



Nieuwsbrief 340



Analysis of cybersecurity vulnerabilities October 2024

Cybercrimeinfo | ccinfo.nl

Reading in [NL](#) or another language

Analyse van kwetsbaarheden op het gebied van cyberbeveiliging oktober 2024

In oktober 2024 werden diverse ernstige cyberkwetsbaarheden ontdekt, die bedrijven, overheden en consumenten in gevaar brachten. Kritieke kwetsbaarheden werden gevonden in netwerkinfrastructuren zoals routers en firewalls, met als gevolg dat kwaadwillenden toegang konden krijgen tot interne netwerken. Cloudbeveiliging was ook een aandachtspunt, met kwetsbaarheden in apparaten van Western Digital en software van Atlassian, wat leidde tot datalekken en cryptojacking. Ook consumenten werden getroffen door kwetsbaarheden in antivirussoftware en smartphones, waarmee hackers systeemrechten konden overnemen of wachtwoorden konden stelen. De maand zag daarnaast een aantal zero-day kwetsbaarheden, die zonder updates onmiddellijk misbruikt konden worden. Het artikel benadrukt het belang van regelmatige updates, goede patchingstrategieën en verhoogd beveiligingsbewustzijn, zodat zowel bedrijven als eindgebruikers zich kunnen wapenen tegen de steeds grotere cyberdreigingen.

[Lees verder](#)



Police cyber news October 2024

Cybercrimeinfo | ccinfo.nl

Reading in [NL](#) or another language

Politie cyber nieuws 2024 oktober

In oktober 2024 werden verschillende belangrijke cybercriminaliteitszaken opgelost door internationale samenwerking. In Nederland werd een deurwaarder veroordeeld voor het verkopen van persoonsgegevens, terwijl een politieagent in Den Haag werd aangeklaagd voor het onbevoegd opvragen van vertrouwelijke informatie. Wereldwijd werden er doorbraken geboekt in de strijd tegen ransomware. Vier leden van de LockBit-groep werden gearresteerd, en ook de Russische criminele organisatie REvil kreeg zware klappen door arrestaties en veroordelingen. Phishing bleef een zorg, met duizenden verstoorde campagnes en een grootschalige actie tegen bankhelpdeskfraude in Nederland. Daarnaast werden in West-Afrika, Ivoorkust en Nigeria cybercriminelen opgepakt voor phishing- en romance-fraude. De gezamenlijke inspanningen van overheden en technologiebedrijven bleken cruciaal in het ontmantelen van criminele netwerken en het bevorderen van de digitale veiligheid.

[Lees verder](#)



Politicians targeted: Data of 41 Dutch MPs leaked on darkweb

Cybercrimeinfo | ccinfo.nl

Reading in [NL](#) or another language

Politici doelwit: Data van 41 Nederlandse parlementariërs op darkweb gelekt

Gegevens van 41 Nederlandse parlementariërs zijn op het darkweb gelekt, inclusief persoonlijke informatie zoals e-mailadressen, wachtwoorden, geboortedata en socialmediaprofielen. Dit verhoogt de risico's voor nationale veiligheid, aangezien criminelen deze data kunnen gebruiken voor phishing, identiteitsfraude en social engineering. Het lek heeft grotere gevolgen dan alleen de betrokken politici, omdat het de integriteit van het parlement en de nationale infrastructuur in gevaar brengt. Onderzoek toont aan dat 18% van de Nederlandse Kamerleden getroffen is, met opvallend veel gevallen van wachtwoorden in platte tekst die direct bruikbaar zijn voor aanvallen. Het probleem is niet alleen lokaal, want ook andere Europese landen kampen met vergelijkbare lekken. Politici moeten dringend stappen ondernemen om hun digitale veiligheid te verbeteren, zoals het gebruik van tweefactorauthenticatie en het vermijden van werkmaatschappijen voor persoonlijke accounts. Dit incident onderstreept de noodzaak van een bredere digitale weerbaarheid.

[Lees verder](#)



Victim analysis and trends from Week 45-2024

Cybercrimeinfo | ccinfo.nl

Reading in [NL](#) or another language

Slachtofferanalyse en Trends van Week 45-2024

In week 45 van 2024 werden wereldwijd diverse sectoren getroffen door ernstige cyberaanvallen, met een focus op ransomware, datalekken en nieuwe malware. Bedrijven, zorginstellingen en overheidsorganisaties staan steeds meer bloot aan digitale bedreigingen. In België werd het bedrijf Interlabel.be aangevallen door de Ransomhub-groep, die systemen vergrendelde en gevoelige gegevens in gevaar bracht. Ook in Nederland was er een verstoring bij ASML, een belangrijke speler in de chipindustrie. In de VS werden zorginstellingen zoals Memorial Hospital getroffen, wat leidde tot ernstige verstoringen in de zorg. Cybercriminelen richten zich ook steeds vaker op overheidsbedrijven en kritieke infrastructures, zoals de EU en energiebedrijven. Verder werden nieuwe malwarevarianten ontdekt, waaronder ToxicPanda en Pygmy Goat, die specifiek gericht zijn op Android-apparaten en netwerkkapappaten. De voortdurende handel in gestolen data op het dark web benadrukt de groeiende risico's voor zowel bedrijven als burgers.

[Lees verder](#)



Tip of the week: Cyber threats - Stay ahead in the digital battlefield

Cybercrimeinfo | ccinfo.nl

Reading in [NL](#) or another language

Tip van de week: Cyberdreigingen - Blijf voorop in het digitale strijdveld

Cybercrimeinfo biedt wekelijkse updates over de snel evoluerende wereld van cyberdreigingen. De site volgt cyberaanvallen, waaronder ransomware en hacks, en documenteert de toename van geavanceerde aanvallen, zoals zero-day-exploits. Ook de gevaren van het darkweb komen aan bod, waar gestolen gegevens en ransomware-as-a-service (RaaS) steeds vaker verhandeld worden. Daarnaast wordt er aandacht besteed aan de groei van digitale oorlogvoering, waarbij landen cyberaanvallen inzetten op vitale infrastructuur te verstoren. Cybercrimeinfo biedt niet alleen informatie over de laatste trends, maar ook praktische tips voor het versterken van digitale beveiliging, zoals het gebruik van multi-factor authenticatie (MFA) en zero-trust beveiliging. Door op de hoogte te blijven van deze dreigingen, kunnen zowel bedrijven als individuen hun digitale veiligheid verbeteren en zich beter voorbereiden op potentiële aanvallen.

[Lees verder](#)



De opsporingstiplijn: 0800-6070

Zaaknummer Politie: 2024449157- Malden

Cybercrimeinfo | ccinfo.nl

Reading in [NL](#) or another language

Malden - Helpdesk fraude

Op 14 september 2024 werd een 85-jarige vrouw uit Malden slachtoffer van bankhelpdeskfraude. Een vrouw die zich als bankmedewerkster voordeed, belde het slachtoffer met de mededeling dat er verdachte activiteiten op haar rekening waren geconstateerd. Om een onderzoek in te stellen, moest de vrouw haar pincodes doorgeven en werd haar gevraagd haar bankpassen af te geven. Later bleek dat er 1.500 euro van haar rekening was gepind. De politie heeft camera-beelden van de dader en roept getuigen op zich te melden. Deze vorm van fraude maakt gebruik van misleiding via telefoongesprekken en benadrukt het belang van alertheid bij onverwachte verzoeken om persoonlijke gegevens. Naast bankhelpdeskfraude zijn ook vormen als vishing en smishing manieren waarop cybercriminelen mensen proberen op te lichten.

[Lees verder](#)



Cybercrimeinfo | ccinfo.nl

Reading in [NL](#) or another language

Verbeter je cyberveiligheid: Test je kennis met onze interactieve quizen

Verken de wereld van cybersecurity en het darkweb met onze interactieve quizen op CyberCrimeInfo. Of je nu een beginner bent of een doorgewinterde expert, onze quizen 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 quizen](#)

De Perfecte Score Club!

| Topscoorer | 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

Maximaal te behalen **punten: 20**

Aantal deelnemers tot nu toe: **942**

Totaal overzicht De Perfecte Score Club!

Cybercrimeinfo | ccinfo.nl

Reading in [NL](#) 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 Betrouwbare 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 ervan 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 pagina](#)

Geen budget? Geen probleem! Help ons de zichtbaarheid van Cybercrimeinfo te vergroten met jouw Google review!

Cybercrimeinfo | ccinfo.nl

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

Deze e-mail is verzonden aan [f\(EMAIL\)](#). • Als u geen e-mails meer wilt ontvangen, kunt u zich [hier afmelden](#). • Voor een goede ontvangst voegt u info@cybercrimeinfo.nl toe aan uw adresboek.

Laposta