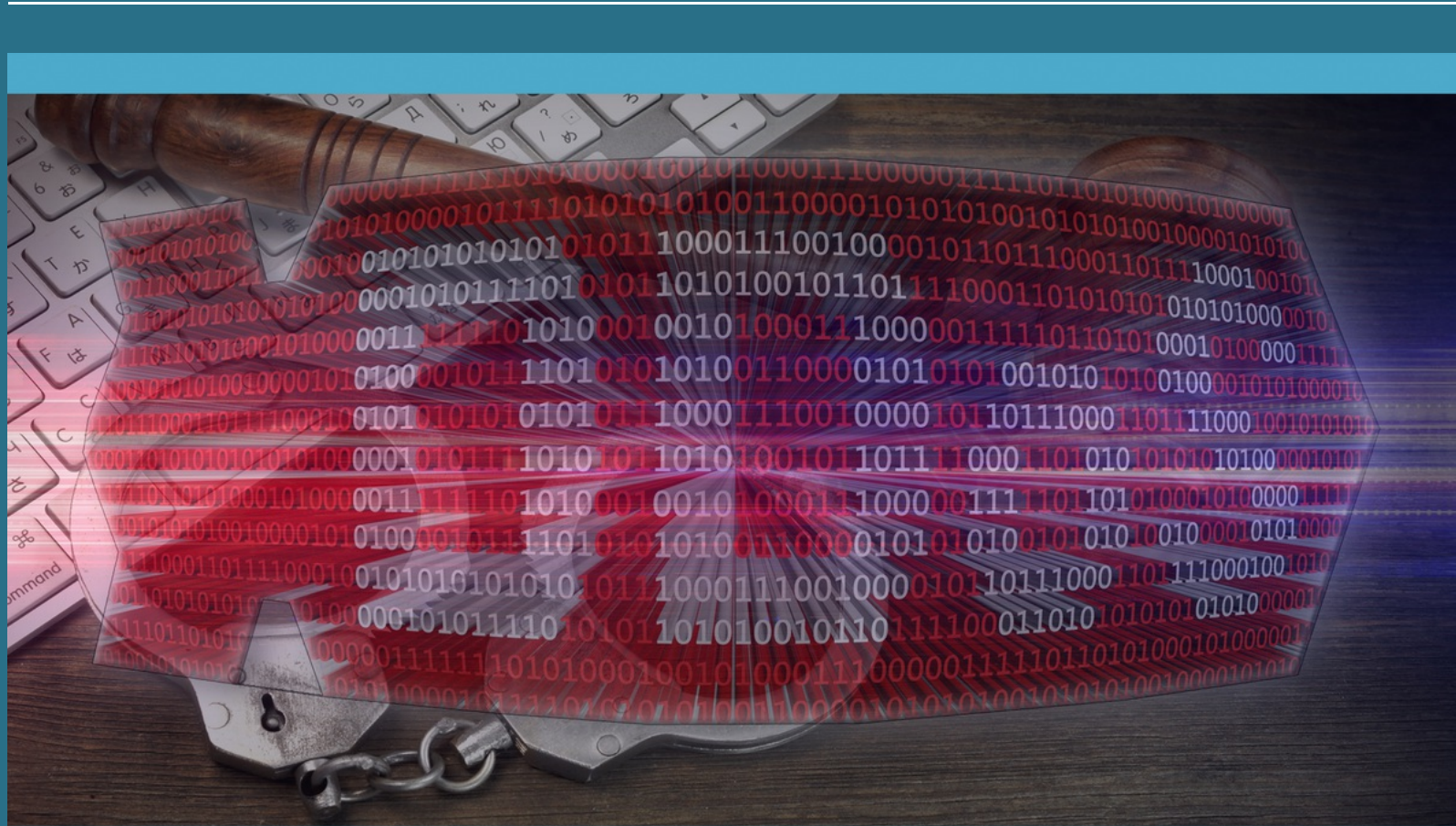
Er komen steeds meer verschillende soorten malware samples op de markt blijkt uit een analyse van G DATA CyberDefense. In totaal werden er vorig jaar meer dan 23,7 miljoen verschillende soorten malware samples geïdentificeerd. Dit staat gelijk aan bijna 65.000 nieuwe varianten malware per dag, oftewel 45 nieuwe aanvalsvectoren per minuut. Vergeleken met 2020 is dit een stijging van ruim 47 procent.

Lees verder

“Staatssecretaris moet focus onder meer op security en infrastructuur leggen”

Het nieuwe kabinet werd een kleine maand geleden beëdigd. In dat nieuwe kabinet zit voor het eerst ook een staatssecretaris voor Koninkrijksrelaties en Digitalisering, Alexandra van Huffelen, die de digitale ambities van het nieuwe kabinet coördineert. Maar wat moeten die ambities eigenlijk zijn? AG Connect vroeg het de ICT-branche.

Lees verder



Een onbereikbare website het is de nachtmerrie van elke online ondernemer

Op die angst speelde een 25-jarige verdachte uit Veenendaal op slinkse wijze in. Hij wordt ervan verdacht DDOS-aanvallen uitgevoerd te hebben op meer dan twintig websites van internetondernemingen, waarbij klanten online bijvoorbeeld bloemen, meubels of verf kunnen bestellen. Na de eerste aanval eiste de verdachte betalingen in bitcoins van de getroffen bedrijven. Daarmee zouden ze nieuwe aanvallen – en een langdurig onbereikbare website – kunnen voorkomen (RDDOS).

Lees verder

“Het gaat niet om één of enkele goede maatregelen, het gaat om het geheel”

Hoe zet je een goed cybersecuritybeleid op? Sándor Incze, CISO bij CM.com, legt stap voor stap uit wat hij gedaan heeft om CM.com tegen cybercriminelen te beschermen. “Het gaat niet om één of enkele goede maatregelen”, zegt hij. “Het gaat om het geheel.” Sándor vergelijkt cybersecurity met het computerspel bubble shooter dat in de jaren ’90 populair was. Dit spel bestaat uit een veld met gekleurde ballen. Als speler heb je de mogelijkheid om telkens een andere kleur ballen weg te schieten.

Lees verder

Bankieren en betalen via de smartphone is dat eigenlijk nog wel veilig?

Mobiel bankieren is inmiddels bij alle banken mogelijk. Handig en snel, want card-readers en TAN-codes zijn dan overbodig. U kunt internetbankieren en zelfs contactloos afrekenen met uw smartphone. Maar is het ook veilig? En hoe zit het met contactloos betalen met de pinpas?

Lees verder

Hoe beschermt u uw iPhone of Android-smartphone tegen spyware

Wellicht het grootste verhaal van 2021 – een onderzoek door The Guardian en 16 andere mediaorganisaties, gepubliceerd in juli – suggereerde dat meer dan 30.000 mensenrechtenactivisten, journalisten en advocaten over de hele wereld het doelwit van 'Pegasus' kunnen zijn geweest.

Lees verder

Overzicht cyberaanvallen week 05-2022

Cyberaanval legt aanvoer van bananen en kiwi’s lam in Antwerpse haven, olieterminal Terneuzen kampt met laad- en losproblemen na cyberaanval en een blik op de nieuwe Sugar ransomware die zich richt op consumenten. Hier het overzicht van afgelopen week en het nieuws van dag tot dag.

Bekijk het weekoverzicht

Phishing, nepshop en fraude meldingen week 06-2022

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?!, Radar, Kassa, of Fraudehelpdesk dan weten, want Samen bestrijden we cybercrime / digitale fraude. Liever anoniem? Klik dan hier. Ben je slachtoffer geworden van oplichting doe dan 'altijd' aangifte bij de politie.

Bekijk het weekoverzicht

Datalek nieuws en overzicht week 06-2022

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.

Bekijk het weekoverzicht

Overijssel - Bankhelpdesk fraude

Wie herkent deze personen?

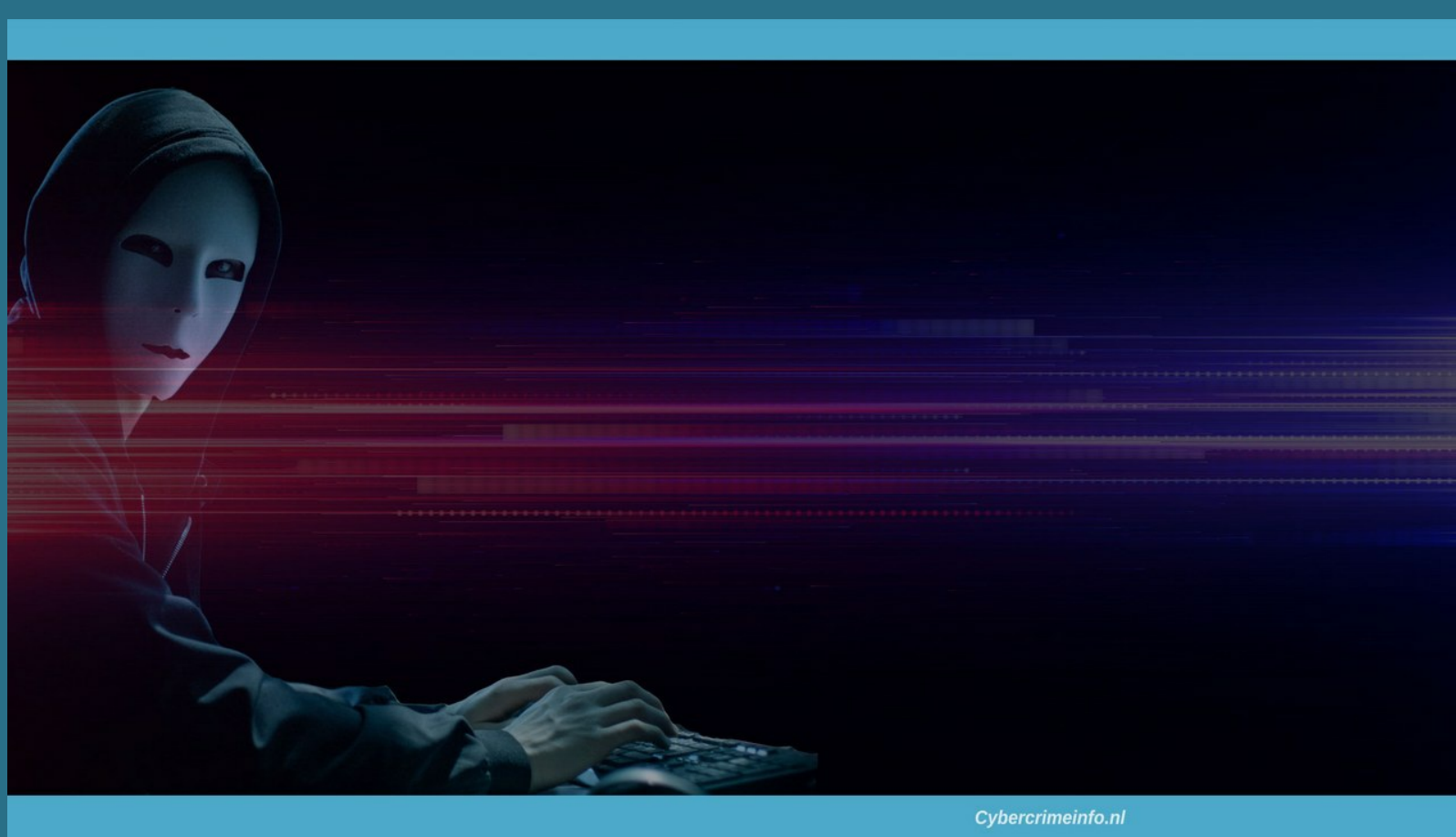
In de afgelopen periode werd vaak aangifte gedaan van oplichting door zogenaamde bankmedewerkers. De daders deden zich voor als bankmedewerker en wisten zo het vertrouwen van de slachtoffers te winnen. Op die manier kregen ze toegang tot pinpassen en bankgegevens. De schade loopt regelmatig op tot in de duizenden euro’s. Ook in de volgende drie zaken hebben we te maken met deze vorm van oplichting. Herkent u een van de verdachten? Geef het door aan ons.

Lees verder

Zaak 26Hain: “What’s up pedos? :)”

What’s up pedos?” gevolgd door een smiley. Zo begon de nu 38-jarige verdachte uit Tilburg, die afgelopen woensdag terechtstond in kinderpornozaak '26Hain', geregeld zijn chat-gesprekken op kinderpornosites op het darkweb. Het Landelijk Parket van het Openbaar Ministerie (OM) eiste in de rechtbank Rotterdam 48 maanden gevangenisstraf, waarvan 8 voorwaardelijk en een proeftijd van 5 jaar met reclasseringstoezicht en psychische behandeling. Het OM verdenkt hem van deelname aan een criminele organisatie in de sleutelpositie van administrator en moderator op diverse kinderpornosites op het darkweb.

Lees verder



Wat is "RDDoS"?

Hoe goed ben jij inmiddels op de hoogte van cybercrime begrippen en vormen?

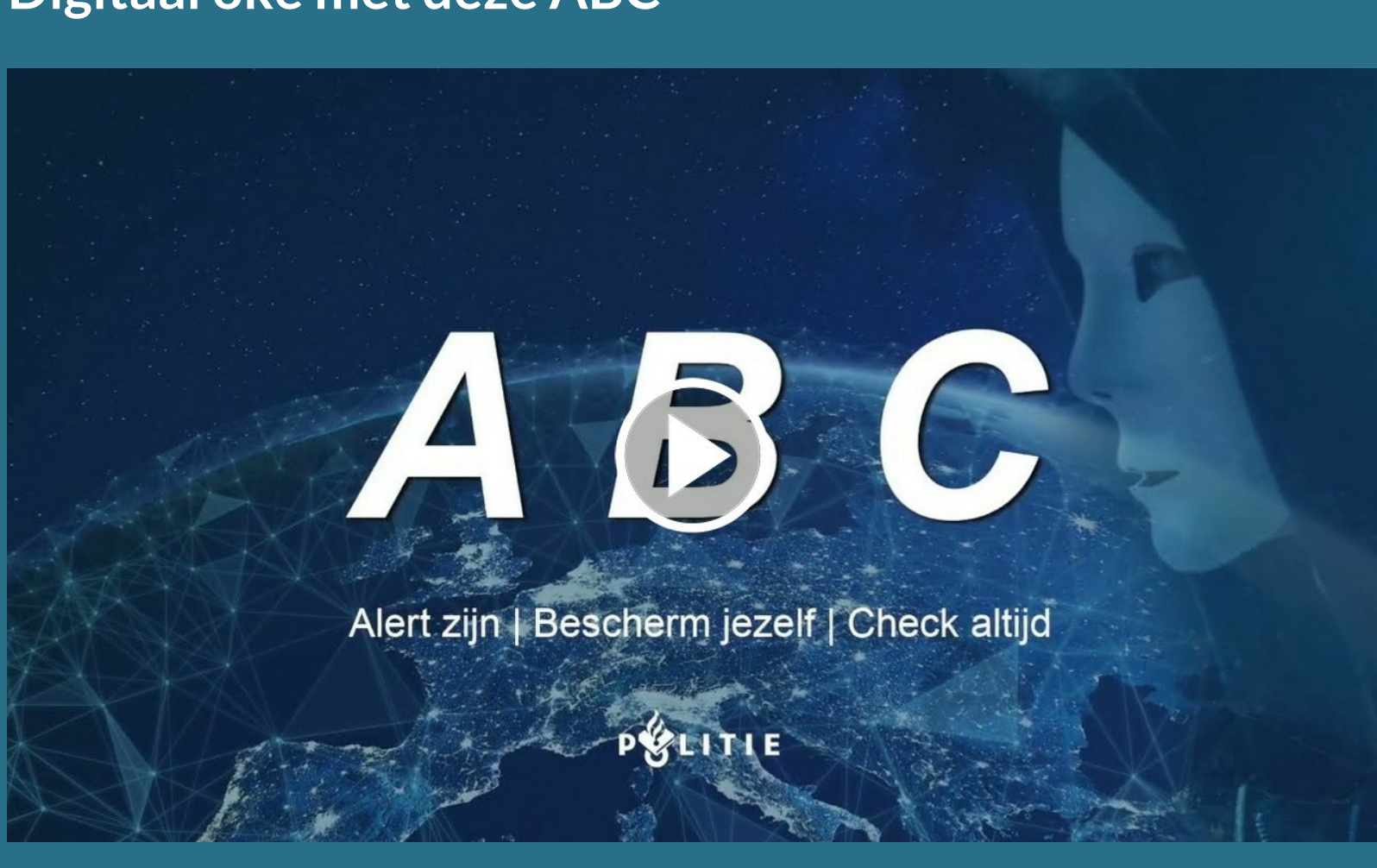
Weet jij wat 'RDDoS' is?
Nee, geen nood, hier kun je het lezen.

Wil je meer vormen en begrippen leren kennen?

Vernieuwde pagina 'Van A tot Z' (nu nog overzichtelijker)

Van A tot Z

Digitaal oké met deze ABC



Meer weten?

Share Tweet Share Pinterest

Wekelijks programma Cybercrimeinfo

Dagelijks nieuwe artikelen op Cybercrimeinfo, een overzicht van de actuele aanvallen en wekelijks terugkerende onderwerpen, hier het programma:

- Ma: Cyberaanvallen / ransomware weekoverzicht
- Di: Gezochte persoon cybercrime / digitale fraude
- Za: Darkweb gerelateerd bericht
- Zo: Oplichting en datalekken weekoverzicht
- Op zondagavond om 19:00 wordt de wekelijkse nieuwsbrief verstuurd.

Lees verder

CYBERCRIMEINFO.NL

Mag ik foto's of plaatjes die ik op Cybercrimeinfo vind gebruiken voor mijn site of blog?

Mag ik foto's of plaatjes die ik op Cybercrimeinfo vind gebruiken voor mijn site of blog? Het korte antwoord is Ja.
Maar hoe zit dit eigenlijk met rechten en het gebruiken van foto's die je op Internet vindt?

Lees verder

Steun Cybercrimeinfo zodat we kunnen blijven bestaan

Om deze website te runnen en iedereen te kunnen blijven voorzien van het laatste nieuws, tips en tricks over digitale criminaliteit, zijn wij op zoek naar donateurs. Hiervan kunnen we onder andere nieuwe apparatuur aanschaffen, want deze hele site draait op vrijwilligers. Kortom, wij kunnen niet zonder jouw steun! Help je mee in de strijd tegen cybercrime?
Iedere donatie, hoe klein ook, is van harte welkom. Alvast bedankt namens het hele team van Cybercrimeinfo.

Doneren kan al vanaf 5 euro!

Doneer