Nieuwsbrief 130 - Week 44-2020

De evolutie van phishing: hoe beschermen we onszelf?

Dat criminelen creatieve methodes verzinnen om je geld te ontfutselen, weten we al langer dan vandaag. Echter, het herkennen van de slimme trucs wordt steeds moeilijker. Waar we enkele jaren geleden nog konden adviseren hoe je een phishing mail of nep website herkent, is het nu haast niet meer uit te leggen aan gebruikers. Slachtoffer worden van oplichting of cybercrime is daarom geen schande. Er zijn voor elke doelgroep listen die een crimineel kan inzetten. Van aanvallen op burgemeesters, wethouders, CEO's, penningmeesters, jongeren tot medewerkers van bedrijven...

LEES MEER »

“Hack tools in je broekzak, het kan. Alles wat je nodig hebt is internet en ’T-RAT’”

Beveiligingsonderzoekers hebben een nieuwe trojan voor externe toegang (Remote Access Trojan of RAT) ontdekt waarvoor reclame wordt gemaakt op een Russisch sprekende ondergronds hack forum. De malware genaamd 'T-RAT' is beschikbaar voor slechts € 38,- ($ 45,-). Het belangrijkste verkoopargument is de mogelijkheid om geïnfecteerde systemen te beheren via een 'Telegram-kanaal' in plaats van een web gebaseerd beheer paneel...

LEES MEER »

FBI:"De recente cyberaanvallen op ziekenhuizen is nog maar het begin"

De recente cyberaanvallen op Amerikaanse ziekenhuizen is nog maar het begin. De Federal Bureau of Investigation (FBI), het ministerie van Volksgezondheid en het Cybersecurity and Infrastructure Security Agency (CISA) zeggen dat cybercriminelen zich voorbereiden op een golf aan ransomware-aanvallen. De hackers zijn volgens de veiligheidsinstanties uit op geld en geven niets om de gezondheid of veiligheid van patiënten. Gezondheidsinstellingen krijgen het advies om hun digitale beveiliging op te schroeven...

LEES MEER »

Oplichting, geweld en beroving: hoe Snapchat misbruikt wordt door criminelen

Snapchat is een populaire app die dagelijks door miljoenen mensen gebruikt wordt. Helaas wordt de app ook steeds vaker misbruikt door criminelen en dat heeft soms verstrekkende gevolgen. Van oplichting tot zelfs geweld en beroving. Maar hoe werkt dat dan? Wij van Cybercrimeinfo.nl mochten bijdragen aan onderstaande video, waarin het Youtube kanaal 'Vrije Vogels' in de huid van oplichters kruipt die via Snapchat hun prooi zoeken. Zo zijn er bijvoorbeeld handelaren die 'Snapchat pakketten' verkopen, waarbij je toegang krijgt tot digitale mappen met foto's om nietsvermoedende mensen op te lichten.
Bekijk onderstaande video om te zien hoe het werkt en krijg inzicht in de donkere kant van de populaire app Snapchat...

LEES MEER »

Beveilig je smartphone tegen hackers met deze 10 praktische tips

Onze smartphones bevatten veel persoonlijke informatie, zoals foto’s, video's, wachtwoorden, bankgegevens en nog veel meer. Tevens gebruikt de meerderheid van de smartphone gebruikers hun smartphone ook voor hun werk. Met deze tips beveilig jij je smartphone en je data nog beter tegen hackers en cybercriminelen...

LEES MEER »

Kamer vragen DDoS-aanvallen

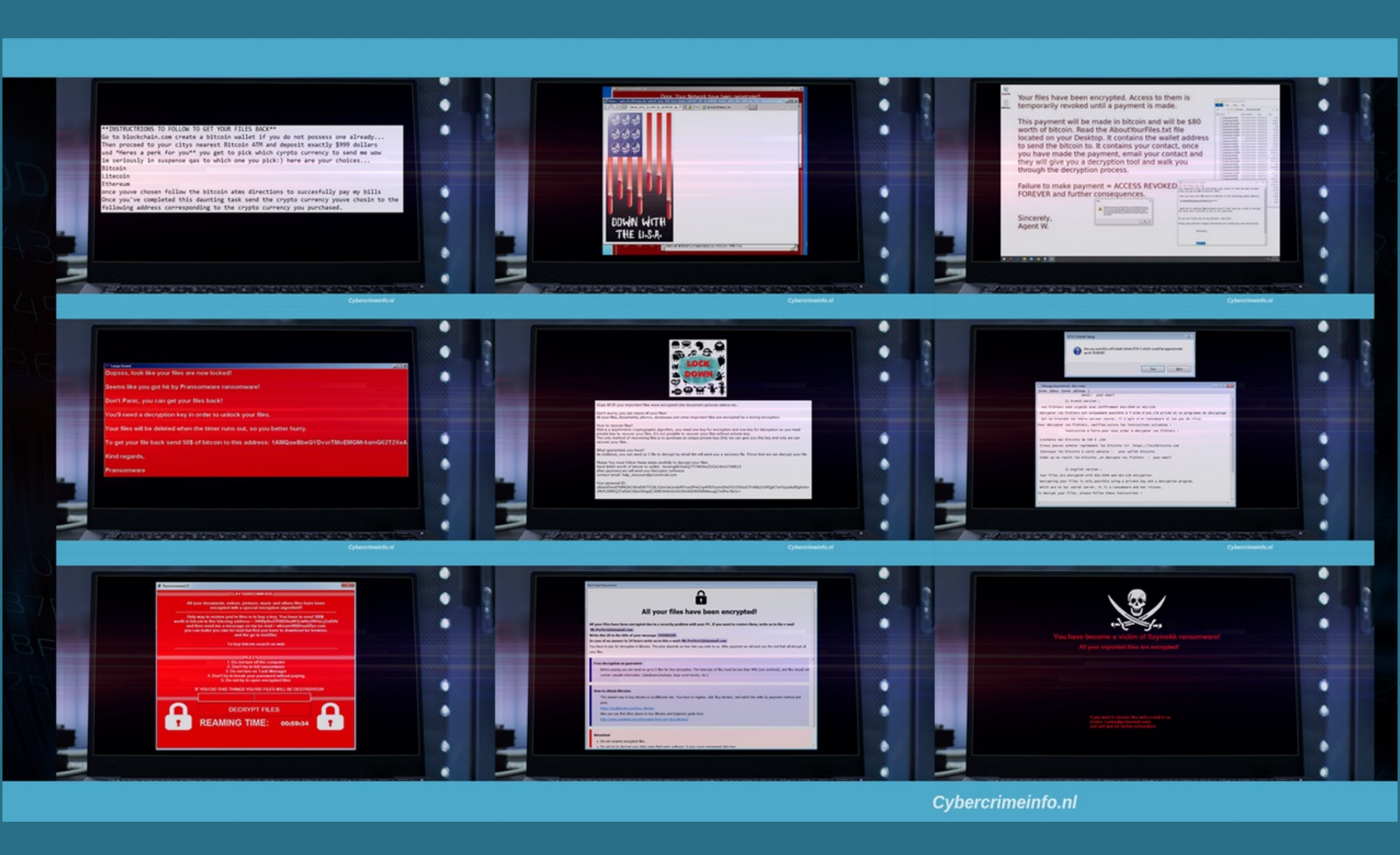
DDoS-aanvallen voorkomen is een onbegonnen zaak. Wel is het mogelijk om de kwetsbaarheid en impact van dergelijke cyberaanvallen te verkleinen. Om dat te bewerkstelligen is het belangrijk dat overheidsinstanties en het midden- en kleinbedrijf (MKB) hierover geïnformeerd worden en samenwerken. Door middel van publiekscampagnes moeten burgers zich bewust worden van de gevaren van DDoS-aanvallen...

LEES MEER »

Berichten lezen voordat ze versleuteld werden

Politie en justitie slaagden er eerder dit jaar in om EncroChat te kraken. Daarbij maakten de opsporingsdiensten meer dan 20 miljoen berichten waarin criminele activiteiten uit de doeken worden gedaan buit. Nu blijkt dat de politie begin 2019 al infiltreerde in de beveiligde chatdienst. Daarbij wist de handhavingsinstantie de hand te leggen op foto’s, notities en financiële gegevens van de chatdienst...

LEES MEER »



Ransomware weekoverzicht week 43 - 2020

Afgelopen week is het druk geweest met nieuws over ransomware, waaronder nieuwe aanklachten tegen door de Russische staat gesponsorde hackers en talloze aanvallen op bekende organisaties. In 2017 was er een aanval waarbij de NotPetya-ransomware werd gebruikt om gegevens op systemen wereldwijd te vernietigen. Deze week heeft de Amerikaanse regering zes Russische inlichtingendiensten, waarvan bekend is dat ze deel uitmaken van de beruchte 'Sandworm'-groep, aangeklaagd wegens hack operaties, waaronder NotPetya. We hoorden ook van talloze aanvallen op grote organisaties, zoals 'Barnes & Noble', het 'Monreal openbaar vervoer (STM)', 'Sopra Steria' en 'Boyne Resorts'...

OVERZICHT »

Datalek nieuws en overzicht week 44-2020

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 »

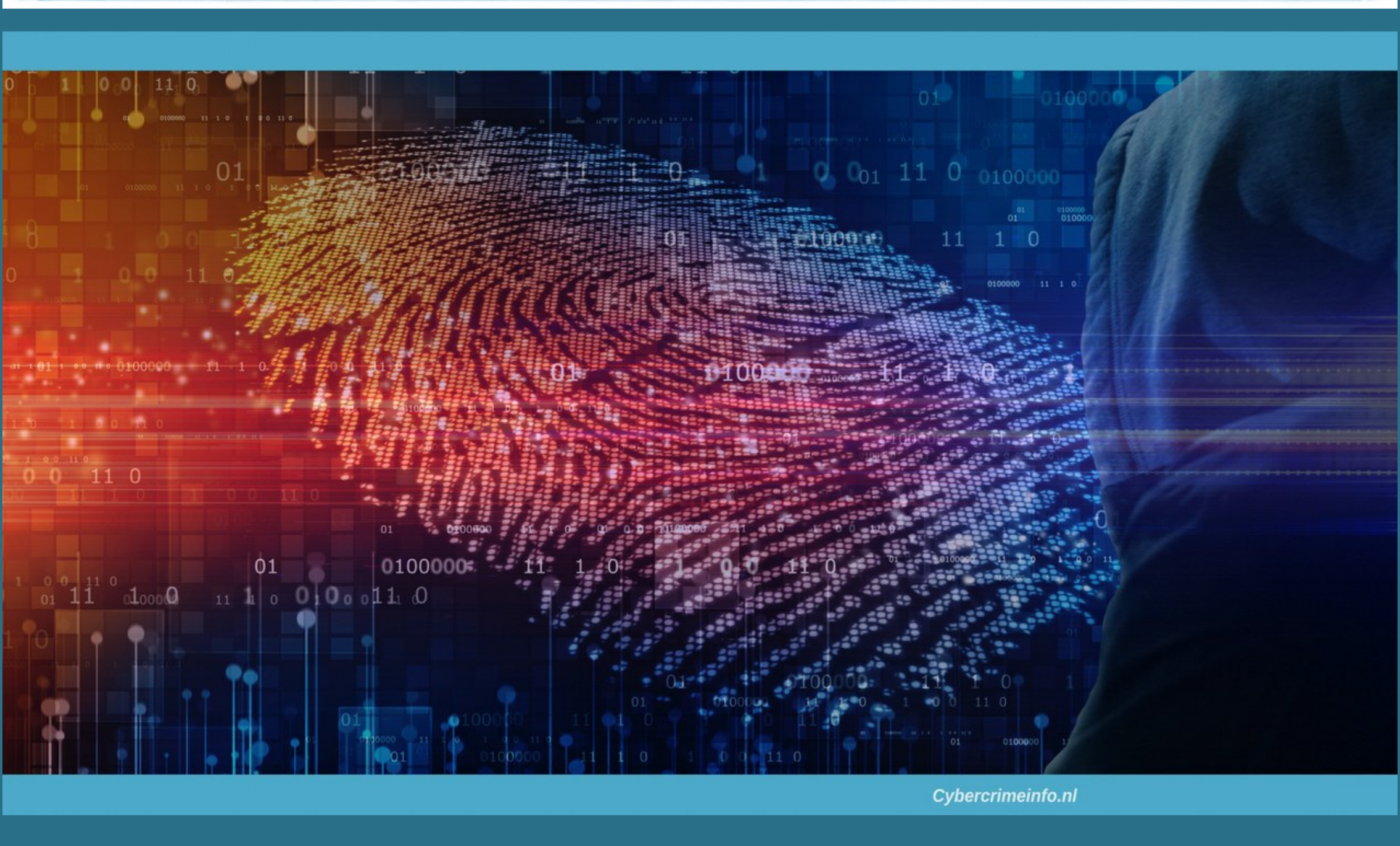
Gezochte Personen

Ijmuiden - Geld opnemen met gestolen pinpas na Whatsapp-fraude

Op dinsdagmiddag 16 juni 2020 wordt een 59-jarige vrouw uit Amsterdam via Whatsapp opgelicht. Ze maakt geld over naar een rekeningnummer en een onbekende man neemt dat geld nog diezelfde dag op bij een geldautomaat aan de Planetenweg in IJmuiden. De transactie en een verdachte staan op beeld. Het slachtoffer ontvangt die dinsdagmiddag rond 16.00 uur een Whatsapp-bericht van een onbekend nummer. In het bericht geeft haar ‘zoon’ aan dat hij een nieuw telefoonnummer heeft. Het slachtoffer twijfelt niet aan het bericht en denkt dat ze inderdaad met haar zoon aan het appen is...

LEES MEER »

Dark Web

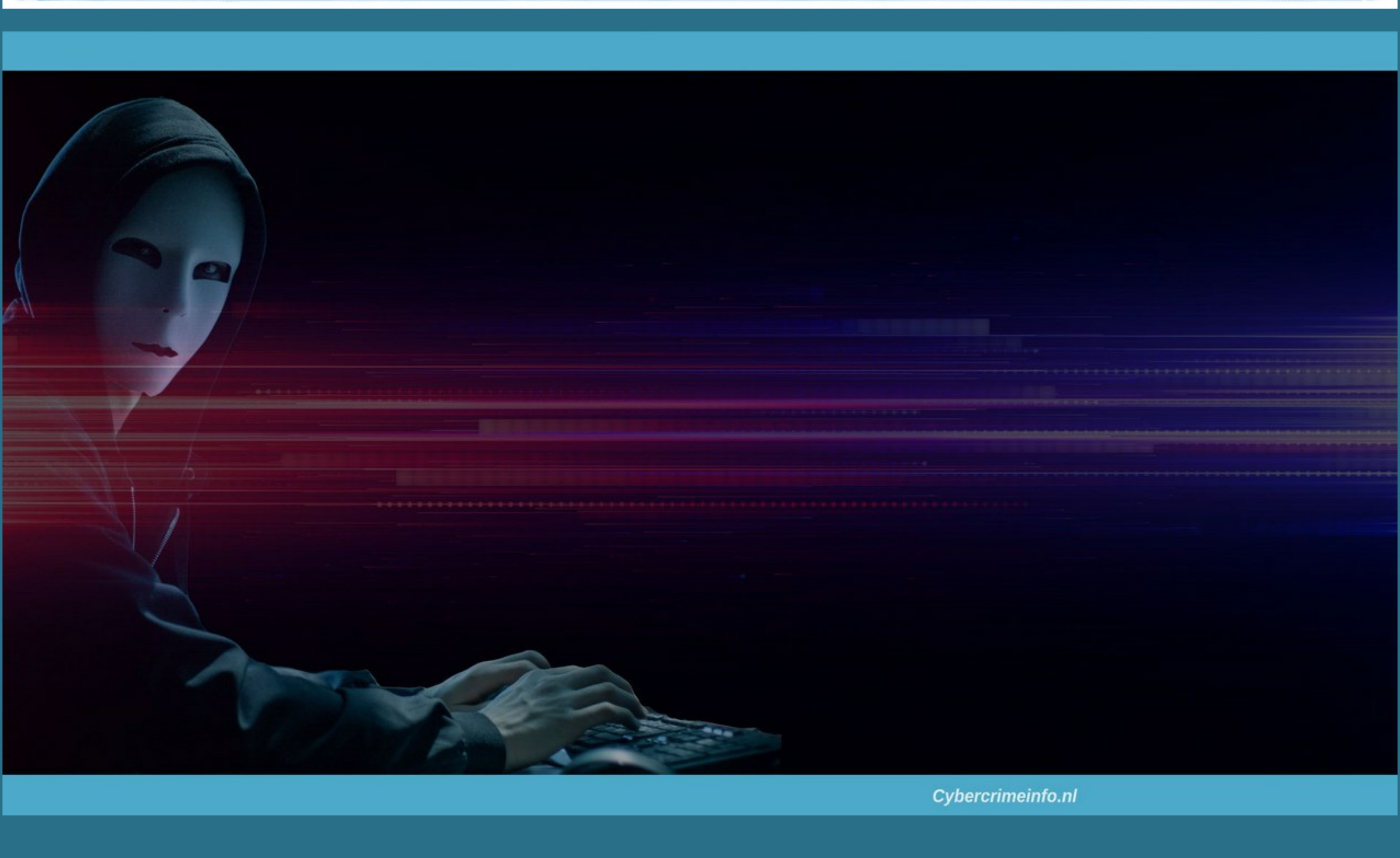


Tweestapsverificatie vingerafdruk te koop met e-mailadressen en wachtwoorden

Beveiliging op het internet is een eindeloos kat-en-muisspel. Terwijl beveiligingsspecialisten voortdurend nieuwe manieren bedenken om onze digitale gegevens te beschermen, verzinnen cybercriminelen nieuwe sluwe manieren om die verdediging te omzeilen. Onderzoekers van de TU/e hebben nu bewijs gevonden van een geavanceerde Russische online marktplaats die honderdduizenden zeer gedetailleerde gebruikersprofielen verhandelt. Deze 'fingerprints' stellen criminelen in staat om ultramoderne tweestapsverificatie te omzeilen, waardoor ze toegang krijgen tot waardevolle gebruikersinformatie, zoals creditcardgegevens...

LEES MEER »

Wat is?



Wat is phishing per post?

Phishing is inmiddels een term die de meeste onder ons wel kennen, want phishing is een populaire truc bij cybercriminelen. Vaak is phishing (of spearphishing) het begin van de meest voorkomende cyberaanvallen. Cybercriminelen proberen je te lokken naar een plek waar ze kunnen toeslaan. Ze lokken of verleiden je door het gemak van een link aan te bieden die ervoor zorgt dat je snel kunt handelen en zo gelijk op de juiste pagina, app of bank omgeving terecht komt. We zien dat er op deze basis kenmerken van phishing is verder geborduurd. Zo kwam er enkele jaren geleden 'smishing' hengelen naar je gegevens via SMS of whatsApp bij...

LEES MEER »

De week in beeld »