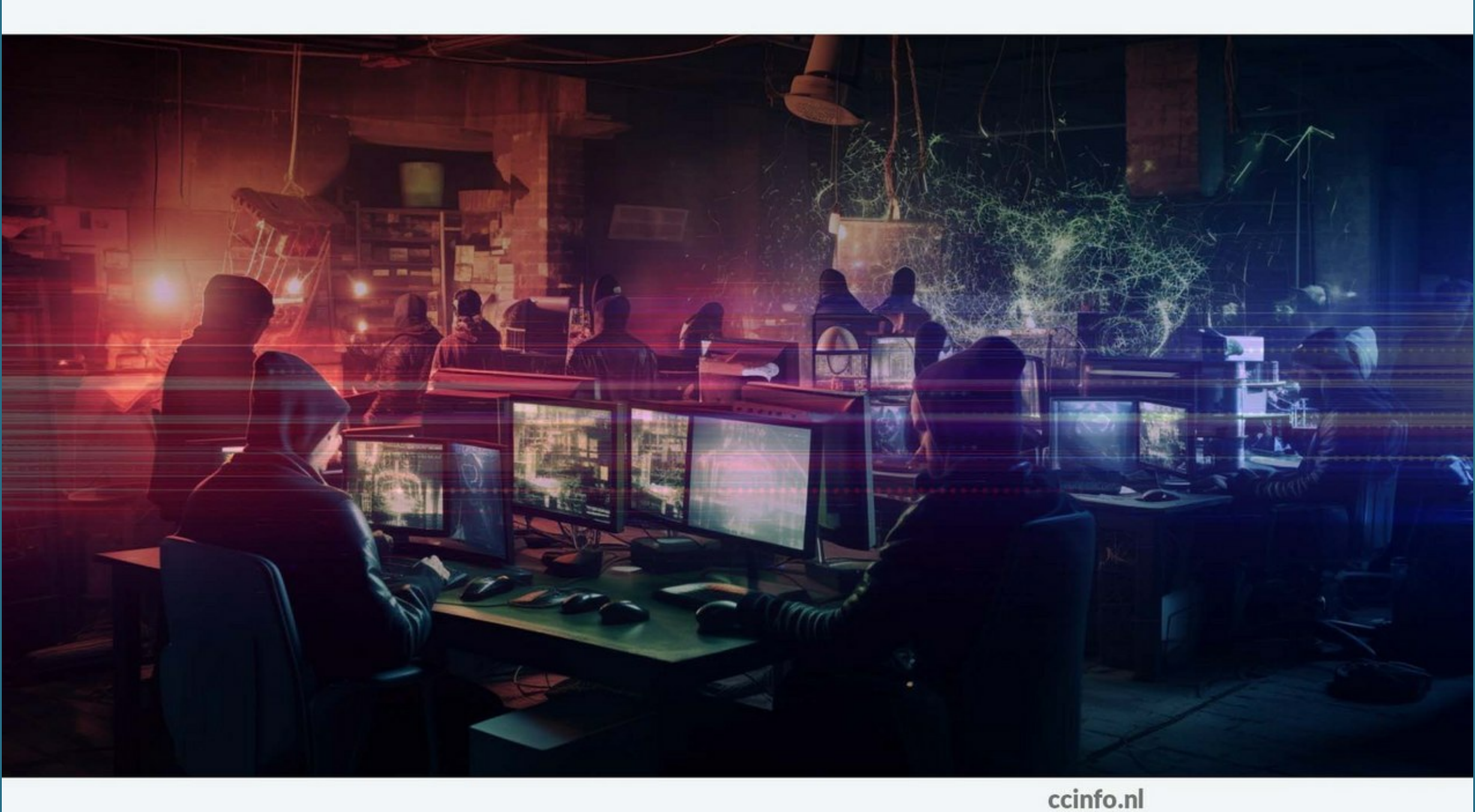
Nieuwsbrief 276 - Week 34-2023


ccinfo.nl

Ransomware: Begrijpen, voorkomen, herstellen

In de complexe en snel veranderende wereld van cybercriminaliteit is ransomware een van de meest verwoestende en groeiende dreigingen. Dit type aanval heeft zich geëvolueerd van rudimentaire experimenten tot geavanceerde, meerlagige operaties. De opkomst van cryptocurrency en Ransomware as a Service (RaaS) heeft de toegankelijkheid en anonimiteit van deze aanvallen vergroot. Voor effectieve verdediging is een uitgebreide aanpak nodig, variërend van proactieve maatregelen zoals back-upstrategieën en incidentresponsplannen tot technieken voor vroege detectie zoals honeypots. Het is cruciaal om te investeren in zowel technologische als menselijke factoren, zoals regelmatige training en bewustwording, om de risico's te minimaliseren.

Lees verder


ccinfo.nl

Noord-Koreaanse crypto-overvallen: Een analyse van $ 2 miljard aan diefstallen sinds 2018

In de afgelopen vijf jaar hebben Noord-Koreaanse hackers een verontrustende reputatie opgebouwd in de wereld van digitale valuta. Met een geschatte buit van $2 miljard aan cryptocurrencies vormen deze cyberaanvallen een ernstige bedreiging voor de financiële stabiliteit en veiligheid van het crypto-ecosysteem. De aanvallen zijn niet alleen opportunistisch maar ook technisch geavanceerd, waarbij gebruik wordt gemaakt van phishing, supply chain-aanvallen en het compromitteren van privésleutels. Deze criminele activiteiten hebben niet alleen een impact op individuele slachtoffers, maar ook op de wereldeconomie, aangezien de gestolen fondsen vaak worden gebruikt voor het financieren van illegale activiteiten zoals terrorisme en wapenhandel. Lees verder op onze website voor een diepgaande analyse.

Lees verder


ccinfo.nl

De opkomst en ondergang van de Cyberbunker

Het verhaal van Cyberbunker illustreert de complexiteit van ethische en juridische vraagstukken in het digitale tijdperk. Ooit een toevluchtsoord voor websites die anonimiteit zochten, werd dit Nederlandse hostingbedrijf uiteindelijk een hub voor illegale activiteiten. Ondanks vijf jaar van intensief onderzoek en een grootschalige inval door de Duitse autoriteiten, roept de zaak nog steeds vragen op over de verantwoordelijkheid van hostingbedrijven. Terwijl de oprichters hun straf uitzitten, blijft de discussie over de grenzen van online vrijheid en verantwoordelijkheid actueel. Het verhaal dient als een waarschuwing voor de risico's van opereren in de grijze gebieden van het internet.

Lees verder

ccinfo.nl

Tip van de week: Cybercriminelen in je computer? Deel 5: Het reinigen en beschermen van Android-apparaten

Het is cruciaal om te begrijpen dat Android-apparaten niet immuun zijn voor cyberaanvallen. Van irritante adware tot gevaarlijke ransomware, de risico's zijn reëel en kunnen ernstige gevolgen hebben. Dit artikel biedt een uitgebreide gids voor het identificeren, isoleren en reinigen van een geïnfecteerd Android-apparaat. Of je nu een technisch onderlegde gebruiker bent of nieuw bent in de wereld van cyberbeveiliging, deze stapsgewijze handleiding is ontworpen om je te helpen je apparaat weer veilig en functioneel te maken. Door waakzaam te zijn en de juiste beveiligingsmaatregelen te nemen, kun je een veilige en beveiligde mobiele ervaring garanderen.

Lees verder

ccinfo.nl

Overzicht cyberaanvallen week 33-2023

In een verontrustende reeks gebeurtenissen hebben cybercriminelen in week 33-2023 Nederland en België getroffen met cyberaanvallen. Deze aanvallen hebben bedrijven, onderwijsinstellingen en zelfs sociale mediaplatforms getroffen, wat gevoelige gegevens in gevaar heeft gebracht en organisaties in crisis heeft gestort. Enkele opvallende incidenten zijn onder andere een cyberaanval op een Nederlands bouwbedrijf, een inbraak bij CVO Antwerpen door de Metaencryptor-malware, hackers die Discord.io aanvielen en gegevens van 760.000 gebruikers stalen, een phishingaanval die 40 miljoen e-mailadressen trof, aanvallers die een backdoor op 1800 Citrix NetScalers installeerden, LinkedIn-accounts die massaal werden gehackt en hackers die een VPN-provider-certificaat gebruikten om malware te ondertekenen. Het volledige overzicht van deze alarmerende cyberaanvallen staat hieronder. Blijf op de hoogte van deze ontwikkelingen die de digitale veiligheid in de regio onder druk zetten.

Bekijk het weekoverzicht

ccinfo.nl

Oost West en Middelbeers - Bankhelpdesk fraude

Op 26 oktober 2022 werd een 72-jarige vrouw het slachtoffer van bankhelpdeskfraude in Oost West en Middelbeers. Een valse bankmedewerker wist haar te overtuigen om haar pincode af te geven. Niet veel later werd haar bankpas opgehaald en werd er een groot bedrag van haar rekening afgeschreven. Deze zaak belicht de aanhoudende dreiging van bankhelpdeskfraude, vaak georganiseerd door criminele netwerken. Het is cruciaal om nooit uw pincode of bankpas aan onbekenden te geven. Heeft u informatie die kan helpen bij de opsporing? Neem dan contact op met de politie via 0800-6070 of meld misdaad anoniem op 0800-7000.

Lees verder

AI chatbot assistent Cybercrime en Cybersecurity

"De AI chatbot assistent: elke dag getraind, elke dag sterker in de strijd tegen criminaliteit."

In het huidige digitale tijdperk, waarin cybercriminaliteit steeds vaker voorkomt, is toegang tot betrouwbare informatie en ondersteuning van cruciaal belang. De Cybercrimeinfo AI chatbot staat te allen tijde voor u klaar om uw vragen over cybercriminaliteit, het darkweb en cybersecurity te beantwoorden. Deze chatbot is direct verbonden met de Cybercrimeinfo-database en haalt geen informatie van het internet. De informatie die de bot verschaft, is uitvoerig gecontroleerd en is volledig betrouwbaar.
Wat deze chatbot onderscheidt, zijn de wekelijkse updates over cyberaanvallen, kwetsbaarheden, opsporingsberichten en betrouwbare artikelen aangaande cybersecurity, cybercriminaliteit en het darkweb. Zo hebt u altijd en overal toegang tot een actuele en betrouwbare cyberassistent die 24/7 beschikbaar is

PS: Wist u dat we ook een 'AI chatbot assistent voor Strafrecht en Strafvordering - Hulpofficier en Opsporingsambtenaar' hebben? Gezien de voortdurende ontwikkelingen in de criminaliteit, is het van essentieel belang om up-to-date te blijven met moderne technologieën die efficiënte, snelle en nauwkeurige oplossingen bieden. De AI Chatbot voor Strafrecht en Strafvordering is ontworpen om uitgebreide informatie te bieden over strafrecht en strafvordering. Of u nu opsporingsambtenaar of hulpofficier bent, deze chatbot staat altijd voor u klaar.

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