Cybercrimeinfo.nl (ccinfo.nl)

NB382

Podcast

Podcast

E-mailadres *

Voornaam

Achternaam

Inschrijven

Inschrijven

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag). Schrijf je in en ontvang het automatisch in je mailbox.

Dagelijks cyber journaal van Cybercrimeinfo

Het Dagelijks Cyber Journaal biedt dagelijkse updates over de belangrijkste cyberdreigingen en incidenten in België en Nederland. Dit is bedoeld voor mensen die de ontwikkelingen in cybercrime willen volgen, maar geen tijd hebben om alles bij te houden. Het biedt een efficiënte manier om snel up-to-date te blijven zonder uren te spenderen aan het zoeken naar relevante informatie. De updates zijn beschikbaar in zowel tekst als via een dagelijkse podcast op Spotify en YouTube.

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag). Schrijf je in en ontvang het automatisch in je mailbox.

Inschrijven

Desolator ransomware, Sitecore ketenlek en Brokewell spyware via Facebook advertenties

Het afgelopen weekend bracht nieuwe cyberdreigingen met zich mee, waaronder de opkomst van de Desolator ransomware, die twee organisaties onder druk zet door gelekte data te dreigen publiceren. Daarnaast werd een fraudeorganisatie ontmanteld die sinds 2019 duizenden ouderen in de VS had opgelicht voor miljoenen dollars. Ook werden verschillende kwetsbaarheden ontdekt, zoals in het Sitecore platform en een mogelijke Android zeroday. Verder werd malvertising ingezet om Brokewell spyware via misleidende Facebook-advertenties te verspreiden, wat tienduizenden Android-gebruikers trof.

Lees verder

ABN Amro malware via email, freepbx kwetsbaarheid en nep WK 2026 websites

Er is een kwetsbaarheid ontdekt in FreePBX-telefooncentrales, die aanvallers in staat stelt om op afstand commando's uit te voeren en gegevens te manipuleren. Ondertussen kampt Orange Belgium met de nasleep van een datalek waarbij klantgegevens van 850.000 mensen zijn buitgemaakt, wat het risico op sim-swapping vergroot. Ook duiken er valse e-mails op die afkomstig lijken van ABN Amro, maar malware installeren op de apparaten van slachtoffers. Daarnaast worden er duizenden nepwebsites gelanceerd rondom het WK 2026, met risico op oplichting en malware.

Lees verder

Datalekken D. Visser, ransomware Identic.be en kwetsbaarheden Linux, Dell, IBM

D. Visser & Zonen, een bloemenexporteur uit Nederland, werd getroffen door een datalek waarbij gevoelige informatie, zoals persoonsgegevens en financiële gegevens, op het darkweb werd aangeboden. Ook werd het Belgische bedrijf Identic.be getroffen door een ransomware-aanval, wat leidde tot verstoringen in de bedrijfsvoering. Daarnaast werden kwetsbaarheden ontdekt in systemen van Linux, Dell en IBM, wat bedrijven in gevaar kan brengen als deze niet snel worden gepatcht. Nieuwe malwarevarianten, zoals ClickFix en TinkyWinkey, vormen eveneens een groeiend risico voor gebruikers.

Lees verder

OM hack, Cloudflare aanval en stijging ticketfraude

Het onderzoek naar de hack van het Openbaar Ministerie (OM) in Nederland is gestart, waarbij de inbraak in de Citrix-systemen ernstige vertragingen veroorzaakte in de strafrechtketen. Cloudflare werd getroffen door een supply chain aanval waarbij API-tokens werden gestolen. Ook werd er een toename van ticketfraude gemeld, met een stijging van 25% in 2024. Daarnaast werden er kwetsbaarheden ontdekt in TP Link, WhatsApp en Android, die de veiligheid wereldwijd in gevaar brachten. Cybercriminaliteit neemt toe, met onder andere spearphishingcampagnes en ransomware-aanvallen.

Lees verder

FSB hackers vallen energiebedrijven aan, AI platformen kwetsbaar

FSB-hackers hebben wereldwijd meer dan 500 energiebedrijven in 136 landen aangevallen, gebruikmakend van een kwetsbaarheid in Cisco-apparatuur. De Amerikaanse overheid heeft een beloning van 10 miljoen dollar uitgeloofd voor informatie over deze hackers. Daarnaast werd een ernstige kwetsbaarheid in AI-platformen ontdekt, die aanvallers in staat stelt kwaadaardige AI-modellen te injecteren. Verder werden nieuwe malwaredreigingen, zoals MystRodX en XWorm, geanalyseerd, evenals een kwetsbaarheid in Apache DolphinScheduler. Deze incidenten benadrukken de groeiende risico's voor digitale infrastructuren wereldwijd.

Lees verder

Van der Valk datalek, SAP kwetsbaarheid en malware voor Mac

Er heeft zich een datalek voorgedaan bij Van der Valk Amsterdam Zuidas, waarbij klantgegevens zoals telefoonnummers en adressen werden gelekt, wat leidde tot phishingaanvallen. Verder werd een kwetsbaarheid in SAP misbruikt, waardoor aanvallers volledige controle over systemen kunnen verkrijgen. Daarnaast is er nieuwe malware ontdekt die gericht is op zowel Windows- als macOS-systemen, waarbij de laatste variant via een valse Microsoft Teams-site wordt verspreid. Geopolitieke spanningen nemen toe door digitale aanvallen van Noord-Korea en Rusland op de crypto-industrie en overheidsinstellingen.

Lees verder

Bankhelpdeskfraude in Breda, pinpas opgehaald en twee keer gepind

In Breda werd een slachtoffer slachtoffer van bankhelpdeskfraude. Na een telefoontje van iemand die zich als bankmedewerker voordeed, werd het slachtoffer onder druk gezet en bleef meer dan twee uur aan de lijn. Een koerier haalde de

pinpas op en diezelfde avond werd er twee keer gepind. De politie zoekt nu de verdachte, die op camerabeelden te zien is, en vraagt om tips. Deze zaak toont de werkwijze van criminelen die met druk en misleiding bankpassen stelen om geld op te nemen.

Lees verder

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer,
In een wereld waarin digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Als onafhankelijke organisatie, volledig gedreven door vrijwilligers, zetten wij ons in om het publiek te informeren en beschermen tegen de gevaren van het digitale tijdperk.

Jouw donatie maakt het verschil. Dit is waarom:

- **Een 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.
- **Bewustwording en preventie mogelijk maken**
  Met jouw donatie help je ons om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen direct bij aan het voorkomen van digitale misdrijven.
- **Ondersteuning van operationele kosten**
  Donaties worden direct gebruikt voor het hosten van onze website en het up-to-date houden van technologische middelen. Hierdoor kunnen we cybercriminelen blijven volgen en jullie informeren over de nieuwste digitale dreigingen.

Elke bijdrage, groot of klein, is van onschatbare waarde in onze strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.

Doneer nu via onze doneerpagina (kies zelf het bedrag dat je wilt doneren) of gebruik de onderstaande QR-code.

We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

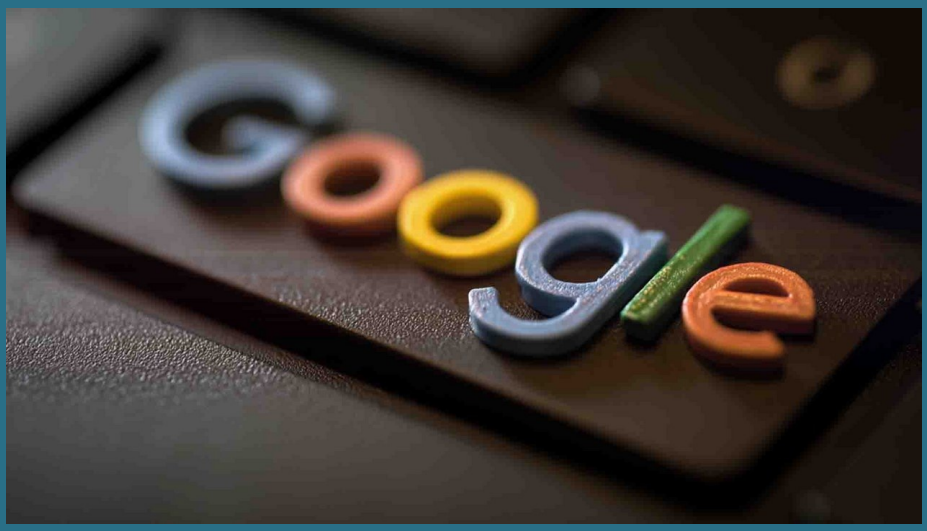
Met vriendelijke groet,
Het team van Cybercrimeinfo

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 (ccinfo)

Schrijf een review

Share Tweet Share Pinterest Bluesky Mastodon