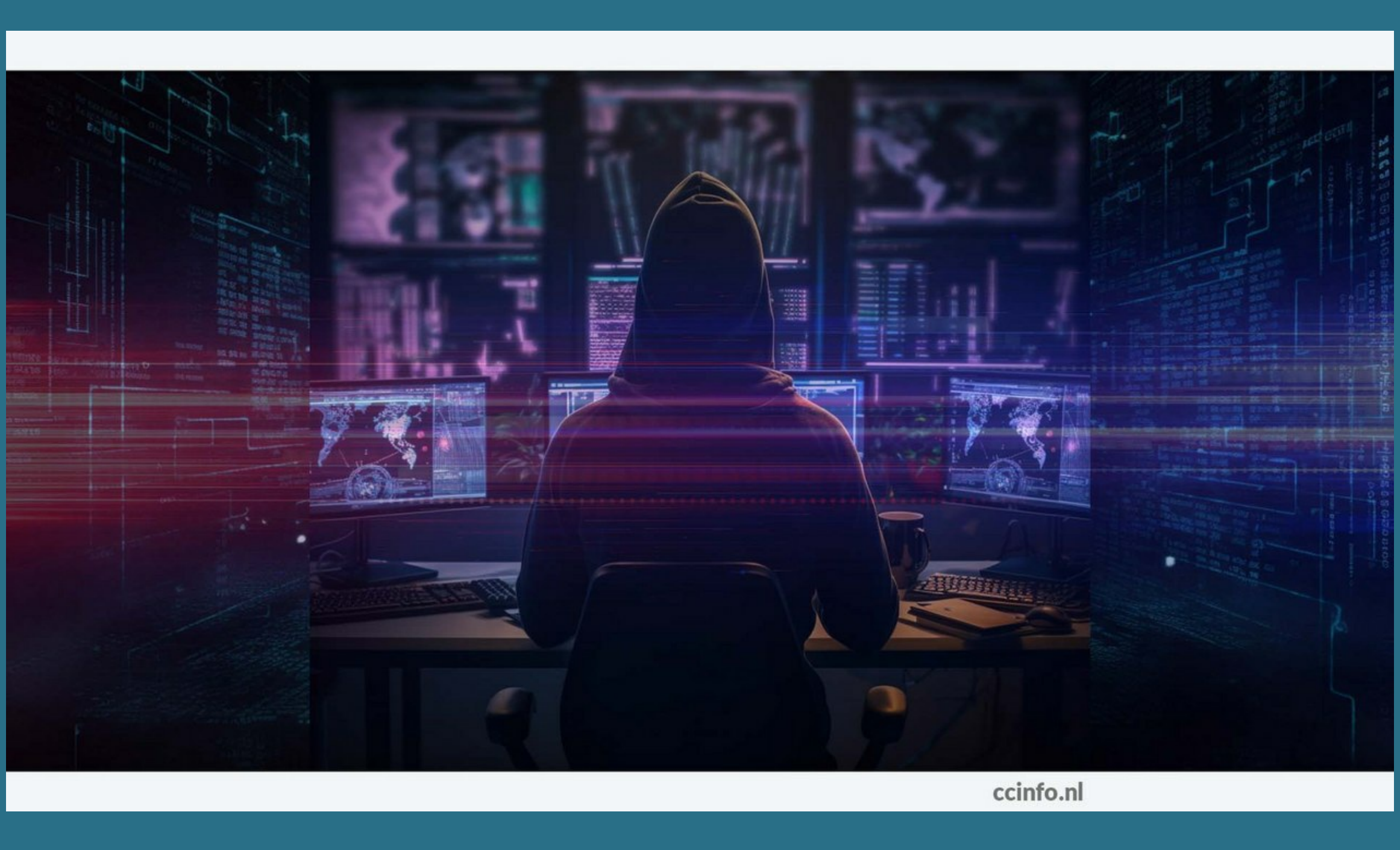
Nieuwsbrief 277 - Week 35-2023

De ontmanteling van het Qakbot-botnet: Een samenwerking van wereldwijde omvang, technologisch vernuft en Nederlandse inzet

Op 29 augustus 2023 behaalde de internationale gemeenschap een significante overwinning in de strijd tegen cybercriminaliteit: de ontmanteling van het beruchte Qakbot-botnet. Deze gecompliceerde operatie, genaamd 'Duck Hunt', was een voorbeeld van uitzonderlijke internationale samenwerking. Landen als de VS, Frankrijk, Duitsland en ook Nederland speelden een cruciale rol in het identificeren en isoleren van geïnfecteerde computers. Het botnet, oorspronkelijk ontworpen om financiële gegevens te stelen, had voor honderden miljoenen dollars aan schade veroorzaakt en meer dan 700.000 computers wereldwijd geïnfecteerd.

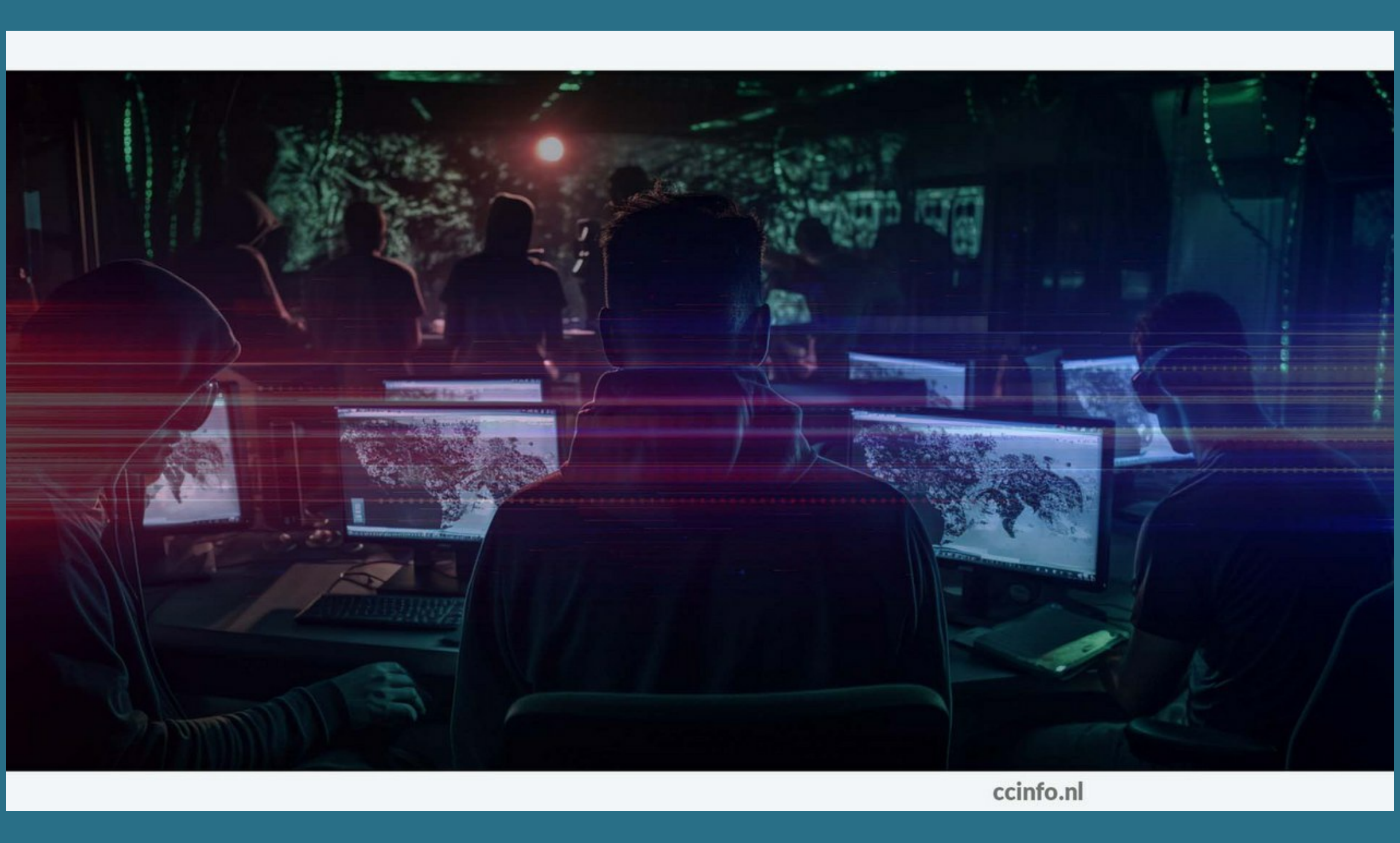
Lees verder



Malvertising: De verborgen bedreiging in het digitale tijdperk

Malvertising is een sluipende vorm van cyberaanval die zich verbergt in de schijnbaar onschuldige wereld van online advertenties. Terwijl u door uw favoriete websites bladert, kunnen malvertisers stiekem kwaadaardige codes invoegen in advertenties die op legitieme sites worden weergegeven. Het verraderlijke aspect is dat u niet eens op de advertentie hoeft te klikken om uw systeem in gevaar te brengen; het simpele feit dat de advertentie laadt, kan al voldoende zijn. Traditionele beveiligingsmethoden zoals antivirussoftware schieten vaak tekort in het identificeren en blokkeren van deze geavanceerde bedreigingen. Nieuwere beveiligingstechnologieën, die gedragsanalyse en heuristische methoden gebruiken, bieden een effectievere verdediging maar vereisen meer technologische expertise. Daarom is het van cruciaal belang om altijd waakzaam te zijn en up-to-date beveiligingsoplossingen te gebruiken.

Lees verder



Het darkweb: De digitale onderbuik van cybercriminaliteit en witwassen

Een van de uitdagingen in de strijd tegen cybercriminaliteit en witwassen op het darkweb is de ingewikkelde economische structuur die criminelen hebben opgebouwd. Deze economie draait niet alleen om directe, illegale transacties, maar ook om het verbergen van winsten via ingewikkelde financiële constructies. Hier spelen cryptocurrency en offshore bankrekeningen vaak een cruciale rol. Deze complexiteit maakt het extra lastig voor autoriteiten om illegale geldstromen te traceren en daadwerkelijk actie te ondernemen. Daarom is een gecoördineerde, internationale aanpak met expertise op meerdere gebieden essentieel om deze problemen effectief aan te pakken.

Lees verder

Tip van de week: Hoe bescherm je jezelf tegen digitale criminaliteit

Het is essentieel om actief maatregelen te nemen voor je digitale veiligheid, gezien de toenemende gevaren van cybercriminaliteit zoals phishing, ransomware en identiteitsdiefstal. Een sterke eerste verdedigingslinie begint bij het gebruik van complexe wachtwoorden, bij voorkeur beheerd door een wachtwoordmanager. Voeg daaraan tweefactorauthenticatie (2FA) toe voor een extra laag beveiliging. Zorg ook voor regelmatige software-updates om kwetsbaarheden te dichten. Wees extra waakzaam bij het klikken op links en het openen van bijlagen in e-mails, vooral als deze van onbekende bronnen komen. Voor een uitgebreide gids over hoe je jezelf kunt beschermen tegen diverse soorten cyberaanvallen, bezoek onze website.

Lees verder

Politie cyber nieuws 2023 augustus

In een tijdperk waarin digitale veiligheid cruciaal is, hebben diverse opsporingsdiensten in augustus 2023 belangrijke vorderingen gemaakt in de strijd tegen cybercriminaliteit. Interpol heeft het bekende 16shop Phishing-platform ontmanteld, wat een significante winst is in het tegengaan van phishing. Bovendien zijn er in Nederland drie arrestaties verricht in een grootschalige zaak van beleggingsfraude, met een geschatte waarde van €56 miljoen. Ook internationaal zijn er stappen gezet; 14 cybercriminelen zijn gearresteerd voor diefstal van zo'n $40 miljoen. Daarnaast hebben de FBI en internationale partners het Qakbot Botnet uitgeschakeld, dat betrokken was bij verschillende vormen van cybercriminaliteit. Deze ontwikkelingen zijn een positieve impuls in de constante strijd tegen cybermisdadigers.

Lees verder

Overzicht cyberaanvallen week 34-2023

In week 34 van 2023 heeft de cyberveiligheidswereld weer flink wat te verduren gehad. De Japanse horlogemaker Seiko werd aangevallen door de BlackCat-ransomwarebende, en Cisco VPN's waren het doelwit van Akira-ransomware. In Denemarken hebben grootschalige ransomware-aanvallen grote schade aangericht bij hostingbedrijven CloudNordic en AzeroCloud. Nieuwe technieken stellen hackers in staat om SYSTEM-privileges in Windows te verkrijgen. Ook was er een gegevenslek bij Discord waarbij gebruikersgegevens werden blootgesteld. Noord-Koreaanse hackers misbruikten een kritieke kwetsbaarheid in ManageEngine om organisaties in verschillende sectoren te compromitteren. Leaseweb werkt aan herstel na een beveiligingsinbreuk, en er wordt onderzoek gedaan naar Russische betrokkenheid bij een aanval op het Poolse spoorwegennet. Lees meer op onze website voor een uitgebreid overzicht en adviezen.

Lees verder

Noorden - Bankhelpdesk fraude

In een recente zaak van bankhelpdeskfraude in Noorden is een 83-jarige inwoner slachtoffer geworden van oplichting. De daders deden zich voor als bankmedewerkers en wisten het vertrouwen van het slachtoffer te winnen. Vervolgens werd een geldbedrag opgenomen bij een lokale bank. De politie heeft goede camerabeelden en roept het publiek op om informatie te delen. Vooral oudere mensen zijn kwetsbaar voor dit soort fraude. Als u meer weet over deze zaak, neem dan contact op met de politie via verschillende kanalen, waaronder de Opsporingstiplijn en Meld Misdaad Anoniem. Uw informatie kan cruciaal zijn om dergelijke criminele activiteiten te stoppen en kwetsbare groepen te beschermen.

Lees verder

Share Tweet Share Pinterest

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