



## Nieuwsbrief 225 - Week 35-2022

**“Many cybercriminals target small businesses in an attempt to gain access to larger organizations”**

Lees verder

**Cyber criminals respond to energy crisis**

**Cybercriminelen springen in op energiecrisis**

Cybercriminelen hebben een nieuwe manier bedacht om slachtoffers te maken. Ze sturen berichten naar nietsvermoedende slachtoffers waarin staat dat ze recht hebben op energietoeslag om de energierekening te betalen. In werkelijkheid is het een phishingbericht, bedoeld om bank- en andere privégegevens van mensen te bemachtigen en geld van hun rekening te stelen. Dat blijkt uit onderzoek van RTL Nieuws. Volgens de nieuwszender zijn honderden Nederlanders in deze valstrik getrap.

Lees verder

**“Attacks by state hackers are sophisticated and often use little-known techniques”**

**“Aanvallen door staatshackers zijn geavanceerd en gebruiken vaak nog amper bekende technieken”**

Cybersecurity Venafi maakt de resultaten bekend van een onderzoek naar de impact van het toenemend aantal cyberaanvallen door staatshackers en de recente geopolitieke ontwikkelingen. 64% van ruim 1.100 ondervraagde securitymanagers denkt dat hun organisatie is aangevallen door hackers die in opdracht van landregeringen werken. Verder heeft 66% de cyberstrategie aangepast in reactie op het conflict tussen Rusland en de Oekraïne.

Lees verder

**“A thousand reviews with an average score of 9.3/10” is sophisticated malware**

**“Duizend reviews met een gemiddelde score van 9,3/10” blijkt sluwe malware te zijn**

Crypto mining malware heeft op sluwe wijze honderdduizenden computers over de hele wereld geïnfecteerd. Uit nieuw onderzoek blijkt dat deze software vaak vermomd als legitiem programma binnenkomt, bijvoorbeeld als een Google Translate applicatie.

Lees verder

**In the depths of the dark web**

**In de krochten van het darkweb**

Hoe gaat het toch met het darkweb? Geen vraag die elke dag in je opkomt, maar De Technoloog vond het toch echt wel tijd voor een update. Marco Corradin was in 2019 al te gast in de podcast om te praten over deze mysterieuze, donkere kant van het internet. Nu praat hij ons bij over alle ontwikkelingen van de laatste drie jaar. Zo is Tor nog altijd zeer belangrijk, maar is Bitcoin inmiddels echt passe, als betaalmiddel voor criminelen.

Lees verder

**'s -Gravenzande - Bankhelpdesk fraude**

Wie herkent deze personen?

Een oplichter misleidde op vrijdag 27 mei een ouder echtpaar uit 's-Gravenzande. Een vrouw deed alsof ze bij een bank werkte en een echtpaar moest overtuigen, waarvoor ze hun bankpassen moest meenemen. Later bracht nog een nepagent een bezoek aan dit echtpaar en nam sieraden mee. We tonen beelden van een persoon die pinde met de bankpassen bij een automaat op de Pretoriaaan in Rotterdam.

Lees verder

**CYBER ATTACKS**

WEEK OVERVIEW

34-2022

**Overzicht cyberaanvallen week 34-2022**

Frans ziekenhuis moeta patiënten weigeren wegens ransomware-aanval, ransomwaregroep steelt privédata bijstandsonvangers Belgische gemeente en Griekse gasnetbeheerder Desfa getroffen door ransomware-aanval. Hier het overzicht van afgelopen week en het nieuws van dag tot dag.

**Bekijk het weekoverzicht**



Share Tweet Share Pinterest

**Steun Cybercrimeinfo zodat we kunnen blijven bestaan**

Om deze website te runnen en iedereen te kunnen blijven voorzien van het laatste nieuws, tips en tricks over digitale criminaliteit, zijn wij op zoek naar donateurs. Hiervan kunnen we onder andere nieuwe apparatuur aanschaffen, want deze hele site draait op vrijwilligers. Kortom, wij kunnen niet zonder jouw steun! Help je mee in de strijd tegen cybercrime? Iedere donatie, hoe klein ook, is van harte welkom. Alvast bedankt namens het hele team van Cybercrimeinfo.

Doneren kan al vanaf 5 euro!

**Doneer**

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](mailto:info@cybercrimeinfo.nl) toe aan uw adresboek.

