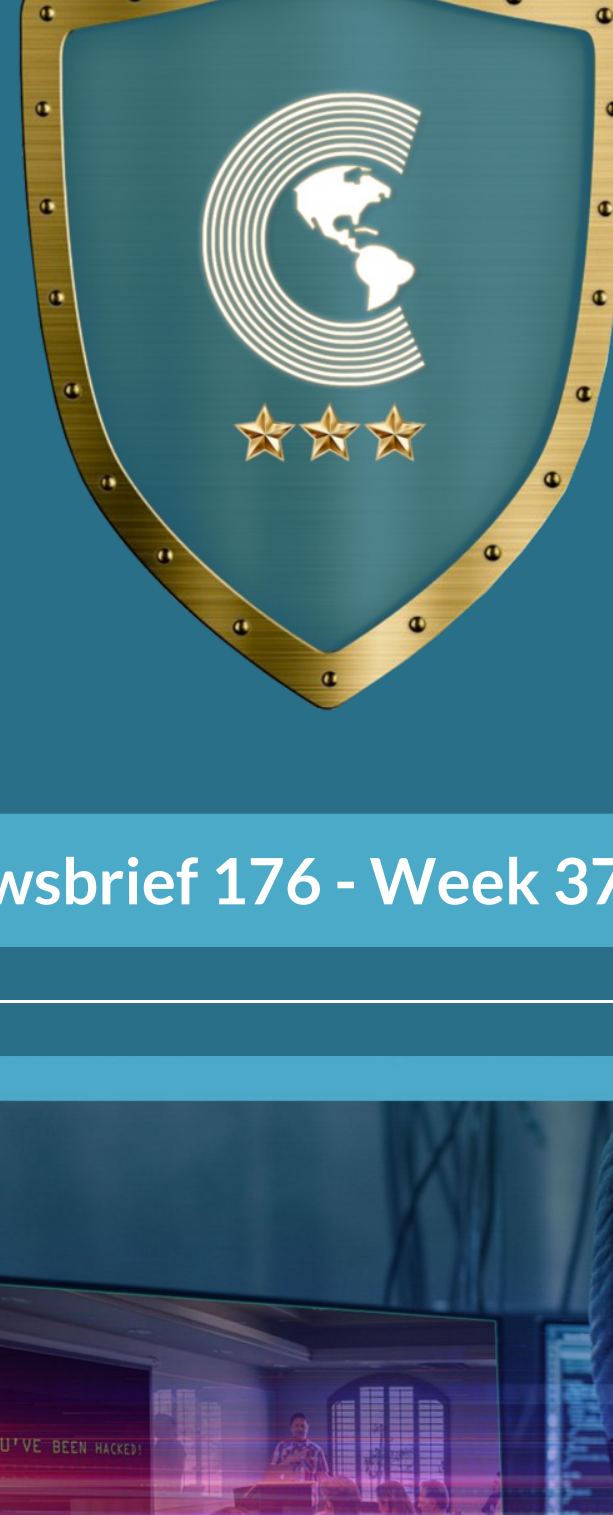




Nieuwsbrief 176 - Week 37-2021



Cybercrimeinfo.nl

Cybercriminelen van Vice Society publiceren gestolen data op het darkweb van ROC Mondriaan

De cybercriminelen van 'Vice Society' die verantwoordelijk zijn voor de cyberaanval op ROC Mondriaan, hebben de gegevens die zij hebben gestolen op het darkweb geplaatst. De aanvallers vroegen om losgeld, maar de scholengemeenschap weigerde deze te betalen.

[Lees verder](#)



Cybercrimeinfo.nl

Apple: "Installeer per direct de beveiligingsupdate"

Software- en elektronica-gigant Apple roept gebruikers van iPhones, MacBooks, iPads en horloges op om zo spoedig mogelijk een beveiligingsupdate te installeren. Dat heeft alles te maken met een ernstig beveiligingslek in de iMessage-app: het was mogelijk om zonder enige interactie van de gebruiker de zogenaamde Pegasus-spyware te installeren. Daarmee kunnen foto's en e-mails worden gestolen, maar ook de microfoon en camera kunnen op afstand worden ingeschakeld.

[Lees verder](#)



Cybercrimeinfo.nl

81% van de Nederlandse zorginstellingen lopen risico op e-mailfraude

Het is inmiddels de norm dat afspraken voor de huisarts, het ziekenhuis en een vaccinatie online worden geboekt. En nu het digitale coronaspoort definitief wordt ingevoerd als toegangsbewijs voor allerlei diensten, is cybersecurity nog nooit een belangrijker thema geweest voor de zorgsector.

[Lees verder](#)



Cybercrimeinfo.nl

Overheid gaat bedrijven waarschuwen bij gevaar cyberaanvallen

Het Digital Trust Center (DTC) gaat vanaf maandag 13 september op beperkte schaal relevante dreigingsinformatie proactief delen met het bedrijfsleven. Ondernemingen en organisaties die geen onderdeel uitmaken van de kritische infrastructuur, krijgen vanaf vandaag informatie over acute kwetsbaarheden en digitale dreigingen. De overheid kijkt of ze op deze manier het bedrijfsleven weerbaarder kan maken tegen hackers.

[Lees verder](#)



Cybercrimeinfo.nl

74% van de ondervraagde organisaties is de afgelopen 12 maanden slachtoffer geworden van ten minste één ransomware aanval

Barracuda heeft het rapport 'The state of network security in 2021' gepubliceerd. Voor dit rapport zijn 750 IT-beslissers over de hele wereld ondervraagd die verantwoordelijk zijn voor de netwerken, de publieke clouds en de security van hun organisatie. Dit heeft inzichten opgeleverd in cloudadoptie, thuiswerken, securityproblemen en andere uitdagingen rond securityrisico's.

[Lees verder](#)



Cybercrimeinfo.nl

Waarom je apparaten moet updaten om cybercriminelen buiten de deur te houden

Houd je aan simpele basismaatregelen en het gros van de hackers vormt geen gevaar meer, schrijven twee beveiligingsmedewerkers van computergigant Microsoft. Een van die maatregelen is simpel: update je programma's zo snel mogelijk, in ieder geval binnen 48 uur. Misschien herken je het: Op een ongelegen moment verschijnt er een melding op het beeldscherm. Er is een nieuwe update beschikbaar. Je kunt gelijk op 'uitvoeren' klikken, maar dan kun je niet verder met waar je mee bezig was. Download je 'm gelijk, of wacht je op een later moment?

[Lees verder](#)

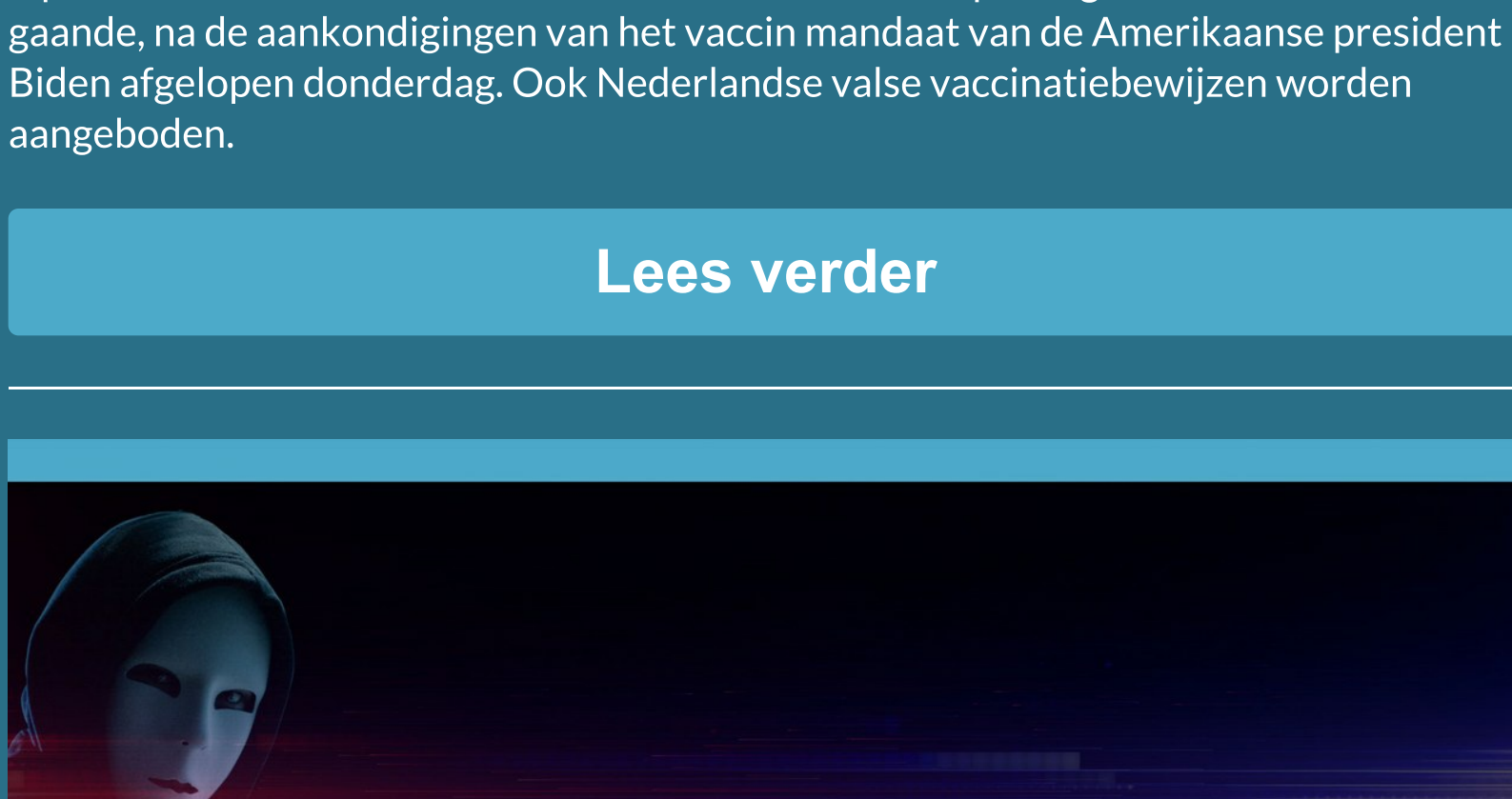


Cybercrimeinfo.nl

Universele decryptor voor slachtoffers 'REvil cybercriminelen' beschikbaar

Cybersecuritybedrijf Bitdefender heeft een universele decoderingssleutel ontwikkeld voor iedereen die in het verleden slachtoffer is geworden van REvil. Deze decryptor werkt niet alleen voor de supply chain attack op Kaseya: bedrijven en organisaties die vóór 13 juli slachtoffer waren van de Russische hackersgroep, kunnen de sleutel gebruiken om hun bestanden te ontgrendelen. Ondanks dat de decryptor gratis en voor niets beschikbaar is, waarschuwen securityexperts om voorzichtig te zijn.

[Lees verder](#)



Cybercrimeinfo.nl

Overzicht cyberaanvallen week 36-2021

Ransomwaregroep cyberaanhuwt slachtoffers om niet naar politie te stappen, hacker zet gestolen gegevens online omdat hogeschool van Arnhem en Nijmegen weigert te betalen en hoe Groove Gang de Ransomware-as-a-Service-markt opschudt om partners te versterken. Hier het overzicht van afgelopen week en het nieuws van dag tot dag.

[Bekijk het weekoverzicht](#)

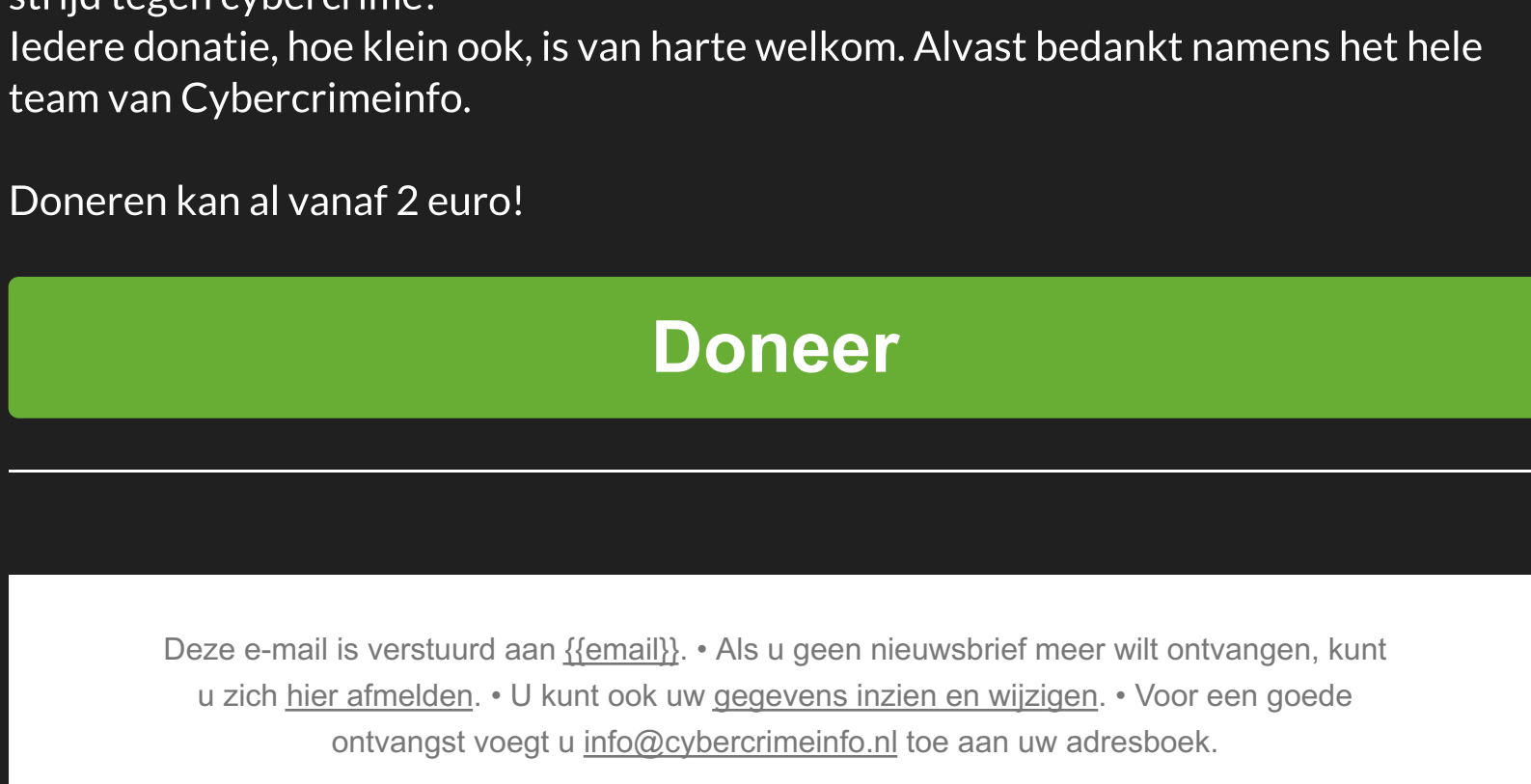


Cybercrimeinfo.nl

Phishing, nepshop en fraude meldingen week 37-2021

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 [Opgelet.nl](#), Radar, Kassa, of Fraudehulpdesk 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](#)



Cybercrimeinfo.nl

Datalek nieuws en overzicht week 37-2021

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 persoonsgegevens (AP)' laat het ons dan weten, want bij een datalek moet er snel gehandeld worden om mogelijke catastrofale gevolgen te voorkomen.

[Bekijk het weekoverzicht](#)

Cybercrimeinfo.nl

Nieuw-Vennep - Pinfraude na spoofing

Een hoogbejaarde vrouw uit de Haarlemmermeer werd de dupe van #spoofing op vrijdag 23 juli. De vrouw werd aan het eind van de middag op haar vaste telefoon gebeld door iemand die zich voordeed als medewerkster van een bank, met het verhaal dat haar bankrekening zou zijn gehackt.

[Lees verder](#)

Cybercrimeinfo.nl

Zwarte markt voor valse vaccinatie certificaten vertienvoudigd

Op de zwarte markt voor valse vaccinatiecertificaten op Telegram is een hausse gaande, na de aankondigingen van het vaccin mandaat van de Amerikaanse president Biden afgelopen donderdag. Ook Nederlandse valse vaccinatiebewijzen worden aangeboden.

[Lees verder](#)

Cybercrimeinfo.nl

Wat is Deep Fake?

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

Weet jij wat 'Deep Fake' is?

Nee, geen nood, [hier kun je het lezen](#).

Wil je meer vormen en begrippen leren kennen?

[Van A tot Z](#)

Cybercrimeinfo.nl

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](#)

Cybercrimeinfo.nl

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 2 euro!

[Doneer](#)

Cybercrimeinfo.nl

Deze e-mail is verstuurd aan [\(email\)](#). • Als u geen nieuwsbrief meer wilt ontvangen, kunt u zich [hier afmelden](#). • U kunt ook uw [gegevens inzien en wijzigen](#). • Voor een goede ontvangst voegt u [info@cybercrimeinfo.nl](#) toe aan uw adresboek.

Laposta