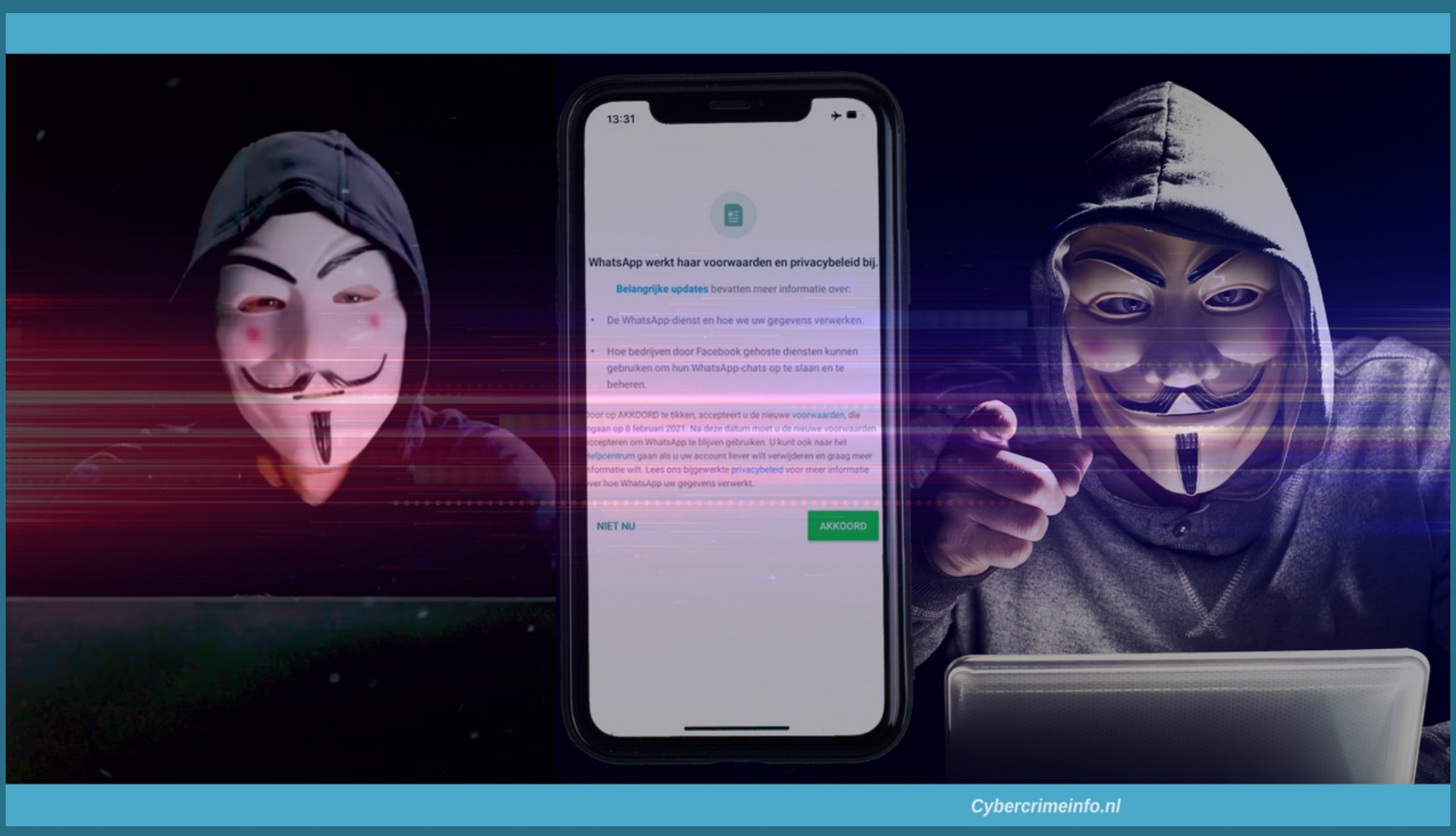
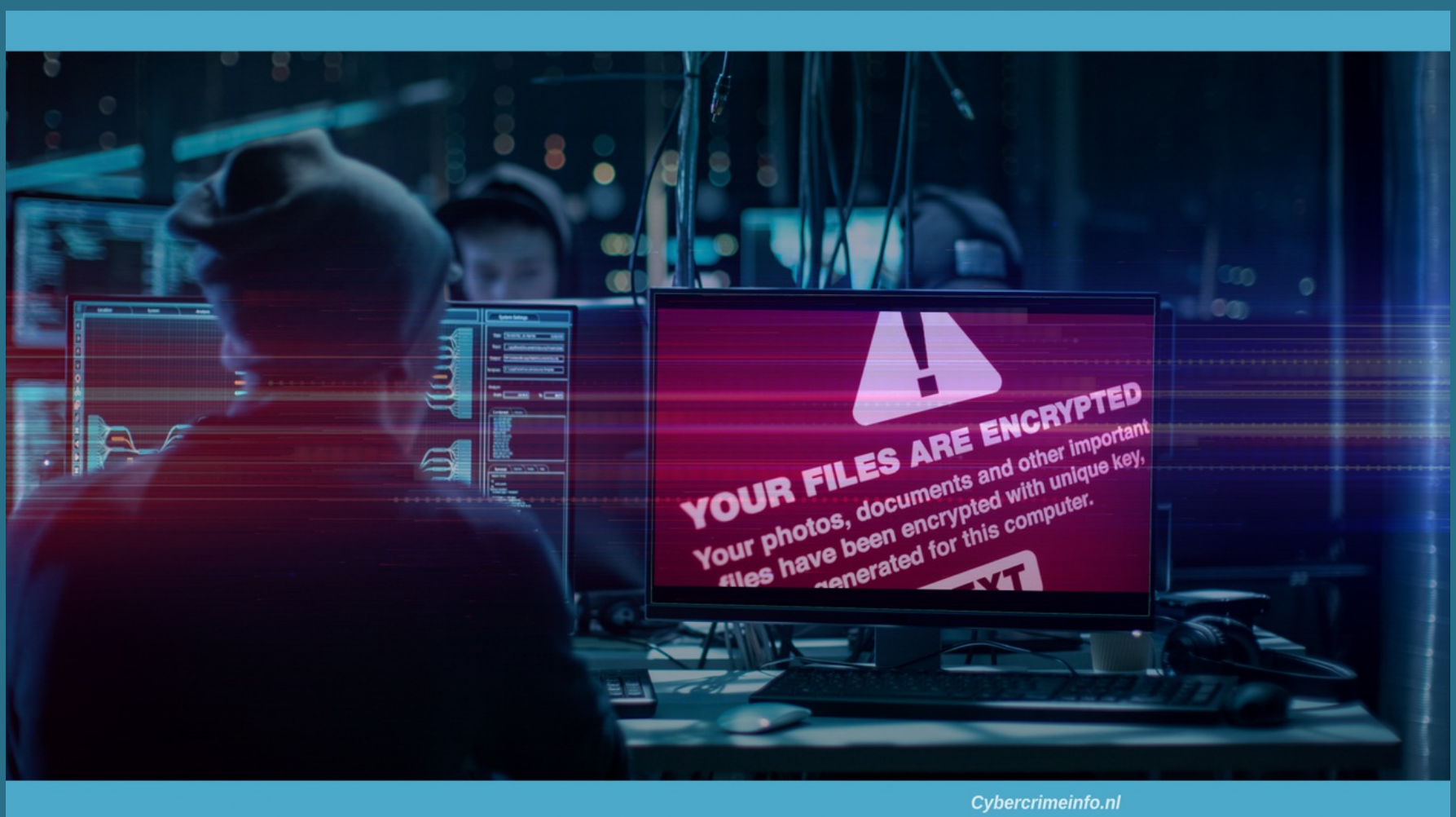
Nieuwsbrief 147 - Week 08-2021



Geruchten WhatsApp, hoe zit dat nu?

WhatsApp gebruikers, dit moet je weten. De app is na 15 mei 2021 nauwelijks meer te gebruiken als je de nieuwe gebruiksvoorwaarden niet hebt geaccepteerd. Nieuwe berichten lezen of versturen is dan niet langer mogelijk: het beleid voor inactieve accounts treedt vanaf die datum in werking. Het beleid voor inactieve accounts houdt in dat je account niet direct wordt verwijderd, maar wel dat de functionaliteit ernstig wordt beperkt. Een berichtendienst waarmee je geen berichten kunt versturen of ontvangen is immers niet zo praktisch...

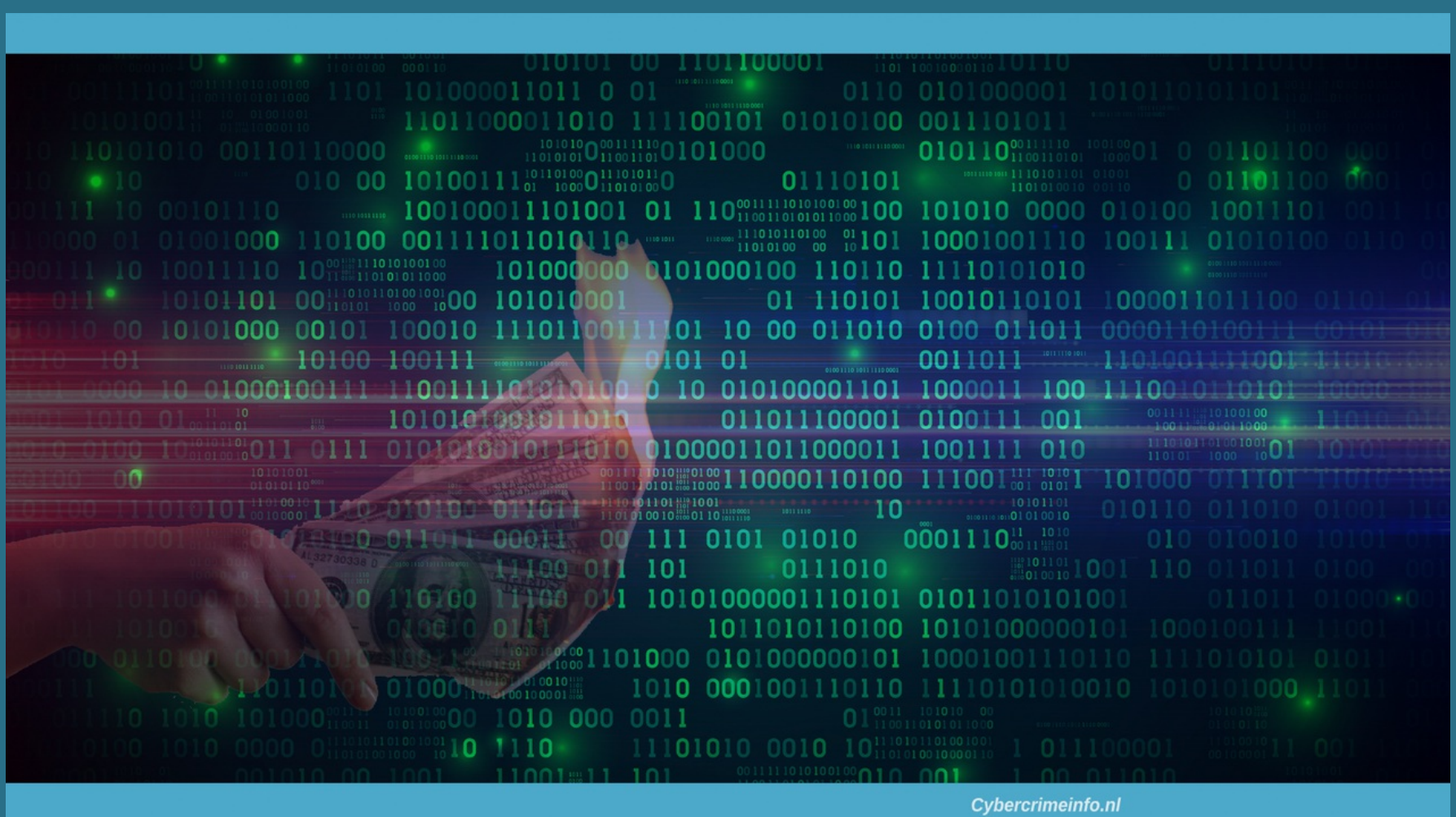
LEES VERDER



Twee derde van organisatie kreeg te maken met ransomware in 2020

Uit onderzoek van Proofpoint blijkt dat ransomware-aanvallen een enorm groot probleem zijn. Zo geeft 66 procent van respondenten aan het slachtoffer te zijn geweest van ransomware. Twee derde van de respondenten in het onderzoek gaf aan dat hun organisatie in 2020 te maken kreeg met ransomware. Meer dan de helft van hen besloot het losgeld te betalen in de hoop snel weer toegang te krijgen tot de gegevens...

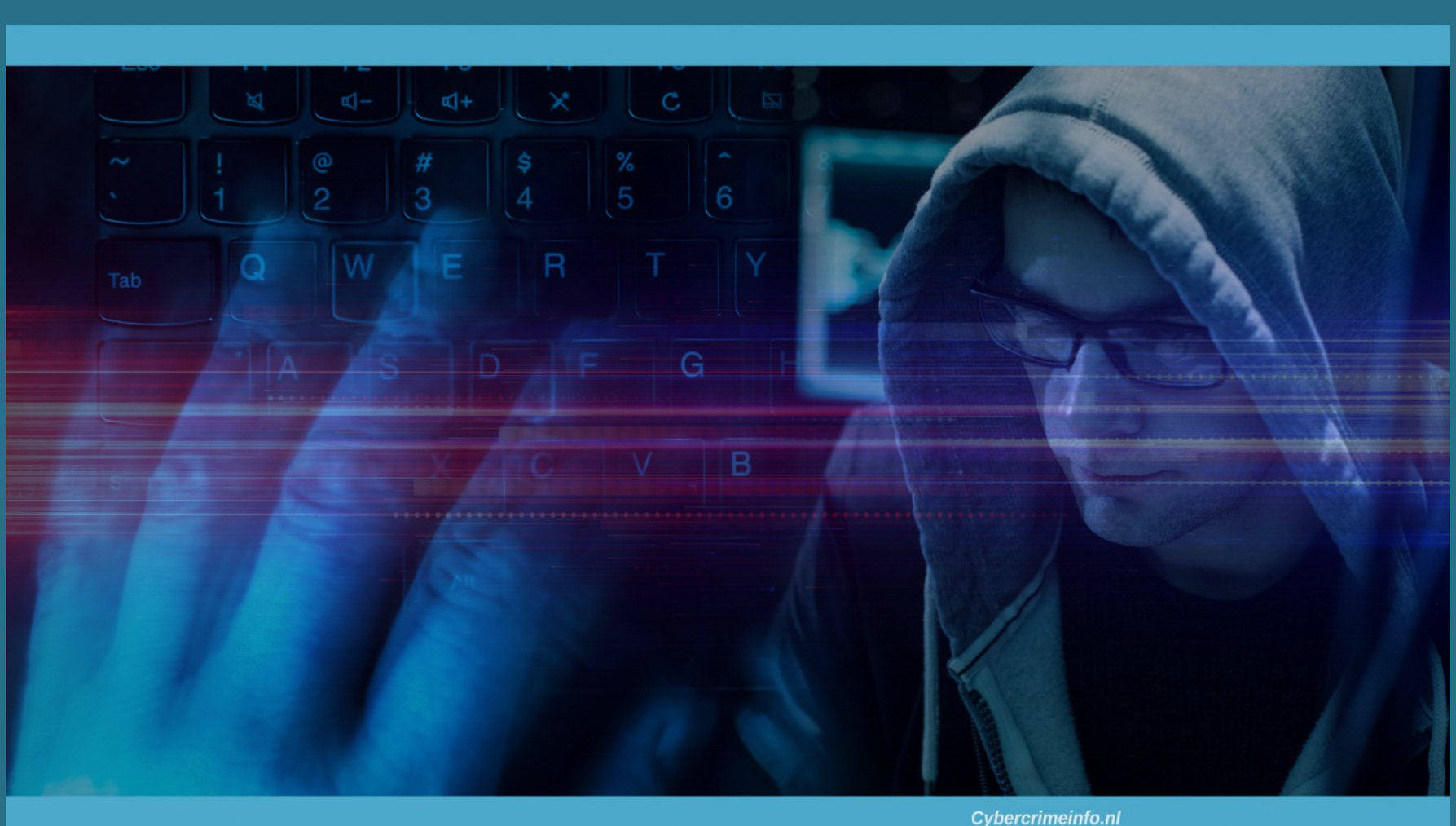
LEES VERDER



Losgeld: "Het besluit dat we hebben genomen gaat in tegen al onze principes, het voelt heel slecht"

Het 'Staring College' is deze week getroffen door een grote ransomware-aanval. De middelbare school, met vestigingen in Lochem en Borculo, heeft na wikken en wegen besloten om losgeld te betalen aan de aanvallers. Dat was enige manier om er zeker van te zijn dat het onderwijs geen gevaar liep. 'Betaal geen losgeld als je het slachtoffer bent geworden van een hacker. Doe je dat wel, dan stimuleer je het verdienmodel van cybercriminelen.' Als buitenstaander is het makkelijk om dit advies te geven...

LEES VERDER



"Credential stuffing zal een bedreiging vormen zolang we van gebruikers eisen dat ze zich online bij accounts aanmelden"

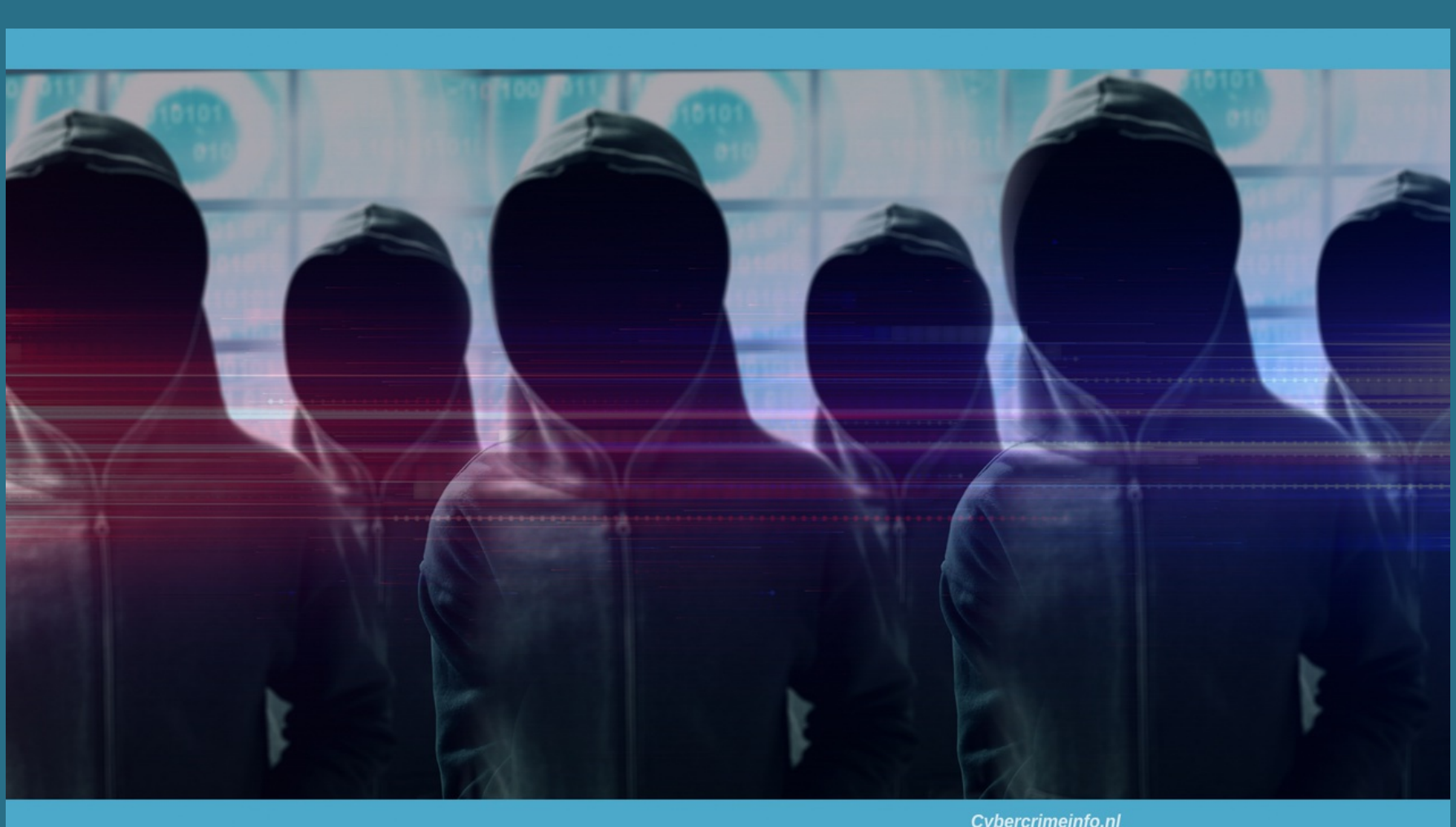
Het aantal jaarlijkse incidenten met inloggegevens is tussen 2016 en 2020 bijna verdubbeld. In dezelfde periode daalde echter de totale hoeveelheid aan gelekte data met 46 procent. Dit blijkt uit het nieuwste Credential Stuffing Report van 'F5'. De gemiddelde omvang van een datalek is ook afgenomen, van 63 miljoen records in 2016 tot 17 miljoen vorig jaar...

LEES VERDER

Malware toename met 229%

Gisteren kondigde 'G DATA CyberDefense' zijn jaarlijkse malware top 10 aan. In 2020 identificeerde de specialisten van het securitybedrijf maar liefst 16.1 miljoen malwaresamples. Dit zijn gemiddeld 76 nieuwe malware samples per minuut. Dit is een toename van 228.6 percent vergeleken met 2019. In 2020 werd Emotet malware het meest in omloop gebracht. In totaal werden er 888.793 verschillende versies geïdentificeerd...

LEES VERDER



We verwachten in de toekomst meer van 'ThreatNeedle' te zien

Cybersecurity onderzoekers hebben een nieuwe campagne geïdentificeerd van Lazarus, een zeer productieve geavanceerde dreigingsactor. Lazarus is actief vanaf ten minste 2009 en is betrokken geweest bij grootschalige cyberspionage campagnes, ransomware-campagnes en zelfs aanvallen op de cryptocurrency-markt. Waar het zich de afgelopen jaren op financiële instellingen richtte, valt Lazarus sinds begin 2020 de defensie-industrie aan via een aangepaste backdoor genaamd 'ThreatNeedle'...

LEES VERDER

Cybercriminelen maken 30.000 klantgegevens buit van Amsterdamse woningcorporatie

De Amsterdamse 'woningcorporatie Stadgenoot' is het slachtoffer geworden van een hacker. Persoonsgegevens van zo'n 30.000 klanten zijn buitgemaakt door de dader(s). Het datalek is inmiddels gedicht en gemeld bij de Autoriteit Persoonsgegevens. Stadgenoot is een van de grotere woningcorporaties in de hoofdstad. Het bedrijf, ontstaan door een fusie tussen twee Amsterdamse woningcorporaties in 2008, verhuurt dertigduizend sociale huurwoningen aan mensen met een lager inkomen. Ook heeft de woningcorporatie enkele duizenden huurwoningen in de vrije sector, parkeerplaatsen en bedrijfsruimten in beheer...

LEES VERDER

"Er kan niet worden gewacht met het delen van incident informatie"

De 'Cyber Security Raad (CSR)' wil versneld incidentinformatie met het bedrijfsleven en burgers delen. In de ogen van de raad is dit 'een van de belangrijkste instrumenten' om de cyberweerbaarheid van de samenleving te verhogen. De CSR adviseert minister Grapperhaus om te onderzoeken of het Landelijk Dekkend Stelsel (LDS) van informatieknooppunten via een 'spoedreparatie' sneller kan worden doorgevoerd...

LEES VERDER

Ransomware weekoverzicht 07-2021

Kia Motors America lijdt aan een ransomware aanval, Underwriters Laboratories (UL) certificeringsgigant getroffen door ransomware en verdachten achter Egregor-ransomware aangehouden in Oekraïne. Hier het overzicht van de nieuwste ransomware vormen en het nieuws van dag tot dag...

LEES VERDER

Digitale fraude, oplichting meldingen week 08-2021

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?!, 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.

LEES VERDER

Datalek nieuws en overzicht week 08-2021

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 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.

LEES VERDER

Gezochte Personen

Den Haag - Bankhelpdeskfraude

De vrouwen werden gebeld door een zogenaamde bankmedewerker. Hij vertelde dat er 2000 euro van hun rekening werd overgeschreven naar een Afrikaans rekeningnummer. Hij had hiervoor een oplossing. In beide zaken moesten de vrouwen aan de telefoon blijven tot een andere zogenaamde bankmedewerker langs was gekomen. Hij zou de pas doorknippen en dan was het probleem opgelost...

LEES VERDER

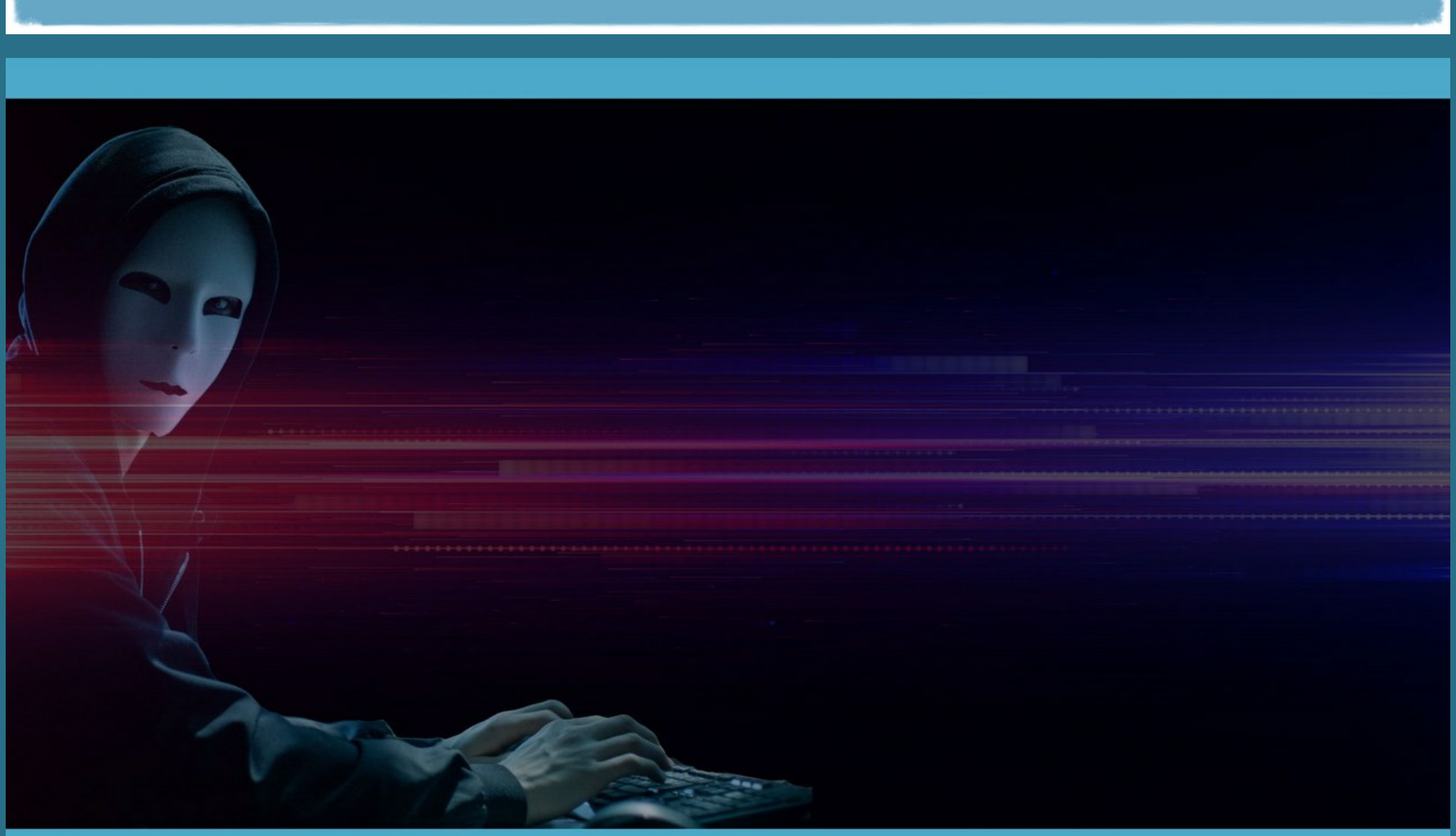
Dark Web

Communicatie middelen en logistieke partners cruciaal voor criminele organisaties

In het artikel KIK het alternatief voor TOR omschreven we een nieuw ecosysteem dat naast het TOR netwerk opereert. We hebben in het verleden verschillende artikelen gewijd aan wat er op KIK te vinden was. Veelal bleek dat de applicatie als ondersteuning diende van de criminele operaties die via het TOR netwerk liepen. Echter vonden we in het verleden dat naast KIK ook Telegram vaak genoemd werd door criminele organisaties als extra verlengstuk in de communicatie/marketingmix van de organisatie. Deze verwijzingen zagen we zwart-op-wit genoemd worden op het Darkweb...

LEES VERDER

Wat is?



Wat is Credential stuffing?

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

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

Wil je meer vormen en begrippen leren kennen? Kijk dan op deze pagina.


CYBERCRIMEINFO.NL

HOME NIEUWS CYBERCRIME DARKWEB VAN A TOT Z TIPS & TRICKS POLITIE LANGUAGES

Cybercrime nieuws

"Hoe kan ik nou zo stom zijn geweest?"

Als je slachtoffer bent geworden van oplichting kan dit emotioneel heel zwaar zijn. Naast de financiële schade kun je ook last hebben van angst, schaamte, stress en een beschadigd vertrouwen in mensen. Hoe kun je hiermee omgaan?

Lees meer »

Hoe word je aan de haak geslagen, en hoe kun je het voorkomen?

Er wordt de laatste tijd een significante toename geregistreerd in het aantal Phishingaanvallen, maar wat zijn dat nu precies? In dit artikel besteden we aandacht aan de diverse technieken en geven we voorbeelden om niet aan de "haak geslagen te worden".

Lees meer »

Over Cybercrimeinfo

"Kennis is macht, maar gedeelde kennis is vermenigvuldigde macht (Robert Noyce)"

LEES VERDER
