Nieuwsbrief 336

Reading in □□ or another language

Nederland in de top 5 van meest getroffen landen door mobiele malware

Nederland behoort tot de top vijf landen wereldwijd die het zwaarst getroffen worden door mobiele malware, naast onder andere de Verenigde Staten en India. De hoge adoptie van technologie, de welvaart en geavanceerde digitale infrastructuur maken Nederland een aantrekkelijk doelwit voor cybercriminelen. Mobiele malware komt in verschillende vormen voor, zoals banking malware, spyware, ransomware en phishing-apps. Deze vormen van malware kunnen financiële schade aanrichten, persoonlijke gegevens stelen of apparaten versleutelen. De gevolgen zijn groot, zowel voor particulieren als bedrijven, met risico's zoals identiteitsdiefstal en financiële verliezen. Om deze dreigingen te bestrijden, wordt aangeraden om bewust om te gaan met app-downloads, beveiligingssoftware te installeren, toestemmingen te beperken en regelmatig back-ups te maken. Voor bedrijven is het essentieel om mobiele apparaten goed te beheren en duidelijke veiligheidsrichtlijnen te implementeren.

Lees verder

Reading in □□ or another language

Hybride cyberaanvallen: de vervagende lijnen tussen staten en criminelen

De grens tussen cybercriminelen en door staten gesponsorde aanvallers vervaagt steeds meer, wat leidt tot een gevaarlijke nieuwe vorm van cyberaanvallen: hybride aanvallen. In deze aanvallen combineren overheden en criminelen hun middelen en technieken om zowel financiële als geopolitieke doelen te bereiken. Recente voorbeelden tonen aan dat landen als Rusland en Noord-Korea steeds nauwer samenwerken met criminele groeperingen om cyberaanvallen uit te voeren op onder andere Oekraïense militaire systemen en bedrijven in de ruimtevaart. Ransomware blijft daarbij een grote bedreiging, vooral voor kritieke infrastructuren zoals de gezondheidszorg. Ook het gebruik van kunstmatige intelligentie (AI) speelt een belangrijke rol, zowel bij de aanvallers als bij de verdedigers. AI maakt cyberaanvallen effectiever en moeilijker te detecteren, maar biedt ook kansen voor snellere respons door beveiligingsteams. Internationale samenwerking en strengere wetgeving zijn essentieel om deze groeiende dreiging te kunnen stoppen.

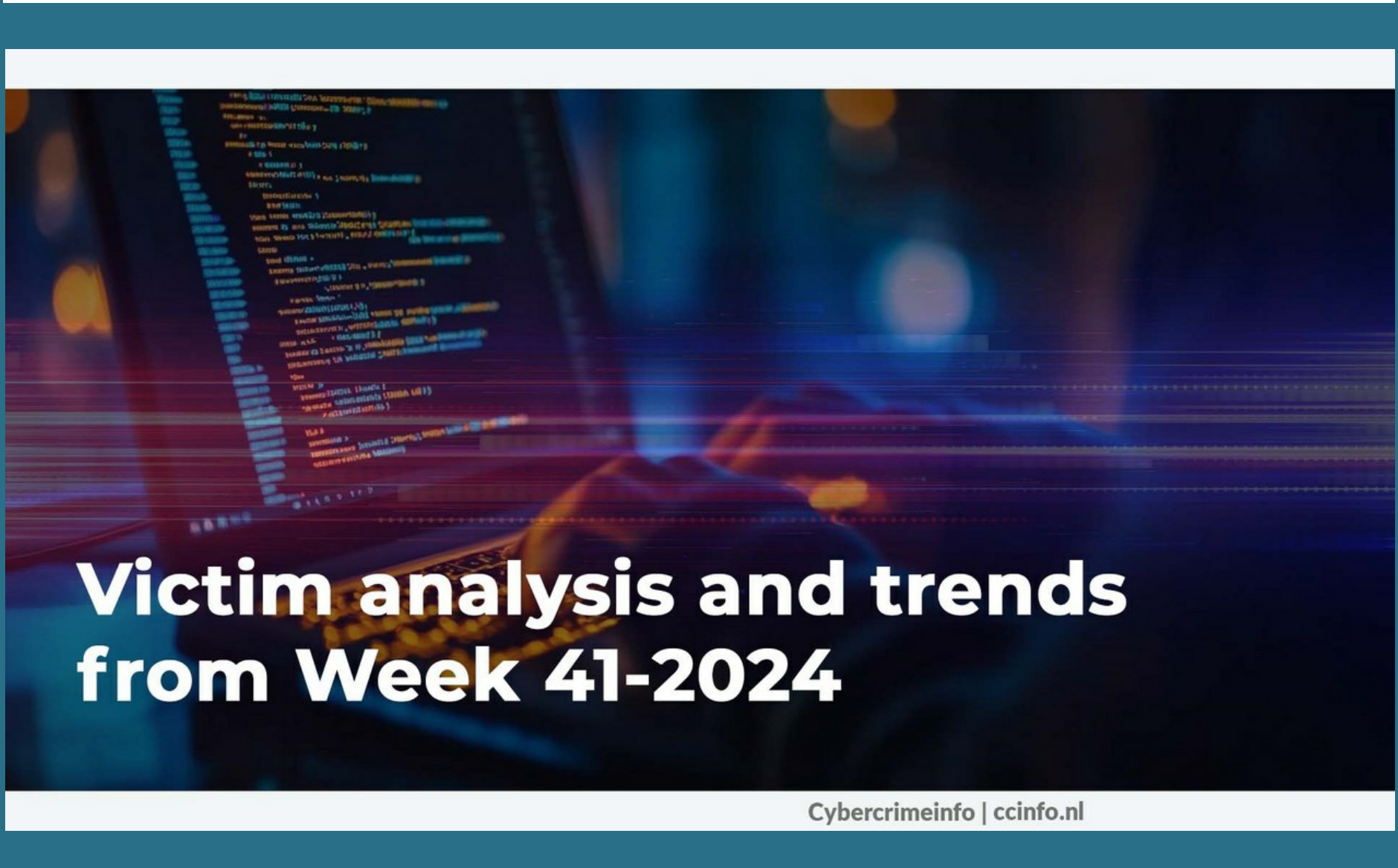
Lees verder

Reading in □□ or another language

De jacht op Bohemia/Cannabia: Een kijken achter de schermen van Darkweb-criminaliteit

In een grootschalige internationale operatie is de darkweb-marktplaats Sipultie ontmanteld, een platform dat vooral bekend stond om de anonieme handel in illegale drugs. Wetshandhavingsinstanties uit Finland, Zweden en andere landen werkten nauw samen om de servers van Sipultie offline te halen en diverse betrokkenen te arresteren. Dit benadrukt het belang van internationale samenwerking in de strijd tegen darkweb-criminaliteit. Sipultie, dat in 2023 werd opgericht als opvolger van Sipulimarket, trok snel veel gebruikers aan en realiseerde een omzet van 1,3 miljoen euro. Ondanks de anonimiteit en beveiligde communicatie op het darkweb, bewijst de sluiting van Sipultie dat zelfs de meest verborgen platforms niet ongrijpbaar zijn. Naast de sluiting van het platform werden ook belangrijke kopers en verkopers geïdentificeerd, wat een grote slag betekent tegen de georganiseerde misdaad op het darkweb.

Lees verder



Reading in □□ or another language

Slachtofferanalyse en Trends van Week 41-2024

In week 41 van 2024 werden verschillende sectoren hard getroffen door cyberaanvallen in Nederland, België en andere delen van de wereld. In Nederland werd een jeugdzorgorganisatie gehackt, waarbij ruim 10.000 e-mailadressen werden blootgelegd. Hoewel geen gevoelige medische informatie is gestolen, blijft de impact op het vertrouwen groot. In België werd Decathlon slachtoffer van een credential stuffing-aanval, waarbij klantgegevens werden misbruikt om spaarpunten te stelen. Daarnaast werden Europese overheidsnetwerken getroffen door geavanceerde aanvallen met op maat gemaakte malware, die zelfs netwerken zonder internettoegang wisten te infecteren. Amerikaanse telecombedrijven zoals AT&T en Verizon kregen te maken met Chinese hackers, die zich richtten op afluistersystemen voor nationale veiligheid. Deze gebeurtenissen onderstrepen het belang van sterke wachtwoorden, multi-factor authenticatie en geavanceerde beveiligingsmaatregelen voor zowel bedrijven als consumenten.

Lees verder

Reading in □□ or another language

Generatieve AI: De nieuwe uitdaging voor cyberveiligheid

Generatieve AI is een snel evoluerende technologie die niet alleen voordelen biedt, maar ook aanzienlijke risico's voor de cybersecurity met zich meebrengt. Deze vorm van kunstmatige intelligentie kan content zoals teksten, video's en zelfs code genereren, wat haar een krachtig hulpmiddel maakt. Helaas wordt deze technologie ook door kwaadwillenden ingezet om complexere en grootschaligere cyberaanvallen uit te voeren. Dit dwingt bedrijven en overheden om hun beveiligingsstrategieën aan te passen.
Het AI Cybersecurity Kwadrant, ontwikkeld door de AIVD en RDI, helpt om de risico's en mogelijkheden van generatieve AI in kaart te brengen. Het model biedt inzichten in zowel aanvallen die gebruikmaken van AI, als de verdediging ervan. Organisaties worden aangemoedigd om proactief te investeren in kennis en technologie om deze nieuwe dreigingen het hoofd te bieden, aangezien de afhankelijkheid van AI-systemen steeds groter wordt.

Lees verder

Reading in □□ or another language

Broek in Waterland en Graft - Helpdesk fraude

Op 13 juni 2024 werd een 81-jarige vrouw uit Broek in Waterland het slachtoffer van bankhelpdeskfraude. Ze werd gebeld door iemand die zich voordeed als bankmedewerker, waarna haar bankpas werd opgehaald en er met haar pas 500 euro werd opgenomen. Een vergelijkbare oplichting vond op 3 augustus plaats in Graft, waar een 86-jarige vrouw slachtoffer werd. De politie vermoedt dat dezelfde dader betrokken is bij beide incidenten. Deze fraude richt zich vooral op kwetsbare ouderen en benadrukt het belang van waakzaamheid. De politie roept op om de verdachte, die op camerabeelden is vastgelegd, te herkennen en tips door te geven. Bankhelpdeskfraude is een vorm van oplichting waarbij criminelen zich voordoen als bankmedewerkers om toegang te krijgen tot financiële middelen.

Lees verder

Reading in □□ or another language

Verbeter je cyberveiligheid: Test je kennis met onze interactieve quizzen

Verken de wereld van cybersecurity en het darkweb met onze interactieve quizzen op CyberCrimeInfo. Of je nu een beginner bent of een doorgewinterde expert, onze quizzen bieden een leuke en uitdagende manier om je kennis uit te breiden.

Wat kun je verwachten?

- **Leer in je eigen tempo:** Ontdek en test je vaardigheden wanneer het jou het beste uitkomt.
- **Ontvang feedback:** Krijg gedetailleerde feedback na elke quiz, zodat je precies weet waar je staat en waar je nog kunt verbeteren.
- **Verdien speciale erkenning:** Behaal een perfecte score en ontvang speciale erkenning voor je prestaties.

Ben je klaar om je kennis te testen en jezelf te meten met anderen? Begin vandaag nog aan je leerreis en vraag je toegangscode aan!

Naar quizzen

De Perfecte Score Club!

Topscorer	Punten	Wanneer
Joost W.	10	04-08-2024
Jasper	10	23-05-2024
Johan	10	16-03-2024
Philip S.	9	17-03-2024
Maxim	9	16-03-2024
Aart	7	21-06-2024
Thijs	7	09-04-2024
Kenan	7	30-03-2024
	NIEUW TOEGEVOEGD	
Dre J.	3	20-10-2024

Maximaal te behalen **punten: 20**
Aantal deelnemers tot nu toe: 932

Totaal overzicht De Perfecte Score Club!

Reading in □□ or another language

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer,
In een wereld waar digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Wij zijn een onafhankelijke organisatie, gedreven door vrijwilligers, die zich inzet voor het informeren en beschermen van het publiek tegen de gevaren van het digitale tijdperk.
Jouw donatie maakt het verschil. Hier is waarom:

1. **Onafhankelijke en Belangrijke Bron van Informatie:** Cybercrimeinfo is geen onderdeel van de Nederlandse Politie. Wij bieden een onpartijdige en toegankelijke bron van actuele informatie over cyberdreigingen, oplichtingstechnieken en preventiemethoden.
2. **Bijdragen aan Bewustwording en Preventie:** Door te doneren help je ons in de missie om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen bij aan het voorkomen van digitale misdrijven.
3. **Ondersteuning van Onze Operationele Kosten:** Donaties worden direct gebruikt voor het hosten van de website en het vernieuwen van onze technologische middelen. Dit stelt ons in staat om op de voet te volgen hoe cybercriminelen opereren en jullie te informeren over de nieuwste digitale gevaren.

Elke bijdrage, hoe klein ook, is van onschatbare waarde in onze continue strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.
We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Doneren kan via de **doneer pagina** (Kies nu zelf het bedrag dat je wilt doneren!) of via onderstaande QR code.

Met vriendelijke groet,
Het team van Cybercrimeinfo

Doneer | Cybercrimeinfo.nl (ccinfo.nl)

Doneer pagina

Geen budget? Geen probleem!

Help ons de zichtbaarheid van Cybercrimeinfo te vergroten met jouw Google review!

Laat jouw stem horen: Steun ons met een Google review!

Wij streven er voortdurend naar om de zichtbaarheid en bereikbaarheid van Cybercrimeinfo te verbeteren. Een fantastische manier waarop jij ons hierbij kunt helpen, is door een review achter te laten op Google. Jouw feedback is onmisbaar voor ons en helpt anderen om ons makkelijker te vinden.
Het plaatsen van een recensie is simpel en kost slechts een minuutje van je tijd. Klik op de volgende link om jouw ervaringen te delen: **Schrijf een review**.
Elke review draagt bij aan onze missie om iedereen beter te informeren over cyberveiligheid. Jouw steun is voor ons ontzettend waardevol!
Hartelijk dank voor je betrokkenheid.

Non-profit team Cybercrimeinfo

Share Tweet Share Pinterest