Cybercrimeinfo (ccinfo.nl)

Het onzichtbare zichtbaar maken

NB381

Podcast

Podcast

Reading in another language

Warlock-ransomware, BSN-datalekken en Windows Server-kwetsbaarheid bedreigen bedrijven

Dit journaal schetst recente dreigingen voor België en Nederland: Orange Telecom bevestigt datadiefstal door de Warlock-ransomwaregroep met gelekte klantdata. In Nederland laait de discussie op over het gebruik van BSN's na diefstal bij Clinical Diagnostics. Een kritieke kwetsbaarheid in Windows Server (CVE-2025-55231) vereist snelle patching. Daarnaast duiken geavanceerde Android-spionagemalware en cryptojacking via misgeconfigureerde Redis-servers op. APT-activiteiten (MURKY PANDA) en nieuwe hacktivistische allianties vergroten de noodzaak van verscherpte monitoring en weerbaarheid.

Lees verder

Reading in another language

Colt gehackt, Mechelse IT'er ontmaskerd en nieuwe hacktivistische allianties versterken dreigingen

Het journaal meldt een ransomware-aanval op telecombedrijf Colt, de ontmaskering van een Mechelse IT-er wegens darkweb-misbruik en gecoördineerde arrestaties rond plofkraken. Jongeren worden doelwit via de online groepering "Com". Technisch springen een kritieke Docker-kwetsbaarheid, Linux-aanvallen door APT36 en misbruik van Windows Taakplanner eruit. Lage MFA-adoptie vergroot risico's. Malwarecampagnes via routers, Android-spyware en malvertising nemen toe. Geopolitiek groeien dreigingen door Noord-Korea, Chinese APT's en nieuwe hacktivistische allianties. Ook waren er storingen bij NS en in Leeuwarden.

Lees verder

Reading in another language

Phishingcampagne via Google Classroom en Citrix-lek vormen bedreiging voor Nederland en België

Het journaal meldt een grootschalige phishingcampagne via Google Classroom die Europese onderwijsinstellingen treft, plus een inbraak bij Salesloft waarbij OAuth-tokens van de Drift-Salesforce-koppeling zijn buitgemaakt. In Nederland en België kwamen bankhelpdesk- en nep-loterijfraude aan het licht. CISA waarschuwt voor ernstige Citrix-, Git- en Netscaler-lekken; ook TheTruthSpy en evoluerende Android-droppers vergroten risico's. Spionage door UNC6384 via "STATICPLUGIN" en nieuwe hacktivistische allianties verhogen de geopolitieke dreiging. Snelle patching en alertheid blijven cruciaal voor organisaties in Nederland en België.

Lees verder

Reading in another language

AI trojan Hook en PromptLock ransomware tonen evolutie van cyberdreigingen

Het journaal schetst een breed dreigingsbeeld: juridische stappen rond het datalek bij Clinical Diagnostics, een grootschalige ransomware-uitval bij Zweedse overheden en nieuwe aanhoudingen in de nepagentenzaak. Kritieke kwetsbaarheden in Securden PAM, Citrix en Chrome vereisen directe patching. Opvallend zijn de AI-gedreven dreigingen met de Hook-trojan en PromptLock-ransomware. Inlichtingendiensten waarschuwen voor routeraanvallen op netwerkapparatuur; bovendien circuleren malafide npm-pakketten en phishingmails namens netbeheerders. Geopolitiek blijven APT's actief en verschuift ransomware richting cloudomgevingen.

Lees verder

Reading in another language

Ransomware Cephalus treft CoCo Yachts, Salt Typhoon infiltreert Nederlandse telecom

Het journaal meldt een ransomware-aanval op CoCo Yachts door ‘Cephalus’, waarbij 1,8 TB aan gevoelige data is buitgemaakt. Chinese groep ‘Salt Typhoon’ infiltreerde routers bij kleinere Nederlandse internet- en hostingproviders binnen een wereldwijde campagne, zonder diepere netwerkinbraak. Politie Rotterdam en FBI haalden VerifTools offline, een platform voor valse identiteitsbewijzen. Daarnaast zijn kwetsbaarheden in FreePBX (misbruik van ACP) en Passwordstate gemeld; noodzaak tot snelle updates, afscherming en back-ups wordt benadrukt voor telecom en bedrijfsnetwerken.

Lees verder

Reading in another language

Datalek bevolkingsonderzoek, Sinobi ransomware via MSP's, kwetsbaarheden in wachtwoordmanagers

Het journaal meldde een fors groter datalek bij Clinical Diagnostics met blootgestelde BSN's en medische gegevens. Sinobi-ransomware misbruikte via MSP's gestolen SonicWall-VPN-accounts, terwijl malafide VS Code-extensies en clickjacking in wachtwoordmanagers extra risico's gaven; MindYourPass bleek niet kwetsbaar. Een Facebook-malvertisingcampagne verspreidde Android-trojans. NightSpire viel organisaties aan via ongepatchte VPN/RDP. Geopolitiek: nieuwe VS-sancties tegen Noord-Koreaanse IT-netwerken en APT29-watering-holecampagnes. Amnesty waarschuwde dat Big Tech de privacy structureel onder druk zet. Wachtheid en patchbeleid blijven cruciaal.

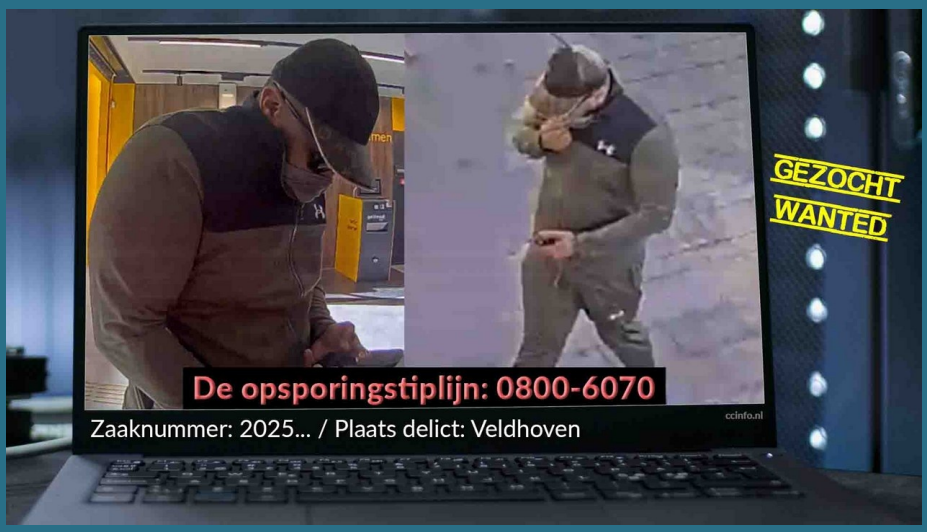
Lees verder

Reading in another language

De dag dat ransomware slim werd, hoe AI de spelregels verandert

Het artikel beschrijft PromptLock, de eerste bekende AI-gedreven ransomware. De malware, geschreven in Go voor Windows en Linux, gebruikt via de Ollama-API een lokaal taalmodel (gpt-oss:20b) om dynamisch Lua-scripts te genereren voor verkenning, exfiltratie en versleuteling (met instructies voor SPECK-128 in ECB). Door zich aan te passen aan het slachtoffer omzeilt zij klassieke detectie. Dit dwingt tot verdediging met gedrags- en anomaliedetectie, gecombineerd met training, strikte rechten, patchbeleid, solide back-ups en incidentrespons.

Lees verder



Reading in another language

Veldhoven en Almere: Helpdesk fraude leidt tot verlies van €4000, politie zoekt verdachte

Een inwoner van Veldhoven werd telefonisch benaderd door een nepmedewerker en raakte door bankhelpdeskfraude €4.000 kwijt, contant opgenomen bij een geldautomaat in Almere. Hij werd via phishingberichten en een ‘wifi-check’ misleid en dacht met de technische dienst van een bank te spreken. De politie zoekt de verdachte, herkenbaar aan zijn postuur en Under Armour trainingspak, en vraagt om tips. Het artikel legt varianten uit (vishing, smishing, tech-support-scams, misbruik van AnyDesk) en vermeldt hoe informatie kan worden doorgegeven.

Lees verder

De Cybercrime Podcast van Cybercrimeinfo

Wil je altijd op de hoogte blijven van het laatste cybernieuws? Abonneer je dan op **De Cybercrime Podcast**. Je ontvangt dagelijks een korte update met betrouwbare informatie over actuele dreigingen, trends en praktische adviezen. De inhoud is zorgvuldig samengesteld door Cybercrimeinfo en eenvoudig te volgen via AI-gegenereerde Nederlandse stemmen. Luister waar en wanneer je wilt via **YouTube** of **Spotify** en versterk je digitale weerbaarheid. Abonneren is gratis en zo geregeld.

AI Chatbots Cybercrimeinfo

AI Chatbots | Ontdek **CyberWijzer**, **RechtRaadgever** en **NIS2Wijzer**, 24/7 beschikbaar voor hulp bij cybercriminaliteit, strafrecht en NIS2-wetgeving. Als je hulp nodig hebt bij het installeren of gebruiken van MindYourPass, gebruik dan AI Gids **VeiligSlot**. De AI **HRMWijzer** bevindt zich momenteel in de testfase van ontwikkeling en biedt richtlijnen en informatie over verschillende aspecten van HRM binnen de politie.

Reading in another language

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.

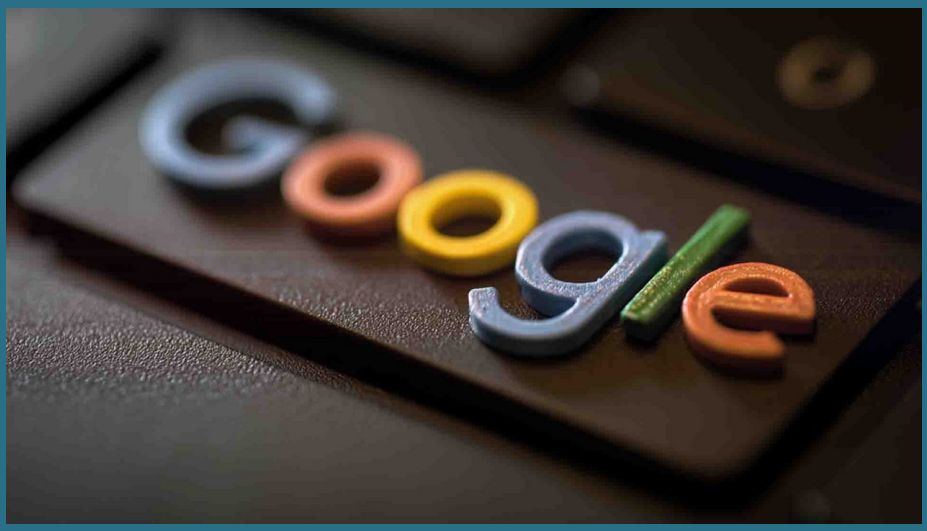
Met vriendelijke groet,
Het team van Cybercrimeinfo

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