Nieuwsbrief 123 - Week 37-2020

Visa-creditcard, waarschuwt webshops voor gevaarlijke malware

'Visa' heeft webwinkels gewaarschuwd voor een nieuwe malware die creditcardgegevens van klanten probeert te stelen. De malware wordt "Baka" genoemd en is volgens Visa, gebaseerd op het ontwerp, door een ervaren ontwikkelaar gemaakt...

LEES MEER »

Veilige kluisrekening fraude: "De totale schade valt in de miljoenen euro’s"

De afgelopen maanden zijn honderden mensen gebeld door oplichters die zich voordeden als medewerkers van de fraudehelpdesk van banken. Met een vlotte babbeltruc slaagden zij erin om hun slachtoffers over te halen hun geld naar een ‘veilige kluisrekening’ over te sluizen...

LEES MEER »

Check het linkje, niet altijd zo makkelijk als je zou denken

Gebruikers op internet vertrouwen op domeinnamen om merken, diensten, professionals en persoonlijke websites te vinden. Cybercriminelen profiteren van de essentiële rol die domeinnamen spelen op internet door namen te registreren die lijken te zijn gerelateerd aan bestaande domeinen of merken, met de bedoeling te profiteren van gebruikersfouten...

LEES MEER »

Exponentieel DDoS aanvallen op online lesomgevingen

DDoS-aanvallen tegen online lesomgevingen groeiden dit voorjaar exponentieel in vergelijking met het voorgaande jaar, zo blijkt uit het 'Digital Education report van Kaspersky'. Voor elke maand, van januari tot juni 2020, is het aantal DDoS-aanvallen met betrekking tot digitale, educatieve middelen met tenminste 350% gestegen, in vergelijking met de overeenkomstige maand in 2019...

LEES MEER »

Eens of oneens: 10 stellingen over digitale veiligheid

1. Ik heb niets interessants voor hackers.
2. Ik gebruik beveiligingssoftware, dus ik ben beveiligd.
3. Aangezien er zoveel aanvallen zijn, heeft het voor mij geen zin om mijn gegevens te beschermen...

LEES MEER »

2,5 jaar gevangenis voor WhatsApp fraude

Twee 28-jarige mannen uit Deventer zijn door de rechtbank Overijssel veroordeeld voor grootschalige oplichting via WhatsApp en het witwassen van op die manier afhandig gemaakt geld. Ook maakten ze zich schuldig aan computervredebreuk...

LEES MEER »

'Password spraying' en 'Brute force' aanvallen in aanloop naar de verkiezingen in de Verenigde Staten

Organisaties betrokken bij de verkiezingen in de Verenigde Staten en het Verenigd Koninkrijk zijn het doelwit van aanvallen waarbij aanvallers via brute force en password spraying toegang tot Office365-accounts proberen te krijgen, zo stelt Microsoft...

LEES MEER »

Als je dacht dat… dan zit je fout en ben je een prooi voor ‘Hackers’

Op het Darkweb kun je verschillende handleidingen vinden over hoe je cybercriminaliteit moet plegen. Eindeloze lijsten met aanmeldingen, wachtwoorden, account nummers en zelfs telefonische ondersteuningslijnen voor slachtoffers om te bellen, dit alles kan eenvoudig online worden gekocht...

LEES MEER »

Bezoekers pornosites doelwit voor cyberaanvallen

Een hackers groep is de afgelopen maanden bezig geweest met het plaatsen van kwaadaardige advertenties op websites met een volwassen thema om gebruikers om te leiden naar exploit kits en deze te infecteren met malware...

LEES MEER »

Ransomware weekoverzicht week 36 - 2020

OVERZICHT »

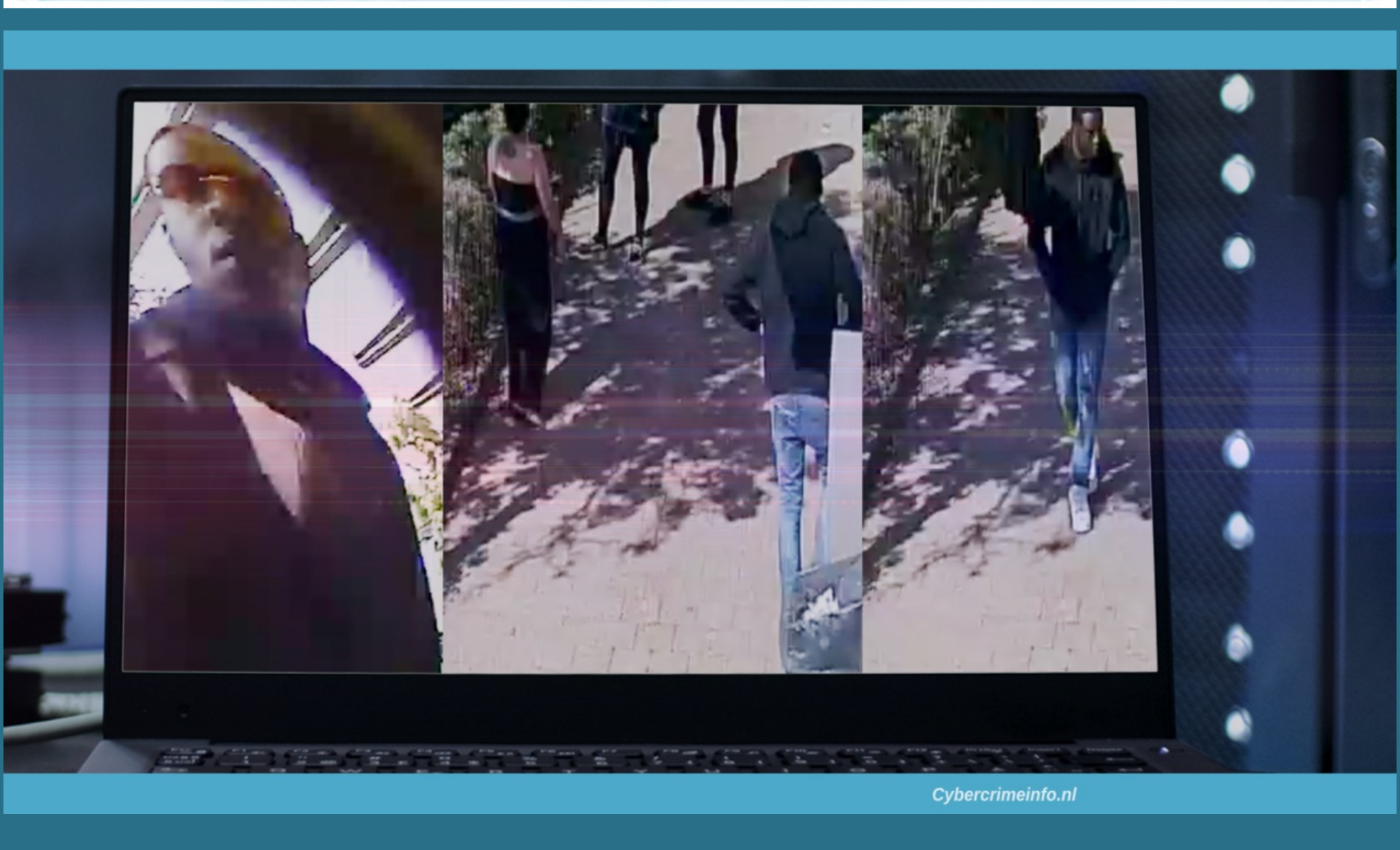
Datalek nieuws en overzicht week 37-2020

OVERZICHT »

Oplichting / Cybercrime overzicht week 37-2020

OVERZICHT »

Gezochte Personen



Gemert - Verdachte pinpasfraude

Op woensdag 15 april 2020 werd een 73 jarige man uit Gemert slachtoffer van pinpasfraude en werd er voor een bedrag van 2.000,00 euro van zijn rekening gepind. Het slachtoffer ontving op woensdagochtend 15 april 2020 een mail met de mededeling dat zijn bankpas op korte termijn vervangen zou moeten worden. In deze mail zat een link om dit direct te kunnen regelen...

LEES MEER »

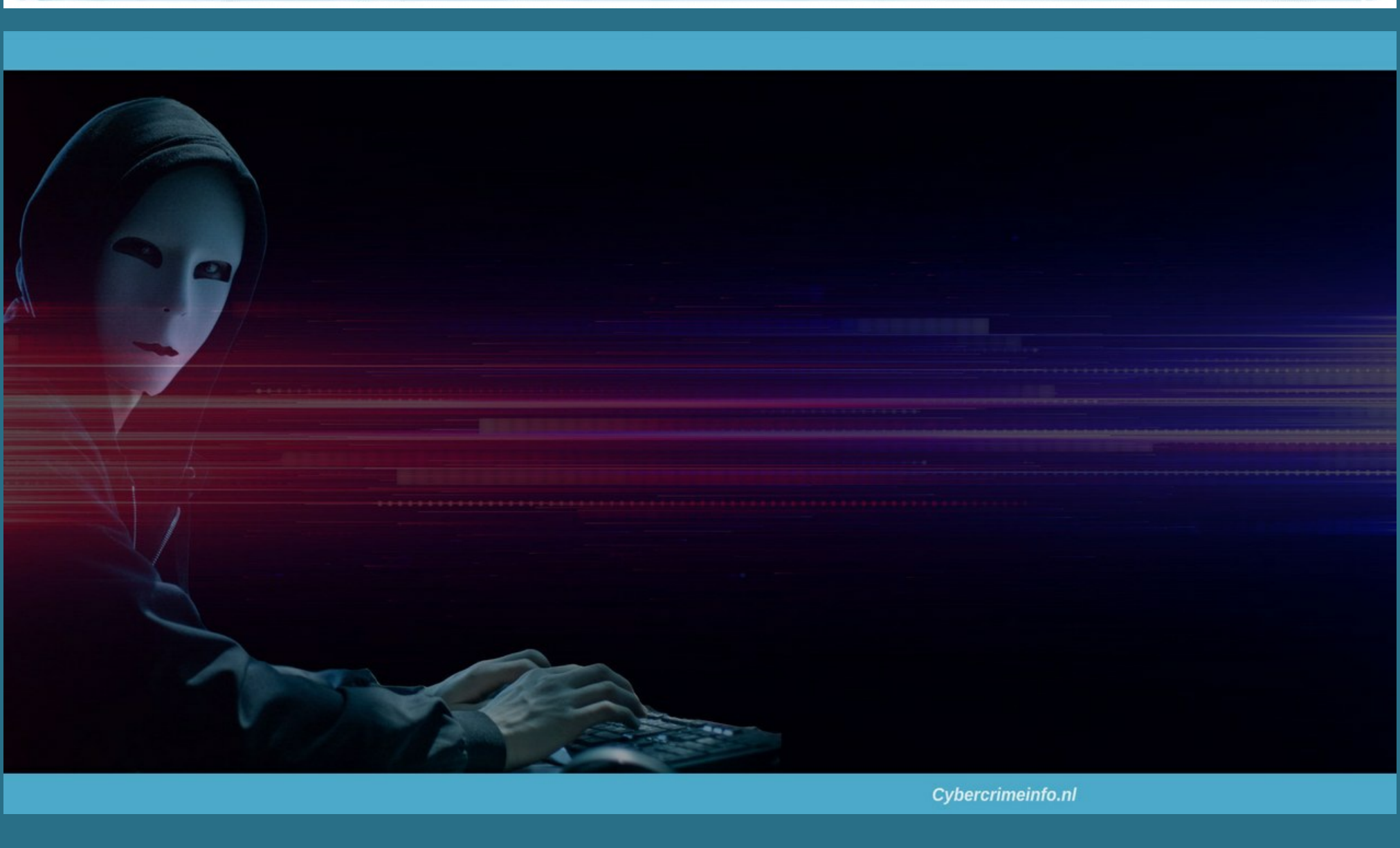
Dark Web

Iraanse hackers adverteren op Darkweb

Volgens een nieuw rapport van CrowdStrike lijkt een vermoedelijke door de Iraanse staat gesteunde hackers groep actief te zijn geweest om extra inkomsten te genereren. De security onderzoekers beweerde dat de nieuw ontdekte 'Pioneer Kitten' actief is sinds ten minste 2017 en voornamelijk gericht is op het stelen van informatie die strategisch nuttig zou zijn voor Teheran...

LEES MEER »

Wat is?



Wat is Cybersquatting?

Cybersquatting, ook wel “Domain name grabbing” of “domeinkaping” genoemd is het registreren van een domeinnaam die identiek of gelijkaardig is aan een merk, handelsnaam, familienaam of elke andere benaming die iemand anders toebehoort, zonder zelf een legitiem recht of belang op deze benaming te hebben en met als doel schade toe te brengen aan een derde of er onrechtmatig voordeel uit te halen...

LEES MEER »

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