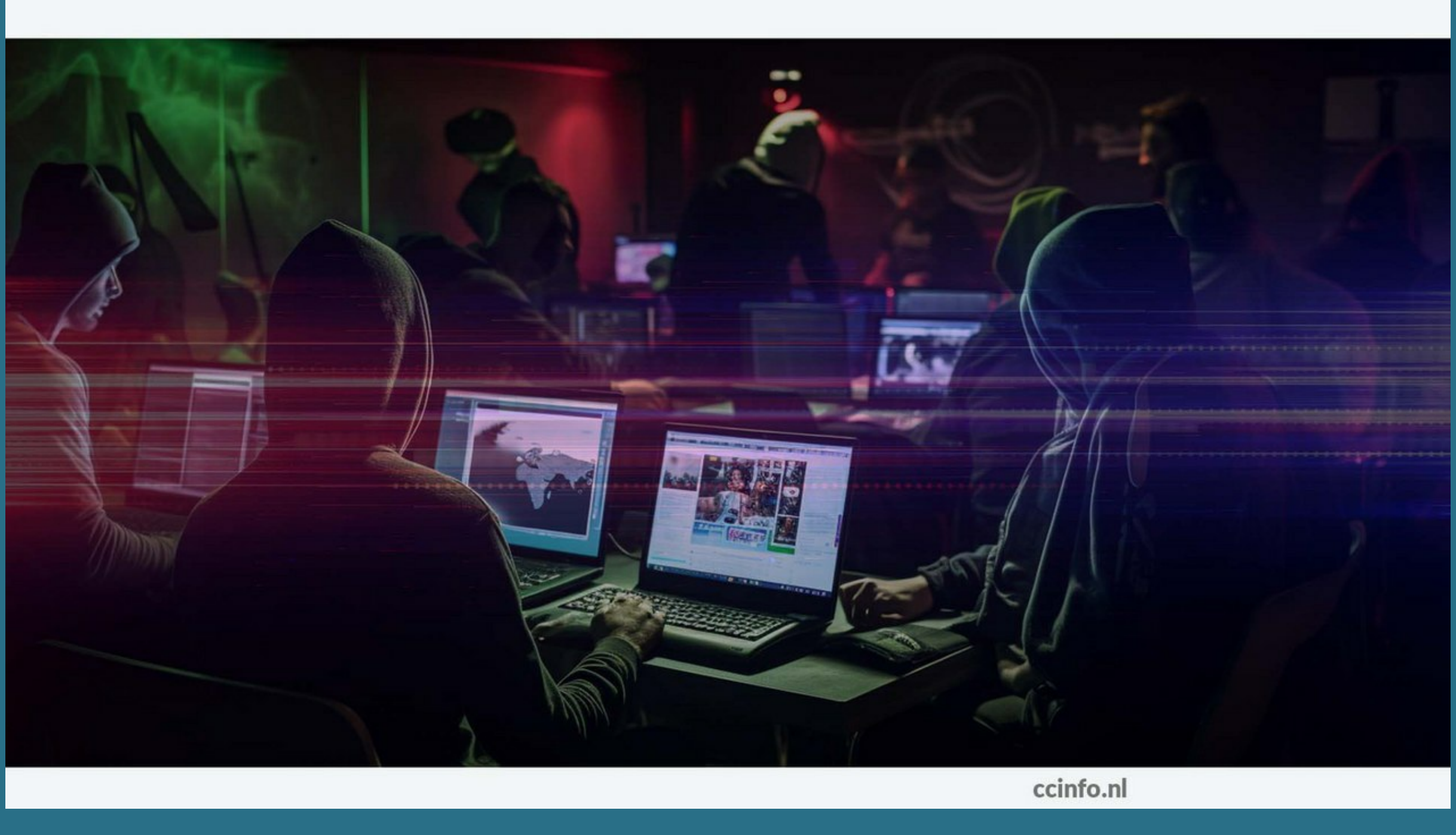
Nieuwsbrief 287 - Week 45-2023


ccinfo.nl

Verhoog uw Cloud veiligheid: Strategieën en Inzichten

In dit artikel, "Verhoog uw Cloud veiligheid: Strategieën en Inzichten", belichten we essentiële bevindingen uit het recente Threat Horizons rapport van Google Cloud. Deze inzichten zijn cruciaal voor organisaties die hun cloudomgevingen willen beschermen tegen de steeds veranderende cyberdreigingen. Het artikel benadrukt de noodzaak van sterke authenticatieprotocollen en multifactorauthenticatie om ongeautoriseerde toegang te voorkomen, met een specifieke focus op de groeiende dreiging van aanvallen op cloud-gehoste SaaS-systemen. Ook wordt het misbruik van kwetsbare software en de toenemende aanpassing van dreigingsactoren in hun aanvalsmethoden besproken. Deze informatie is essentieel voor het versterken van uw verdediging tegen deze risico's. Lees verder voor diepgaande aanbevelingen en praktijken om uw cloudveiligheid te verbeteren.

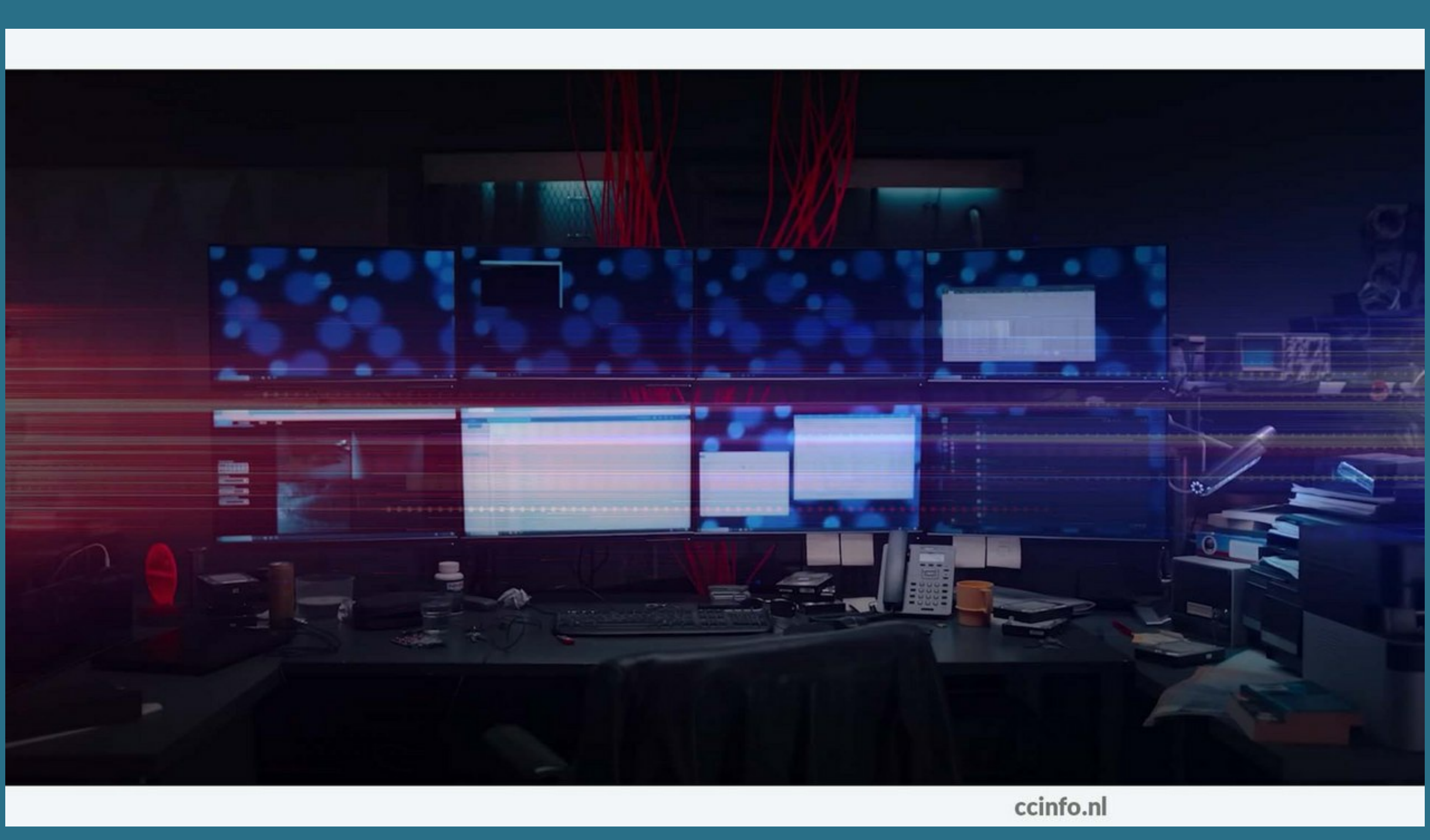
Lees verder


ccinfo.nl

Farnetwork: De sleutelspeler in ransomware-as-a-service markt

In dit artikel op Cybercrimeinfo.nl duiken we in de schaduwrijke wereld van ransomware, met een focus op 'Farnetwork', een sleutelspeler in de ransomware-as-a-service (RaaS) markt. Ontdekt door Group-IB's diepgaande analyse, onthult dit artikel de geavanceerde tactieken en de impact van Farnetwork, die verbonden is aan meerdere ransomware-stammen. Hun innovatieve RaaS-model biedt niet alleen software, maar ook toegang tot reeds gecompromitteerde netwerken. Deze benadering stelt hun klanten in staat om doeltreffende aanvallen uit te voeren zonder zelf op zoek te gaan naar kwetsbare systemen. Farnetwork, actief sinds 2019, heeft onlangs een pauze aangekondigd, maar experts geloven dat dit slechts tijdelijk is. Hun tactieken, waaronder het 'double extortion scheme', benadrukken de noodzaak voor bedrijven en individuen om zich bewust te zijn van de risico's en de juiste beveiligingsmaatregelen te nemen. Lees het volledige artikel voor een dieper inzicht in de duistere wereld van RaaS-programma's en de diverse ransomware-stammen van Farnetwork.

Lees verder


ccinfo.nl

De schaduwwereld van Cyberbunker: Een kijkje in het donkere hart van de cybercriminaliteit

In onze meest recente publicatie op Cybercrimeinfo.nl, "De schaduwwereld van Cyberbunker: Een kijkje in het donkere hart van de cybercriminaliteit", duiken we diep in de verborgen wereld van cybercriminaliteit. Deze intrigerende verkenning onthult de geschiedenis van de beruchte Cyberbunker, een voormalige NAVO-faciliteit omgetoverd tot een duistere hub van het darkweb. Door het verhaal van Herman Xennt, de charismatische leider achter deze operatie, te volgen, krijgen lezers een uniek inzicht in de complexe wereld van digitale misdaad. Dit artikel belicht niet alleen de technische en ethische uitdagingen van cybercriminaliteit, maar ook de internationale inspanningen die nodig zijn om deze bedreigingen aan te pakken. Onze diepgaande analyse en gedetailleerde verslaggeving bieden een essentieel perspectief voor iedereen die geïnteresseerd is in de hedendaagse digitale veiligheid.

Lees verder

ccinfo.nl

Overzicht van slachtoffers cyberaanvallen week 44-2023

Deze week hebben we een zorgwekkende toename gezien van cyberaanvallen wereldwijd, variërend van ransomware-aanvallen op grote multinationals tot gerichte phishingpogingen op kleinere organisaties. Opmerkelijke incidenten omvatten de aanval op de gezondheidszorggigant Henry Schein door de BlackCat ransomware en de cyberinbraak bij Boeing door de LockBit Ransomware Groep. Deze incidenten onderstrepen het voortdurende risico van cybercriminaliteit en de noodzaak voor versterkte cyberbeveiliging in alle sectoren. In Nederland hebben verschillende bedrijven, waaronder TANATEX Chemicals, ook te maken gehad met cyberaanvallen, wat het belang benadrukt van waakzaamheid en preventieve maatregelen. Lees meer over deze ontwikkelingen en krijg gedetailleerd advies over hoe u uw organisatie kunt beschermen door op de link te klikken en het volledige artikel op onze website te lezen.

Lees verder

ccinfo.nl

Tip van de Week: Waakzaam online winkelen - voorkom fraude bij webwinkels

In onze editie van "Tip van de Week" op CyberCrimeInfo.nl, belichten we de toenemende risico's van fraude bij online winkelen. Met de digitale evolutie zijn malafide webwinkels een prominente bedreiging geworden, vaak gebruikmakend van buitenlandse banken en betaaldienstverleners om hun frauduleuze activiteiten te verbergen. Deze winkels lijken professioneel en bieden verleidelijke deals, maar leiden vaak tot financiële schade en teleurstelling bij consumenten. In ons artikel bespreken we hoe deze criminelen te werk gaan, de uitdagingen bij het opsporen van deze frauduleuze praktijken, en delen we essentiële tips om jezelf te beschermen tegen dergelijke online oplichting. Lees verder voor diepgaande inzichten en strategieën om veilig online te winkelen.

Lees verder

ccinfo.nl

Woerden - Bankhelpdesk fraude

In dit artikel lichten we een recente zaak van bankhelpdeskfraude in Woerden uit, waarbij een 66-jarige vrouw bijna €5500 verloor door geraffineerde oplichters. De daders, vermomd als bankmedewerkers, wisten de vrouw te overtuigen van een neppe dreiging van diefstal van haar rekening. Na het overhandigen van haar bankpas aan een zogenaamde 'koerier', werden de gelden opgenomen. De politie heeft duidelijke beelden en signalementen van de verdachten vrijgegeven. Wij roepen onze lezers op om eventuele informatie over de daders te delen.

Lees verder

CyberWijzer, uw persoonlijke cybersecurity expert!

"Elke dag getraind, elke dag sterker in de strijd tegen criminaliteit."

Heb je je ooit afgevraagd wat onze CyberWijzer AI Chatbot zo uniek maakt? Het antwoord is simpel: deze bot is niet zomaar een bot. Of je nu een beginner bent op het gebied van cyberveiligheid of al jaren ervaring hebt, CyberWijzer heeft voor iedereen een passend antwoord. Bovendien bieden we nu uitgebreide informatie over virussen en malware, inclusief instructies voor het verwijderen ervan.
Ben je nieuwsgierig geworden? Bekijk dan de voorbeeldvragen 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