

Nieuwsbrief 48 (week 14-2019) - © CCINL |
www.cybercrimeinfo.nl



47.000 computers besmet met Emotet Malware

Antispam organisatie Spamhaus heeft 47.000 computers ontdekt die met de Emotetmalware besmet zijn. Emotet bestaat al sinds 2014 en was oorspronkelijk malware voor het stelen van bankgegevens. Inmiddels is het een "modulaire malwarefamilie" die allerlei aanvullende malware op systemen kan installeren...

[LEES MEER >>](#)



Ransomware infecteert hoofdstad staat New York

Systemen van de Amerikaanse stad Albany, hoofdstad van de staat New York, zijn afgelopen weekend met ransomware besmet geraakt. De beveiligingssoftware van de stad, die 98.000 inwoners telt, ontdekte de ransomware. Vanwege de infectie werden burgers die huwelijks-, geboorte- en overlijdenscertificaten wilden aanvragen naar een andere stad doorgestuurd. Ook vergunningsaanvragen kon de stad niet meer afhandelen...

[LEES MEER >>](#)



CCINL ontvangt veel meldingen over '50 uur om te betalen'

De mail begint als volgt: 'Ik heb slecht nieuws voor je.' In de mail wordt beschreven dat jouw besturingssysteem gehackt is en de hacker volledige toegang heeft tot jouw mailaccount. Dit lijkt behoorlijk echt doordat de mail van jouw eigen e-mailadres verstuurd is maar de hacker heeft geen toegang tot jouw account...

[LEES MEER >>](#)



3,3 miljoen Nederlanders in 2018 slachtoffer van Cybercrime!

Een computer of netwerk werd besmet (ransomware), of iemand kreeg toegang tot een e-mailadres of account op sociale media (hacking). Ongeveer 300.000 mensen werden de dupe van identiteitsfraude. Volgens het bedrijf Symantec hebben in totaal 5,8 miljoen Nederlanders weleens te maken gehad met cybercrime. Twee op de drie mensen verwachten dat ze het komende jaar getroffen worden...

[LEES MEER >>](#)



CT- en MRI-Scan via mitm aanval te hacken

De CT- en MRI-scans die ziekenhuizen uitvoeren zijn kwetsbaar voor man-in-the-middle-aanvallen, waardoor aanvallers tumoren in de scan resultaten kunnen verwijderen of toevoegen. Hierdoor lopen patiënten risico op een verkeerde diagnose, aldus onderzoekers van de Ben-Gurion University...

[LEES MEER >>](#)



Phishingaanval op iPhone-gebruikers via configuratieprofiel

iPhone gebruikers zijn het doelwit van een phishingaanval geworden waarbij aanvallers het slachtoffer zover proberen te krijgen om een configuratieprofiel te installeren. Configuratieprofielen zijn eigenlijk bedoeld voor ontvangers en beheerders en maken het mogelijk om allerlei instellingen aan te passen...

[LEES MEER >>](#)



Cybercrime? Laat je niet verrassen!

Meer info? www.cybercrimeinfo.nl

Aangifte cybercrime? www.politie.nl

Interesse in een presentatie over Cybercrime?

"We merken dat daar veel behoefte aan is", ook behoefte aan een presentatie?

Mail dan naar info@cybercrimeinfo.nl

© CCINL | "Samen voor veiligheid"

Missie: 'Bestrijding en weerbaarheid verhogen, voor de crime van de toekomst/heden'...

[LEES MEER >>](#)



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 Inschrijven voor de berichtenservice kan door [HIER](#) te klikken.

Tik vervolgens in de balk chatbericht het woord "ja" om de berichten automatisch te ontvangen.

© CCINL | www.cybercrimeinfo.nl

© CCINL | "Samen voor veiligheid"



Wat is Man In The Middle Attack?

Sinds het mogelijk is om berichten te versturen, loopt men ook het gevaar dat berichten worden onderschept of ongemerkt worden gemanipuleerd. Vroeger werden daarvoor bodes opgewacht of telefoons afgetapt; tegenwoordig biedt het internet aanzienlijk subtielere manieren om te spioneren. Een groot deel van het wereldwijde dataverkeer gaat via openbare netwerken – en dat vaak ook nog zonder fatsoenlijke encryptie. Daar komt nog bij dat de overdrachtswegen binnen het wereldwijde computernetwerk voor gebruikers ondoorzichtig zijn...

[LEES MEER >>](#)



Nieuwsbrief gemist?

Geen probleem, ga naar [Nieuwsbrief archief en download](#) de Nieuwsbrieven.

Nog niet ingeschreven voor de wekelijkse nieuwsbrief?

[Meld u dan aan voor onze nieuwsbrief >>](#)

We vragen geen geld en doen dit vrijwillig

Maar een beoordeling voor ons werk zouden we zeer waarderen

Missie website: 'Bestrijding en weerbaarheid verhogen, voor de crime van de toekomst/heden'

© CCINL | www.cybercrimeinfo.nl

We zouden het zeer waarderen als u een online recensie voor ons wilt schrijven.

Beoordeel ons op 'Klanten vertellen'

Beoordeel ons op 'Facebook'

Beoordeel ons op 'Google' (rechter kolom knop "Een Review Schrijven")

Bedankt alvast,

Peter Lahousse

© CCINL | www.cybercrimeinfo.nl

Missie: 'Bestrijding en weerbaarheid verhogen, voor de crime van de toekomst/heden'

Deze e-mail is verstuurd 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.

