Nieuwsbrief 126 - Week 40-2020

Zeroday malware die traditionele antivirus handtekeningen omzeilt in de lift

Maar liefst 70 procent van alle cyberaanvallen tijdens het tweede kwartaal van 2020 zetten zero-day malware in. Dat is een stijging van 12 procent ten opzichte van het eerste kwartaal, zo blijkt uit het nieuwe Internet Security Rapport over Q2 van 2020 van securityleverancier 'WatchGuard Technologies'. Deze malware omzeilt traditionele antivirus-handtekeningen en zijn hierdoor moeilijker detecteerbaar...

LEES MEER »

"Vannacht, 30 september, vond een cyberaanval plaats op onze hogeschool"

Vannacht, 30 september, vond een cyberaanval plaats op onze hogeschool. Onze IT-afdeling kon snel ingrijpen, maar om ervoor te zorgen dat het niet verder verspreidt, mag je voorlopig niet inloggen op het AP-netwerk. Daarom blijven alle de campussen in Antwerpen, Mechelen en Turnhout vandaag voorlopig gesloten. Externe tools zoals Teams, Digitap en mail blijven beschikbaar van thuis uit...

LEES MEER »

"Gemeenten moeten regie voeren over hun cyber risico management"

Niet hackers, maar medewerkers zelf zijn veelal verantwoordelijk voor een cyberaanval bij een gemeente. Dan gaat het niet zozeer om een vergissing, maar om medewerkers met verhoogde toegangsrechten en kwade bedoelingen. Dit type cyberaanval is uiterst gevaarlijk, omdat het zeer moeilijk is om deze ontdekken en er iets aan te doen...

LEES MEER »

Verdachte aangehouden na installeren keyloggers

De politie heeft woensdagmorgen een 29-jarige man uit Zuidhorn aangehouden op verdenking van cybercrime. Hij wordt er van verdacht dat hij 'keyloggers' heeft geïnstalleerd op computers van mensen met wie hij samenwerkte. Vervolgens zou hij hebben ingelogd op een aantal van hun privé accounts (hacking). Meerdere mensen hebben aangifte gedaan.
De verdachte is meegenomen naar het politiebureau om hierover te worden verhoord...

LEES MEER »

Dertien aanhoudingen door Cyberteam Antwerpen in een omvangrijke phishing zaak

Het cyberteam van politiezone Antwerpen heeft een phishingbende opgerold die op slechts enkele dagen tijd vele duizenden euro’s zou hebben afgetroggeld bij nietsvermoedende slachtoffers. Woensdagochtend zijn in opdracht van de onderzoeksrechter zestien huiszoekingen verricht in Antwerpen, Essen, Schelle en Sint-Jans-Molenbeek. Dertien verdachten zijn gearresteerd...

LEES MEER »

“We hebben letterlijk de stekkers eruit getrokken om alle lopende oplichtingspraktijken een halt toe te roepen”

In een lopend onderzoek van politie en Openbaar Ministerie Noord-Nederland naar grootschalige cyberfraude zijn maandag 28 september twee verdachten (een man en een vrouw, beiden 21 jaar) aangehouden in Groningen. De man zou tussen 2 en 21 september maar liefst 120.000 sms-berichtjes (smishing) hebben verstuurd met daarin een phishing link waarmee hij de controle kon overnemen van bankrekeningen. Over het hele land zijn slachtoffers gemaakt. Het totale schadebedrag moet nog worden vastgesteld...

LEES MEER »

Cybercriminelen bekwamer en meedogenlozer

Microsoft heeft een nieuwe editie van haar beveiligingsrapport uitgegeven. Daarin staat het Amerikaanse hard- en softwarebedrijf uitgebreid stil bij de laatste ontwikkelingen op het gebied van malware en cybersecurity. Niet alleen neemt het aantal cyberaanvallen toe, tevens worden ze met de dag geavanceerder, zo valt er te lezen. Het toenemend aantal aanvallen is volgens Microsoft slechts gedeeltelijk toe te schrijven aan de wereldwijde coronapandemie...

LEES MEER »

Politie: "Focus op cybercrime tijdens veiligheidsweek (5-11 oktober)"

De politie Zeeland-West-Brabant sluit dit jaar aan bij de week van de veiligheid. Hierbij richten wij ons op ‘digitale weerbaarheid’ met een cybercrime campagne via met name social media. Districtschef Wietske Muller is portefeuillehouder voor gebiedsgebonden politiezorg en digitalisering politiewerk. Zij ziet het aantal digitale slachtoffers met de dag toenemen: “Door een hele week de aandacht op cybercrime te richten en dan vooral op de preventieve kant, willen we de kans pakken om onze burgers daarin weerbaarder te maken en hen de helpende hand toe te steken.”...

LEES MEER »

Ransomware weekoverzicht week 39 - 2020

Afgelopen week zagen we aanhoudende aanvallen op grote organisaties, terwijl nieuwe ransomware-operaties zich haasten om deel te nemen aan een moderne ransomware-goudkoorts.
In de afgelopen week waren ransomware aanvallen gericht op twee grote organisaties en verstoorde operaties. De eerste is brillengigant Luxottica, die afgelopen zondag werd geraakt, en Tyler Technologies, aanbieder van technologie diensten van de overheid, die later in de week door 'RansomExx' werd geraakt...

OVERZICHT »

Datalek nieuws en overzicht week 40-2020

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.

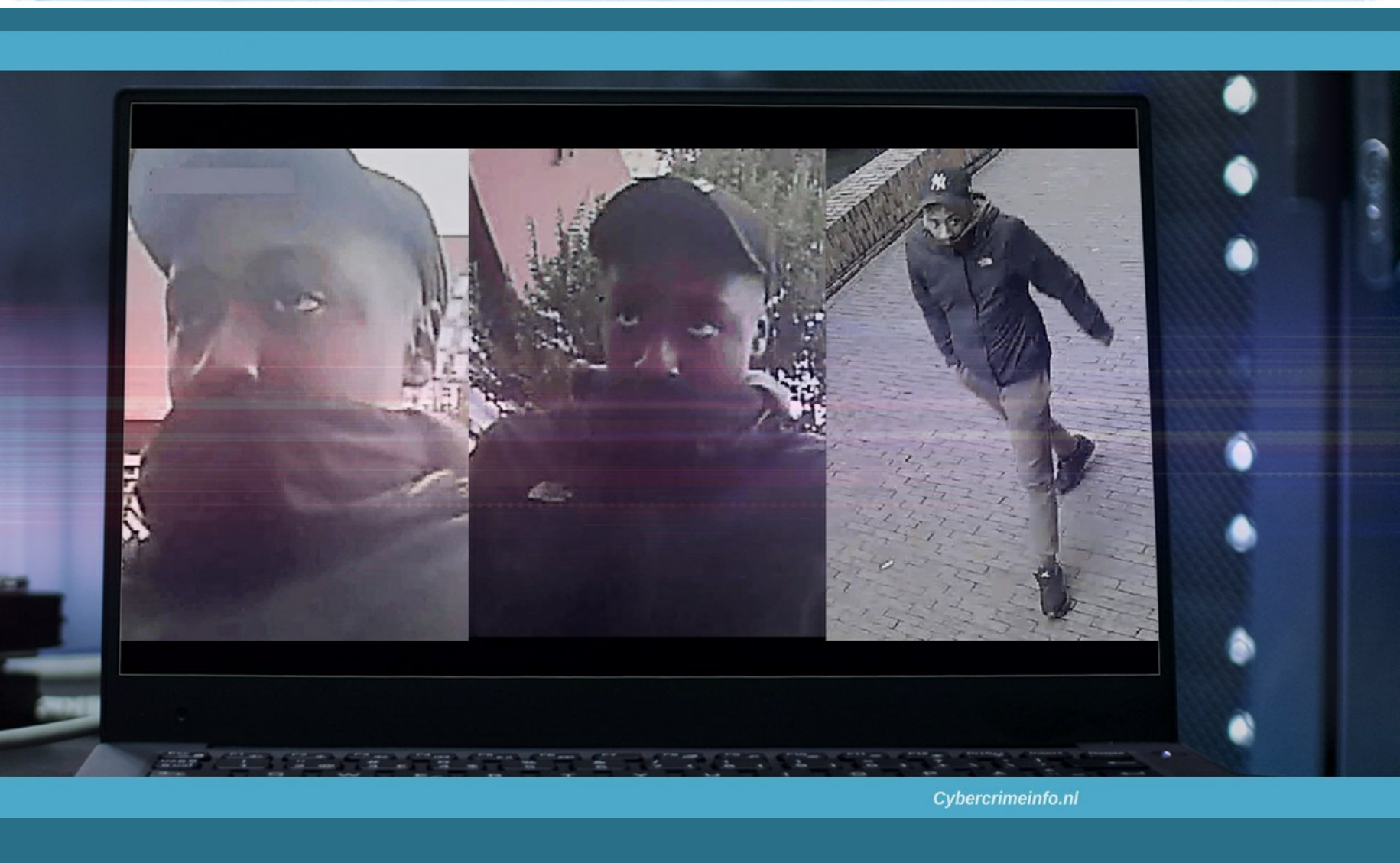
OVERZICHT »

Gedigitaliseerde oplichting / misdaad overzicht week 40-2020

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 »

Gezochte Personen



Zaandam - Een euro pinnen voor pakket

Donderdag 3 oktober 2019 werd een 74-jarige vrouw uit Zaandam slachtoffer van een babbeltruc. Rond 15:15 uur werd bij haar een pakketje bezorgd. De bezorger vroeg haar 1 euro te pinnen voor het pakket. Hij pakte daarop haar bankpas aan en hield het bij het pinapparaat. Nadat de dame had gepind, gaf hij een pas terug en vertrok de bezorger. Even later ontdekte het slachtoffer dat ze een andere pinpas had teruggekregen. Toen ze de bank belde om haar pas te blokkeren was het al te laat. Bij twee pinautomaten was een groot geldbedrag van haar rekening opgenomen...

LEES MEER »

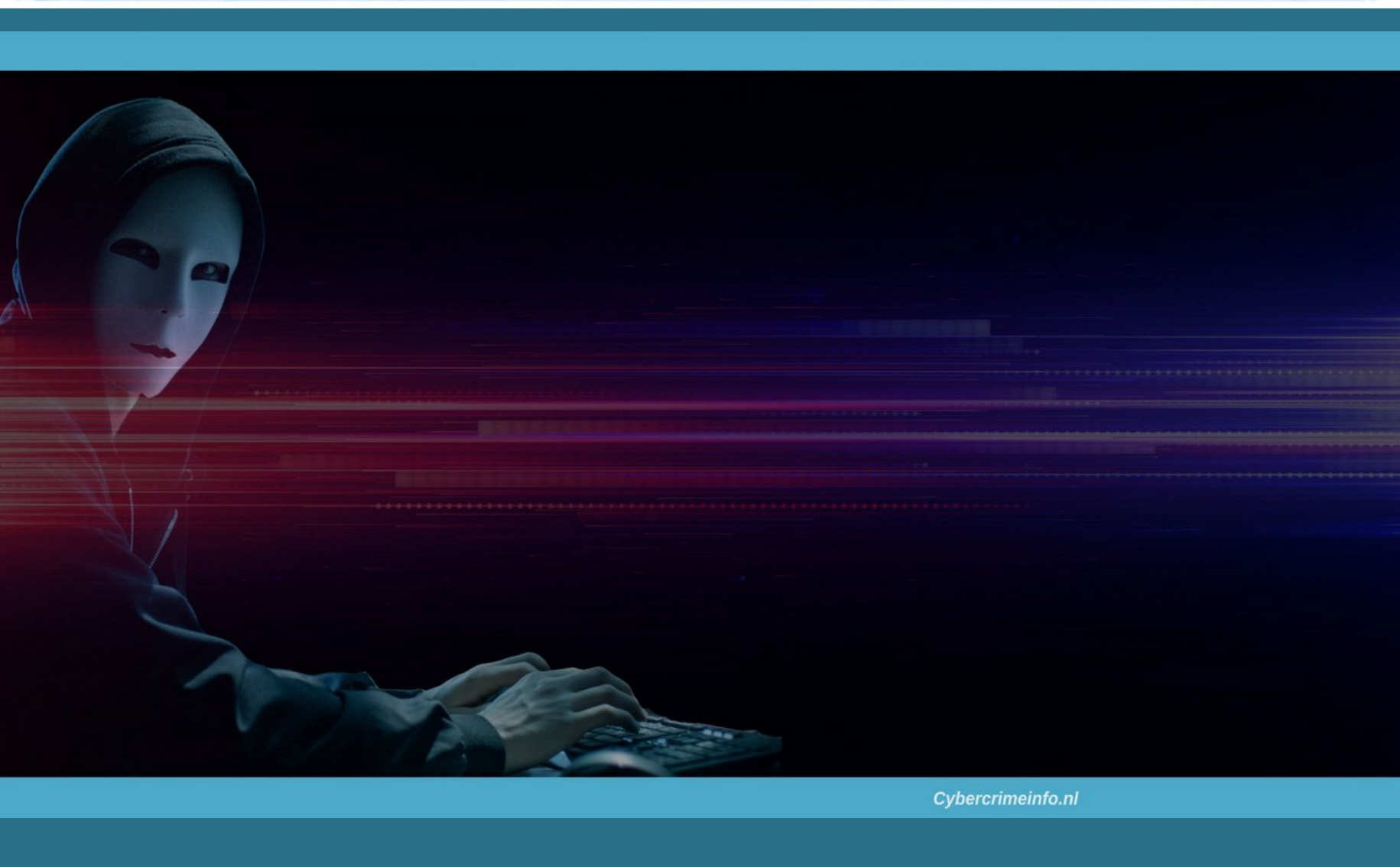
Dark Web

Darkweb kiezersdatabase-rapport werpt nieuwe twijfels op over het Russische verkiezingshack verhaal

Een nieuw rapport dat aantoont dat kiezersdatabases van Amerikaanse staten openbaar beschikbaar waren, doet twijfels rijzen over het verhaal dat de Russische inlichtingendienst in 2016 ‘hun pijlen gericht hadden’ op verkiezingswebsites van staten in Amerika. Een artikel van 1 september in het Moskouse dagblad Kommersant over een 'darkweb' site met een database met persoonlijke informatie van miljoenen geregistreerde Amerikaanse kiezers ondermijnt een van de centrale thema’s van de Russische hysterie waarvan de Amerikaanse politiek vergeven is...

LEES MEER »

Wat is?

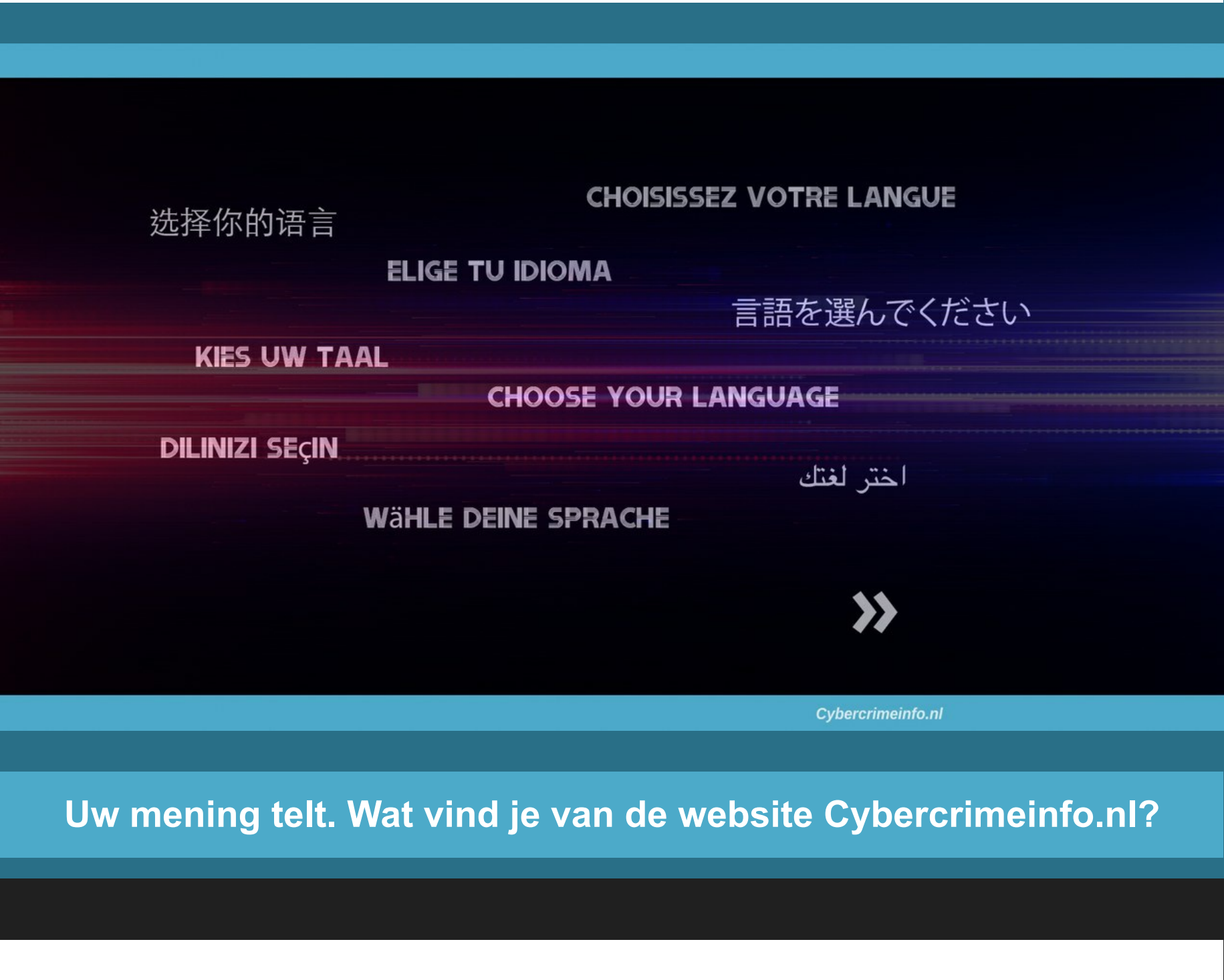


Wat is een Keylogger?

Een 'keylogger' is software die veelal ongemerkt de toetsaanslagen op een keyboard registreert. Keyloggers zijn (vaak) een vorm van malware, omdat ze kunnen worden gebruikt om heimelijk te monitoren wat een gebruiker intypt. Op die manier kan de keylogging-software berichten aflezen en belangrijke wachtwoorden en inloggegevens registreren. Deze gegevens worden veelal doorgesluisd aan de cybercriminelen die achter de desbetreffende keylogger-software zitten...

LEES MEER »

De week in beeld



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