Nieuwsbrief 143 - Week 04-2021

Cybercrimeinfo.nl

Waarom online surveillance anno 2021 een permanentere rol moet krijgen binnen de opsporingsdiensten

Het voorkomen van cybercriminaliteit is een belangrijke overheidstaak. De overheid is daarnaast ook verantwoordelijk voor de openbare orde en veiligheid, die tegenwoordig steeds vaker in het geding komt. Steeds vaker worden in de digitale wereld oproepen gedaan tot crimineel gedrag, zoals nu met de rellen in verschillende steden...

LEES MEER

Cybercrimeinfo.nl

Betalen of een permanent bombardement aan DDoS-aanvallen

Het is de nachtmerrie van ieder bedrijf: servers, netwerken en zakelijke IT zijn niet beschikbaar vanwege een cyberaanval. Cybercriminaliteit maakt deel uit van het dagelijkse digitale leven en is een bloeiende economie geworden. De gevolgen voor getroffen bedrijven zijn kostbaar. Een recent onderzoek van Allianz-dochter AGCS laat zien hoe duur cybercriminaliteit kan zijn voor bedrijven...

LEES MEER

Cybercrimeinfo.nl

Gebruik je Apple iPhone en ben je interessant voor Statelijke actoren (hackers)? Update dan onmiddellijk!

Apple heeft een beveiligingsupdate uitgegeven om drie zero-day-kwetsbaarheden te dichten. Omdat Apple gelooft dat anonieme cybercriminelen deze kwetsbaarheden al benutten, raadt het bedrijf alle iOS- en iPadOS-gebruikers aan om hun besturingssystemen te updaten...

LEES MEER

Cybercrimeinfo.nl

Internationale politieoperatie 'LadyBird' geslaagd

Met het uit de lucht halen van servers achter de agressieve malware Emotet is een belangrijke slag geslagen in de strijd tegen cybercriminaliteit: de Emotet-besmetting is niet langer actief op de computers van ruim 1 miljoen slachtoffers wereldwijd. Het uit de lucht halen gebeurde deze week in de omvangrijke internationale politieoperatie LadyBird...

LEES MEER

Cybercrimeinfo.nl

Twee mannen aangehouden die persoonsgegevens aanboden op Telegram

De politie heeft zaterdag 23 januari 2021 twee mannen aangehouden op verdenking van computervredebreuk (hacking). De mannen worden verdacht van het te koop aanbieden van persoonsgegevens uit de systemen die de GGD gebruikt voor de Covid-19 testen. Op vrijdag 22 januari kregen politie en OM meldingen van de GGD dat er op Telegram persoonsgegevens uit een GGD-systemen te koop zouden worden aangeboden. Hierop startte het cybercrime team van de politie Midden-Nederland direct een onderzoek...

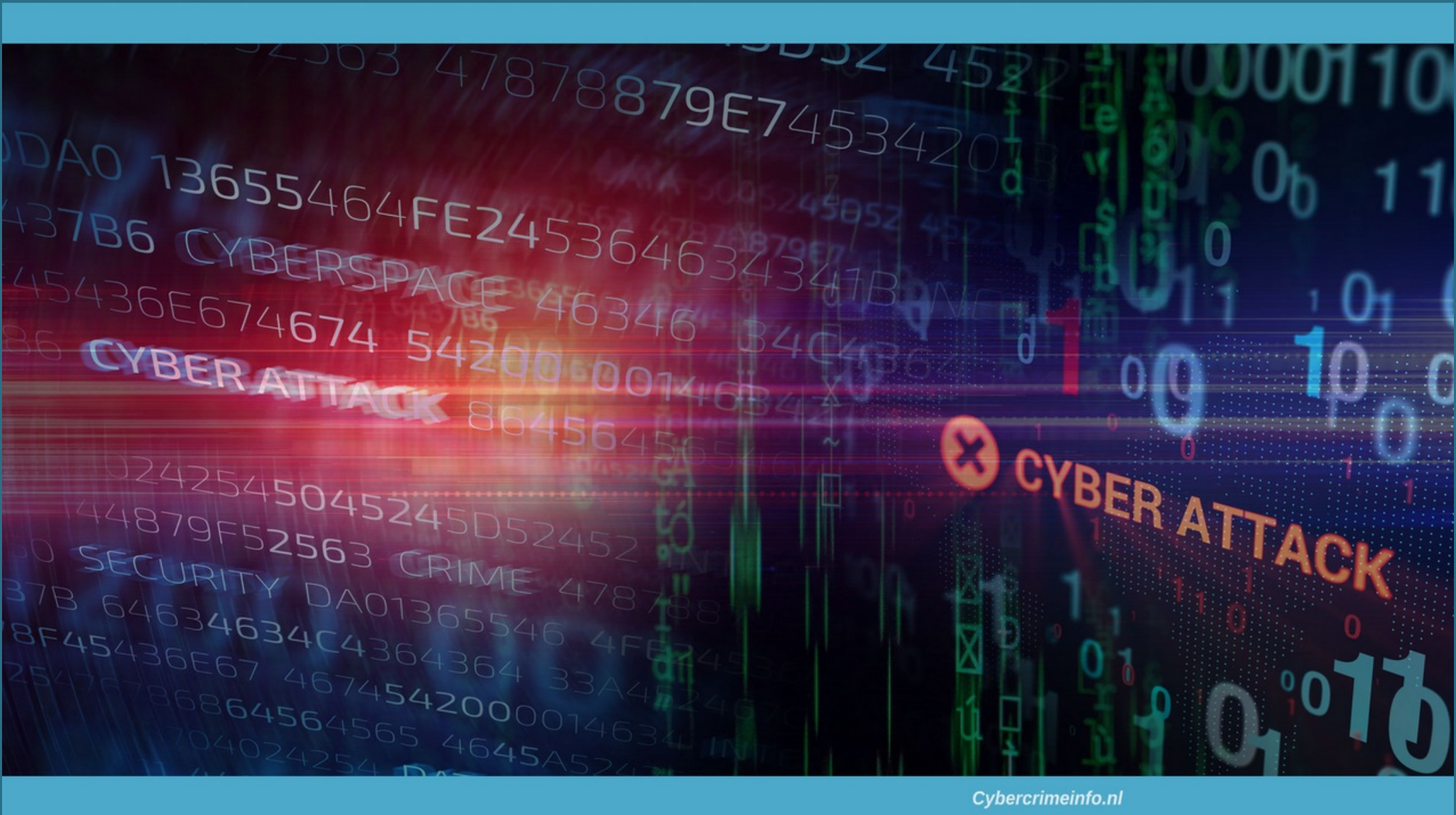
LEES MEER

Cybercrimeinfo.nl

Hackers hebben maar twee uur nodig om het hele bedrijfsnetwerk over te nemen

Er komt mogelijk een nieuwe golf van ransomware-aanvallen aan. Daarvoor waarschuwt het Nederlandse beveiligingsbedrijf Northwave, dat vaak slachtoffers van dat soort aanvallen bijstaat. Het Nederlandse beveiligingsbedrijf waarschuwt ons voor een nieuwe golf aan ransomware-aanvallen. Dit jaar heeft het bedrijf al meerdere phishingmails voorbij zien komen die zogenaamd afkomstig zijn van DocuSign...

LEES MEER



Cybercrimeinfo.nl

Dreiging 'supply chain-aanvallen' wordt steeds groter

De dreiging van digitale 'supply chain-aanvallen' wordt steeds groter omdat partijen binnen hun keten, door toenemende digitalisering, globalisering en outsourcing, steeds meer informatie met elkaar delen. Dat is nodig om de keten efficiënt te kunnen laten functioneren, maar creëert ook risico's...

LEES MEER

Cybercrimeinfo.nl

Ransomware weekoverzicht 03-2021

Amerikaans district betaalt losgeld na ransomware-aanval, Schotse milieu regelgever getroffen door 'aanhoudende' ransomware aanval, en Intel voegt op hardware gebaseerde ransomware detectie toe aan 11e generatie CPU's. Hier het overzicht van de nieuwste ransomware vormen en het nieuws van dag tot dag...

OVERZICHT

Cybercrimeinfo.nl

Digitale fraude, oplichting meldingen week 04-2021

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 Opgelicht?! of Fraudehelpdesk dan weten want Samen bestrijden we cybercrime. Liever anoniem? Klik dan hier

OVERZICHT

Cybercrimeinfo.nl

Datalek nieuws en overzicht week 04-2020

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

Cybercrimeinfo.nl

Rijssen - Vrouw slachtoffer van spoofing

Een bejaarde vrouw werd op 27november gebeld door iemand die zich voordeed als medewerker van haar bank. De persoon aan de telefoon overtuigde de vrouw om haar bankpas door te knippen en de pincode in te spreken...

LEES MEER

Dark Web

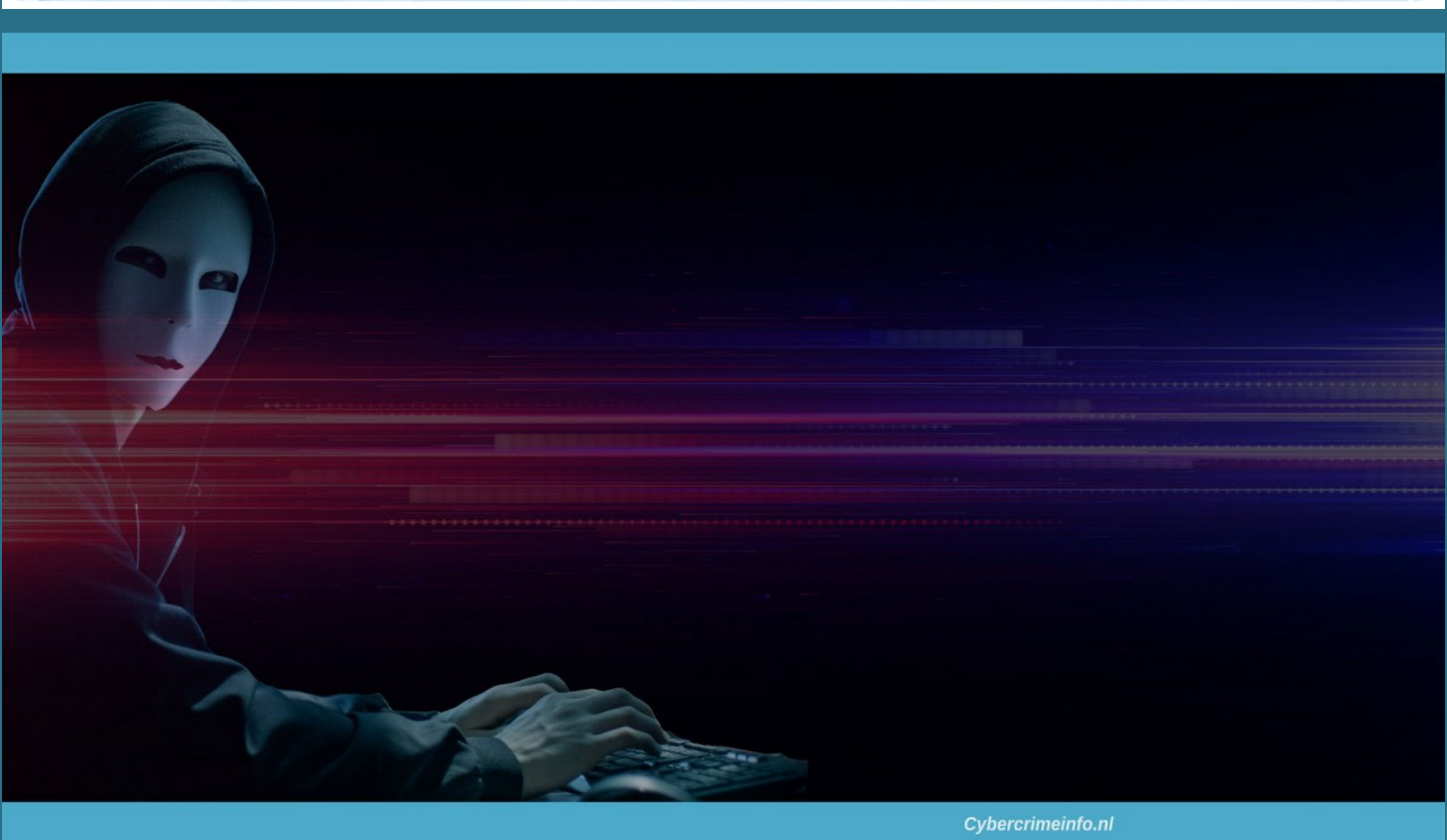
Cybercrimeinfo.nl

Zes aanhoudingen in darkweb onderzoek 'Ringwood'

De Politie heeft afgelopen dinsdag zes personen aangehouden die verdacht worden achter de darkweb market 'DutchMasters' te zitten. DutchMasters hield zich op het darkweb bezig met de productie, verkoop en distributie van harddrugs. De totale omzet van DutchMasters wordt geschat op tientallen miljoenen euro's...

LEES MEER

Wat is?



Cybercrimeinfo.nl

Wat is een supply chain aanval?

Een supply-chain-aanval is een aanval waarbij een bedrijf of individu wordt getroffen door een aanval die vanuit een leverancier (een 'supplier') wordt uitgevoerd. In veel gevallen is dat een aantrekkelijke manier van malware verspreiding of spionage...

LEES MEER

De week in beeld

Cybercrimeinfo.nl