Cybercrimeinfo.nl (ccinfo.nl) Bekijk de webversie

Nieuwsbrief 266 - Week 24-2023

Nieuwe dreiging op de digitale golven: De strijd tegen Russische hackers en DDoS-aanvallen op Nederlandse havens.

In het tijdperk van digitalisering vormt cybercriminaliteit een voortdurende zorg voor veel organisaties wereldwijd. Recentelijk werden verschillende Nederlandse havenbedrijven getroffen door gerichte Distributed Denial-of-Service (DDoS) aanvallen, wat resulteerde in aanzienlijke verstoringen. De DDoS-aanvallen waren specifiek gericht op de websites van deze bedrijven, waardoor ze uren tot dagen onbereikbaar waren. Hoewel de interne systemen van de havens niet werden aangevallen, waren de aanvallen ontwrichtend. De daders, een groep genaamd 'NoName057(16)', zijn hacktivisten die digitale aanvallen uitvoeren op entiteiten die zij als tegenstanders van Rusland zien. Deze reeks aanvallen benadrukt de noodzaak voor organisaties om hun cyberbeveiligingsmaatregelen voortdurend te herzien en bij te werken om zich te beschermen tegen dergelijke dreigingen.

Lees verder

Cybercriminaliteit in 2023: De evolutie van tools en technieken

De wereld van cyberbeveiliging is voortdurend in beweging. Elk jaar brengt nieuwe bedreigingen en uitdagingen met zich mee, waardoor organisaties en individuen hun beveiligingsprotocollen voortdurend moeten herzien en bijwerken. Het jaarlijkse 'Human Factor Rapport' van Proofpoint biedt inzicht in het cybercriminele landschap. Uit het rapport blijkt dat cybercriminelen hun activiteiten hebben verhoogd en gebruikmaken van ongebruikelijke tools en technieken om hun doelen te bereiken. Het rapport benadrukt de toename van de snelheid en complexiteit van aanvallen, evenals het gebruik van minder bekende exploits en bestandstypen. Het beveiligen van systemen en gegevens wordt steeds complexer, en naast robuuste beveiligingsoplossingen is het belangrijk om preventieve maatregelen te nemen en een cultuur van beveiligingsbewustzijn te creëren. De strijd tegen cybercriminaliteit vereist voortdurende inspanningen van iedereen om systemen en gegevens veilig te houden.

Lees verder

Opkomst en ondergang van een internationaal darkweb-drugsimperium: Een baanbrekende zaak

De wereld van de darkweb-drugshandel heeft een grote klap gekregen met het recente vonnis van het Gerechtshof in 's-Hertogenbosch, Nederland. In een baanbrekende zaak die meer dan 14 maanden duurde, heeft het hof een grootschalige internationale handel in verdovende middelen via het darkweb aan het licht gebracht. Het vonnis, ECLI:NL:GHSHE:2023:1948, werpt licht op de activiteiten van een criminele organisatie die betrokken was bij de distributie van illegale stoffen, waarbij verschillende opslagplaatsen werden gebruikt om de drugs op te slaan. Dit baanbrekende vonnis getuigt van de voortdurende strijd tegen druggerelateerde misdrijven en de vastberadenheid van wetshandhavingsinstanties om deze illegale activiteiten te bestrijden.

Lees verder

Tip van de week: Hoe beschermen tegen DDoS-aanvallen

Bescherm uw netwerk tegen DDoS-aanvallen door preventieve maatregelen te nemen en effectief te reageren op deze cyberdreiging. DDoS-aanvallen zijn een ernstige bedreiging die netwerken, servers en diensten overbelasten, waardoor bedrijven en organisaties onbereikbaar worden. Het is belangrijk om te investeren in professionele DDoS-beschermingsdiensten die geavanceerde technologieën en expertise bieden om de bronnen van een aanval te detecteren en neutraliseren. Daarnaast kan het vergroten van de bandbreedte en het hebben van een redundante netwerkinfrastructuur helpen om de impact van een DDoS-aanval te beperken. Het vroegtijdig detecteren van aanvallen en het hebben van een responsplan zijn ook essentiële stappen om de schade te beperken. Bewustzijn, planning en investering in goede beveiligingspraktijken en -technologieën zijn cruciaal om de continuïteit van online activiteiten te waarborgen en de risico's van cyberaanvallen te beheersen.

Lees verder

Overzicht cyberaanvallen week 23-2023

In week 23-2023 zijn er verschillende cyberaanvallen opgemerkt. Microsoft OneDrive is getroffen door DDoS-aanvallen, waardoor het wereldwijd offline ging. Landal GreenParks heeft een datalek ontdekt en heeft 12.000 gasten gewaarschuwd. Er is ook een ransomware-hack geweest bij Belgische bedrijfsaccounts, waarbij een half miljoen accounts zijn blootgelegd. In het Verenigd Koninkrijk is er een bevestiging van een mega-hack bij Britse bedrijven met mogelijke Russische betrokkenheid. In België is phishing een groeiend probleem, waarbij bijna 40 miljoen euro verloren is gegaan in 2022. Daarnaast is er ook aandacht voor de SpinOk Android-malware, die op 30 miljoen extra apparaten is geïnstalleerd. Dit is een overzicht van de cyberaanvallen van de afgelopen week.

Bekijk het weekoverzicht

Eindhoven - Bankhelpdesk fraude

De politie is op zoek naar een pinfraudeur die betrokken is bij spoofing en pinfraude op verschillende locaties, waaronder Valkenswaard, Eindhoven en Rotterdam. De verdachte pleegt grote geldopnames met een bankpas die niet van hem is, maar van een 75-jarige vrouw uit Valkenswaard. De vrouw werd eerder gebeld door een nepbankmedewerker die haar bankgegevens wist te verkrijgen met een smoes. Als u informatie heeft over deze zaak, kunt u dit doorgeven via het tipformulier. De verdachte is te zien op afbeeldingen waarop hij ook de bankpas bij de vrouw thuis heeft opgehaald. Hij draagt een donkere hoody met een slangenafbeelding op de rug en is gezien bij verschillende winkels en een pinautomaat in Eindhoven. Uit onderzoek blijkt dat de pas ook in Rotterdam is misbruikt, dus mensen in die omgeving kunnen de verdachte mogelijk herkennen. Als u wilt helpen bij de opsporing, kunt u een tip doorgeven via het tipformulier of telefonisch via 0800-6070. Anoniem een tip doorgeven is ook mogelijk via 0800-7000.

Lees verder

Actuele cyberassistent die 24/7 beschikbaar is!

"De Cybercrimeinfo AI Chatbot - Elke dag getraind, elke dag beter in de strijd tegen digitale criminaliteit."

De Cybercrimeinfo AI Chatbot staat altijd paraat om uw vragen te beantwoorden over cybercriminaliteit, het darkweb en cybersecurity. Deze chatbot is exclusief verbonden met de Cybercrimeinfo-database en vertrouwt alleen op zorgvuldig gecontroleerde informatie uit deze bronnen. Alle informatie die de bot biedt, is grondig gecontroleerd en betrouwbaar. Hoewel de chatbot gespecialiseerd is in cybercriminaliteit, cybersecurity en het darkweb, kan hij voor vragen buiten dit domein toegang hebben tot internetbronnen om u van relevante en actuele informatie te voorzien. Wat de chatbot echt uniek maakt, is de wekelijkse update van informatie over cyberaanvallen, kwetsbaarheden, opsporingsnieuws en betrouwbare artikelen over cybersecurity, cybercrime en het darkweb. Klik hieronder om het volledige artikel te lezen op onze website.

AI Chatbot

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

Share Tweet Share Pinterest