

Nieuwsbrief 132 - Week 46-2020



Cybercrimeinfo.nl

Criminelen gaan nu nog een stap verder na spoofing

De politie waarschuwt voor een vorm van bank helpdeskraude, ook wel spoofing genoemd, waarbij een nep bankmedewerker naar de woning van het slachtoffer gaat. Er zijn inmiddels al een aantal gevallen bekend waarbij slachtoffers duizenden euro's zijn kwijtgeraakt. Een "medewerker van hun bank" kwam naar het huis van de slachtoffers of om geld over te maken op een zogenaamde "veilige rekening", dit heet een "kluisrekening", of om de pinpas van het slachtoffer op te halen...

[LEES MEER »](#)



Cybercrimeinfo.nl

"Binnen minuut alles kwijt"

Internetcriminelen maakten dit jaar miljoenen euro's buit via spoofing. Dit is een gewiekste vorm van oplichting, waarbij slachtoffers hun zuurverdiende centen zelf overhevelen naar zogenaamd veilige rekeningen. "Achteraf bleek alles fake." "Op mijn lopende bankrekening stond letterlijk geen cent meer", vertelt Luk Leclercq, die december vorig jaar slachtoffer werd van spoofing. De rekening waar naar hij geld overmaakte, bleek in handen van criminelen die zich voordeden als zijn bank...

[LEES MEER »](#)



Cybercrimeinfo.nl

Tweede Kamerverkiezingen 2021 met behulp van "niet" hackbaar OSV systeem?

De Kiesraad kiest eieren voor zijn geld. Bij de volgende Tweede Kamerverkiezingen, die in maart 2021 plaatsvinden, gaat ze extra controles uitvoeren om de uitslagen vast te stellen. De 'Ondersteunende Software Verkiezingen' (OSV) is hiervoor ontwikkeld en veilig bevonden, maar de Stichting 'Tegen Hackbare Verkiezingen' waarschuwt voor fraude...

[LEES MEER »](#)



Cybercrimeinfo.nl

Zes getroffen ziekenhuizen met ransomware in een staat kregen hulp van de Nationale Garde

Gouverneur Phil Scott van de Amerikaanse staat Vermont heeft de 'Nationale Garde' van de staat ingezet om zes door ransomware getroffen ziekenhuizen te helpen. De zes ziekenhuizen en medische centra van het 'University of Vermont Health Network' raakten eind oktober besmet met ransomware...

[LEES MEER »](#)



Cybercrimeinfo.nl

De meest gebruikte malware en kwetsbaarheden aanvallen

'Trickbot'- en 'Emotet'-trojans zijn in oktober nog steeds de top twee van meest voorkomende malware. De trojans zijn verantwoordelijk voor de sterke toename van ransomware aanvallen op ziekenhuizen en zorgverleners wereldwijd. De FBI en andere Amerikaanse overheidsinstanties hebben onlangs een waarschuwing afgegeven over ransomware aanvallen gericht op de gezondheidszorg, waarbij wordt gewaarschuwd dat de naar schatting meer dan een miljoen Trickbot-infecties wereldwijd worden gebruikt om bestand versleutelende ransomware zoals Ryuk te downloaden en te verspreiden...

[LEES MEER »](#)



Cybercrimeinfo.nl

De gevaren van IoT zichtbaar in Rotterdam

Tot dinsdagmiddag was het voor iedereen mogelijk om de kleuren van de Erasmusbrug aan te passen via zijn tablet, smartphone of laptop. Door een gat in de beveiliging was het mogelijk om zonder gebruikersnaam en wachtwoord in te loggen op het systeem dat de lichtkleuren regelt. De gemeente Rotterdam heeft het bedieningssysteem uitgeschakeld en contact opgenomen met de leverancier van het systeem om herhaling te voorkomen...

[LEES MEER »](#)



Cybercrimeinfo.nl

"Ze zij zijn hun gewicht in goud waard. Hierdoor konden we twee verdachten op heterdaad aanhouden"

Bank helpdeskrans en babbeltrucs komen dagelijks voor en heeft een grote impact op de slachtoffers. Dinsdag 10 november was het helaas ook weer raak. Een 70-jarige vrouw uit Dordrecht is het slachtoffer geworden van Bank helpdeskrans fraude en een poging tot babbeltruc. Door adequaat optreden van de bureaus van het slachtoffer, konden de verdachten op heterdaad worden aangehouden. Ook in andere babbeltruc zaken in Dordrecht zijn aanhoudingen verricht. Mooie resultaten in impact volle zaken...

[LEES MEER »](#)



Cybercrimeinfo.nl

Ransomware weekoverzicht week 45-2020

Afgelopen week is het druk geweest met wereldwijde aanvallen en is een van de grootste ransomware criminele operaties Maze "officieel" gestopt. De week begon met de "officiële" aankondiging van de beruchte cybercriminelen dat ze zouden stoppen met de 'Maze-ransomware'. Tevens is vernomen dat veel van de aangesloten criminele organisaties nu overstappen op een nieuwere ransomware-operatie genaamd 'Eggor'. Er verscheen ook een nieuwe ransomware genaamd 'RegretLocker' die de Windows Virtual Storage API's gebruikt om virtuele machine harde schijven (VHD's) te koppelen om elk bestand afzonderlijk te versleutelen...

[OVERZICHT »](#)



Cybercrimeinfo.nl

Fraudehulpdesk en Opgelicht?! meldingen week 46-2020

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, smilere bericht of werd je gebeld en vertrouwd je het niet? Laat het ons, of onze collega's van Opgelicht?! of Fraudehulpdesk dan weten want Samen bestrijden we cybercrime. Liever anoniem? Klik dan hier.

[OVERZICHT »](#)

Cybercrimeinfo.nl

Datalek nieuws en overzicht week 46-2020

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 meld is aan de 'Autoriteit persoons gegevens (AP)' laat het ons dan weten, want bij een datalek moet er snel gehandeld worden om mogelijk catastrofale gevolgen te voorkomen. O, ja, doe je dit liever anoniem dan kan dit hier.

[OVERZICHT »](#)

Cybercrimeinfo.nl

Gezochte Personen

Cybercrimeinfo.nl

Holten - Wie zijn deze pingers?

Een vrouw opende op zaterdag 15 augustus een email die ze van haar bank had ontvangen. Om blokkade van haar rekening te voorkomen klikte ze op de link in de mail en vulde de gevraagde gegevens in. Daarna werd het slachtoffer gebeld door iemand die zich voordeed als bankmedewerker. Om haar geld veilig te stellen moest ze het tijdelijk naar andere rekeningen verplaatsen. Nadat ze de instructies had opgevolgd werd het gesprek beëindigd. Het geld van het slachtoffer is vervolgens op verschillende locaties door verschillende personen gepind. Hiervan zijn beelden...

[LEES MEER »](#)

Cybercrimeinfo.nl

Dark Web

Cybercrimeinfo.nl

Naar schatting 85 miljoen euro aan Covid-gerelateerde goederen en diensten die te koop worden aangeboden op het darkweb

Na Donald Trump's snelle herstel van Covid-19 vorige maand, verschenen er advertenties op het darkweb ("de onderkant van het internet") waarin het medicijn van 'Regeneron Pharmaceuticals Inc.' werd aangeboden waarbij ze beweerden dat dit het 'wondermiddel' was wat de president snel beter maakte. Terwijl het nog niet was goedgekeurd voor openbare verkoop...

[LEES MEER »](#)

Cybercrimeinfo.nl

Wat is?

Cybercrimeinfo.nl

Wat is spoofing?

Spoofing is het aannemen van een andere identiteit. Dit kan worden gedaan met een e-mailadres, telefoonnummer, website of IP-adres...

[LEES MEER »](#)

[De week in beeld »](#)

Deze e-mail is verzonden aan [\[email\]](#). • Als u geen nieuwsbrief meer wilt ontvangen, kunt u zich [hier afmelden](#). • U kunt ook uw [gegevens inzien en wijzigen](#). • Voor een goede ontvangst voegt u [info@cybercrimeinfo.nl](#) toe aan uw adresboek.

 Laposta