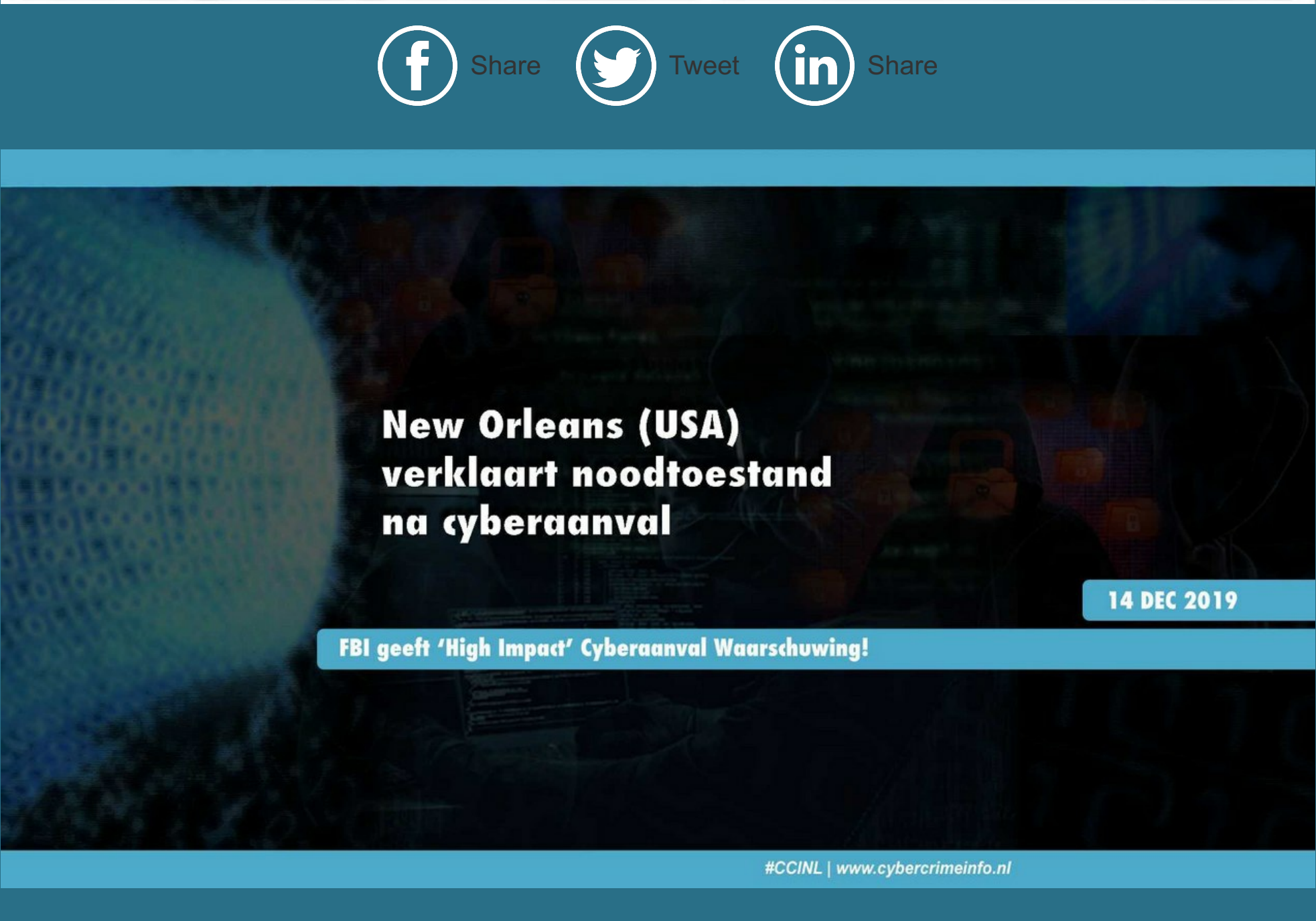
Nieuwsbrief 84 (week 50-2019) #CCINL | www.cybercrimeinfo.nl

#CCINL | www.cybercrimeinfo.nl
www.computercriminaliteit.net
www.darkwebinfo.nl

Share Tweet Share



New Orleans (USA) verklaart noodtoestand na cyberaanval

De aanval begon op vrijdag 13 december om 17.00 uur volgens de NOLA Ready-campagne van de stad New Orleans, beheerd door het Office of Homeland Security and Emergency Preparedness. NOLA Ready tweette dat “verdachte activiteit werd gedetecteerd op het netwerk van de stad,” en naarmate het onderzoek vorderde, “ activiteit die een cyberaanval aangeeft werd gedetecteerd rond 11 uur” Uit voorzorg bevestigde de NOLA tweet dat de IT-afdeling van de stad opdracht gaf alle werknemers om computers uit te schakelen en de verbinding met Wi-Fi te verbreken. Alle stadsservers werden ook uitgeschakeld en werknemers moesten de stekker uit het stopcontact halen elk van hun apparaten...

LEES MEER >>

Phishing verdrievoudigd

Het aantal gevallen van phishing is verdrievoudigd. Bij de Fraudehelpdesk kwamen dit jaar driemaal zo veel meldingen van phishing binnen. Vorig jaar waren dat er nog zo'n 2.600, dit jaar zijn dat er al bijna 8.200. Sowieso kan 2019 met recht het jaar van de fraude worden genoemd, want ook andere vormen van fraude namen explosief toe...

LEES MEER >>

Cybercriminelen hergebruiken oude aanvalstechnieken

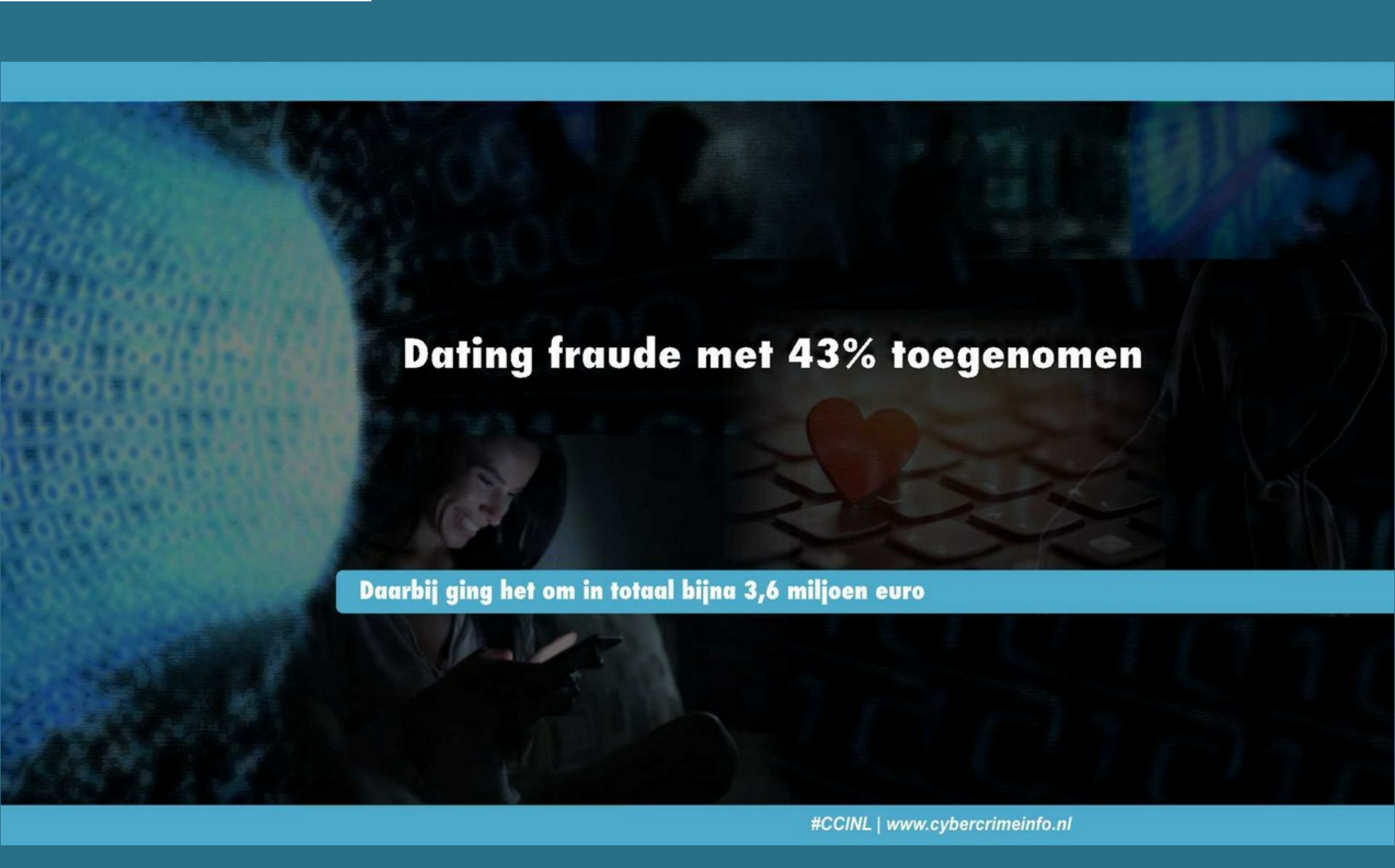
Cybercriminelen ontwikkelen niet alleen nieuwe malware en zero day-aanvallen, maar hergebruiken ook tactieken die in het verleden succesvol zijn gebleken. Daarmee kunnen ze zoveel mogelijk kansen binnen het aanvalsoppervlak benutten. Dat blijkt uit het Fortinet Threat Landscape Report van FortiGuard Labs, waarin wordt gesteld dat cybercriminelen phishing-tactieken inruilen voor de injectie van kwaadaardige code in openbaar toegankelijke internetdiensten. Het is een tactiek om organisaties te overrompelen in aanloop naar de drukke feestdagen...

LEES MEER >>

Cybercrime aanval: Het incident kostte hem uiteindelijk bijna 8 ton en betekende het einde van zijn bedrijf, zijn huis en zijn relatie!

Xander Koppelmans werd letterlijk door schade en schande wijzer. In 1990 startte hij in Goes het reclamebureau PHGR dat uiterst succesvol werd en campagnes maakte voor zo'n 400 bedrijven en overheidsorganisaties, waaronder heel grote. Tot 2 april 2015. Medewerkers merkten dat ineens heel veel data van de servers verdween. In paniek belde Koppelmans zijn ICT-dienstverlener die de servers direct uitschakelde...

LEES MEER >>



Dating fraude met 43% toegenomen

Het aantal slachtoffers van datingfraude in 2019 ten opzichte van 2018 met 43 procent toegenomen. Het gaat hier om mensen die opgelicht worden door iemand die beweert geïnteresseerd te zijn in een relatie.
Een veelvoorkomende truc is dat het slachtoffer geld moet overmaken zodat zijn of haar geliefde de reis naar Nederland kan betalen. Maar datingsites kunnen ook misbruikt worden om iemand chantabel te maken. ‘Geef de toegangscodes of we lichten je partner in’...

LEES MEER >>

Datalek overzicht week 50-2019

WEEK OVERZICHT >>

PSV-cybercrime Phishing Smishing Vishing overzicht week 50-2019

WEEK OVERZICHT >>

Gezochte Personen

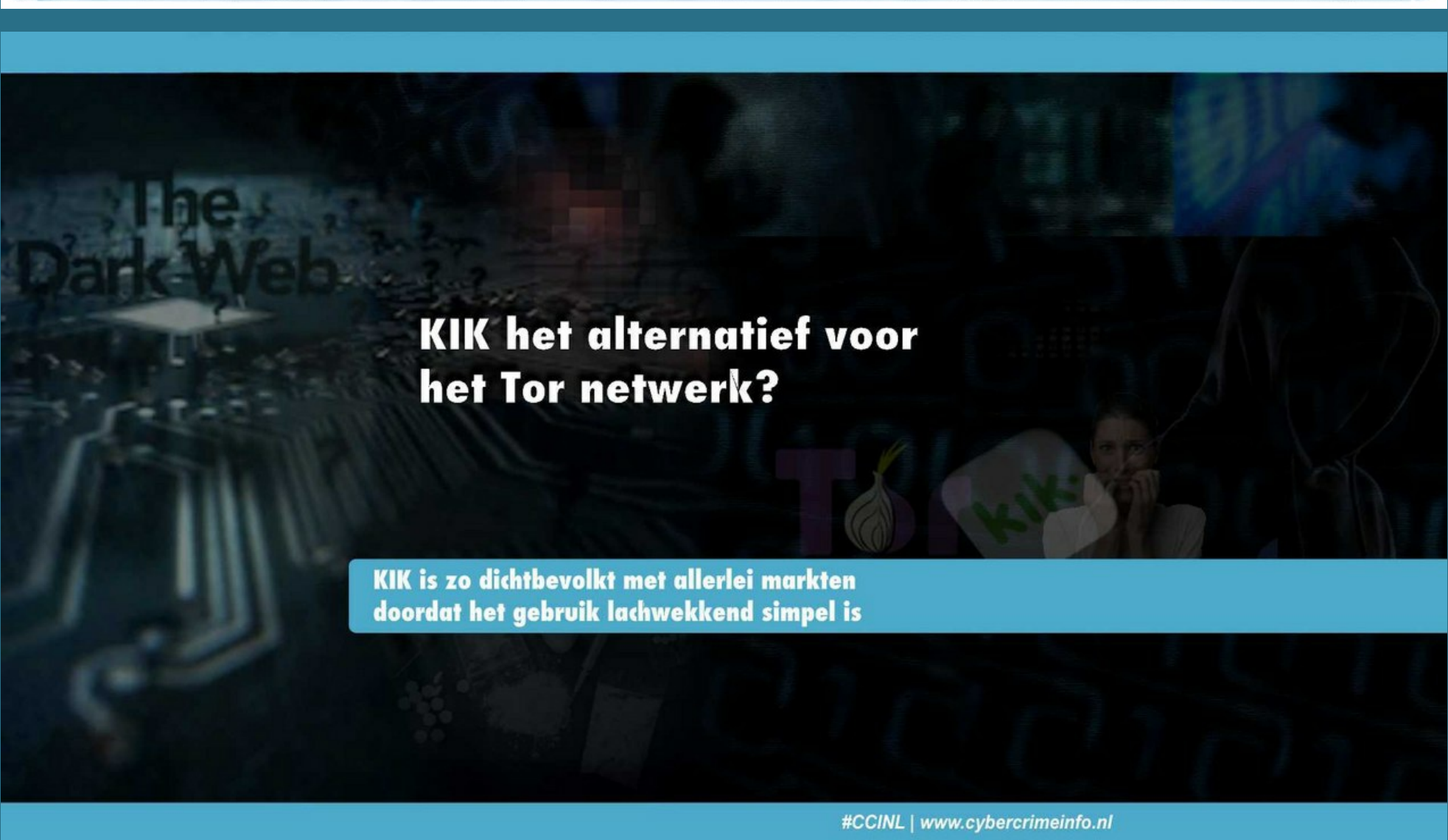
Gouda - Postpakket fraude Gouda

Zaaknummer: 2019045057
Datum delict: 14-02-2019
Plaats delict: Gouda

Een 90-jarige mevrouw uit Gouda werd op 14 februari 2019 slachtoffer van een postpakket fraude.
De bezorger liet weten dat er 1 euro gepind moest worden om het pakket in ontvangst te kunnen nemen. Het betalen van deze euro heeft met een mobiel pinautomaat plaats gevonden. Toen het slachtoffer de volgende dag haar geld wilde pinnen werd haar pinpas direct ingeslikt door de pinautomaat met de melding dat haar pas om veiligheidsreden was geblokkeerd. Toen ze bij haar bank verhaal ging halen bleek er bijna 4500 euro van haar rekening te zijn gehaald. Er worden camerabeelden getoond van een man die met deze bankpas geld heeft opgenomen...

LEES MEER >>

Dark Web



KIK het alternatief voor het Tor netwerk?

Doordat het TOR netwerk al enkele jaren zwaar op de korrel worden genomen door de verschillende opsporingsdiensten zijn criminelen, in hun eeuwige spel met de handhavingsdiensten, gedwongen om alternatieven te zoeken om hun anonimiteit redelijkerwijs te waarborgen op het Internet. Concreet gezegd maken criminelen gebruik van een bedrijfscontinuïteit strategie op het Darkweb, dat vergelijkbaar is met de modulaire bedrijfskolom van een multinational. Dit is gesimplificeerd, want het organisatiemodel heet met een lastige term: decentralized autonomous organization (- lees: decentrale autonome organisatie)...

LEES MEER >>

Wat is?

Exploitkit

Wat zijn Exploitkits?

Voor een cybercrimineel je pc schade kan toebrengen, moet hij eerst weten welke kwetsbaarheden je systeem vertoont. Hij zoekt als het ware een scheurtje in je verdediging, zodat de daaropvolgende aanval meer kans op slagen heeft. Dat hele proces kan geautomatiseerd worden door middel van een 'exploitkit'. De kit is een stukje code die je computer onderzoekt op zulke gaten; indien het een lek tegenkomt, zoals bijvoorbeeld in verouderde software, kan die code malware bezorgen op je systeem. Exploitkits buiten die kwetsbaarheden uit, wat meteen de naam verklaart...

LEES MEER >>

Stop Cybercrime

Cybercrime tegenmaatregelen

Gegevens op straat door datalek? Check hier

LEES MEER >>

Have i Been Pwnd

Schrijvers CCINL

Nieuwe schrijver bij #CCINL

WIE IS SPB >>

Als eerste op de hoogte van Cybercrime nieuws?

U kunt zich inschrijven voor de automatische berichten service van Messenger, zo krijgt u ook als eerste de berichten van #CCINL | www.cybercrimeinfo.nl

Als eerste op de hoogte »Klik hier«

Tik vervolgens in de balk chatbericht het woord “**ja**” om de berichten automatisch te ontvangen.

Nieuwsbrief gemist?

Geen probleem, klik hieronder voor alle Nieuwsbrieven...

Nieuwsbrief Archief

Nog niet ingeschreven voor de wekelijkse nieuwsbrief?

Dat kan hieronder. Elke zondag of uiterlijk op maandag ontvang je dan de nieuwsbrief van #CCINL | www.cybercrimeInfo.nl
Zo blijf je altijd op de hoogte van het nieuws over Cybercrime en Darkweb...

Inschrijven *wekelijkse* nieuwsbrief »Klik hier«

#CCINL | www.cybercrimeinfo.nl
www.computercriminaliteit.net
www.darkwebinfo.nl