Cybercrimeinfo.nl (ccinfo.nl)

"Omdat wat waardevol is, beschermd moet worden"

NB383

Luister naar de discussiepodcast over het nieuws van de afgelopen week. (19 min)

Luister de podcast nu op Youtube

Luister de podcast nu op Spotify

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

AI en softwaremisbruik helpen hackers cryptosleutels te stelen

Hackers maken gebruik van softwaremisbruik en AI-tools om cryptosleutels te stelen. Ze misbruiken bijvoorbeeld het "Nx project" en npm-pakketten om software-updates met schadelijke code te verspreiden, waardoor toegangstokens en geheime sleutels worden gestolen. In enkele gevallen werden Ethereum-wallets aangetast en geld naar criminele accounts overgemaakt. Deze aanvallen tonen de zwakke plekken in de softwareleveringsketen en de geavanceerde technieken die criminelen gebruiken, zoals AI om waardevolle gegevens te extraheren. Beveiliging blijft een prioriteit, vooral voor gebruikers van cryptowallets.

Lees verder

LunaLock ransomware richt zich op artiesten en kwetsbaarheden in populaire software

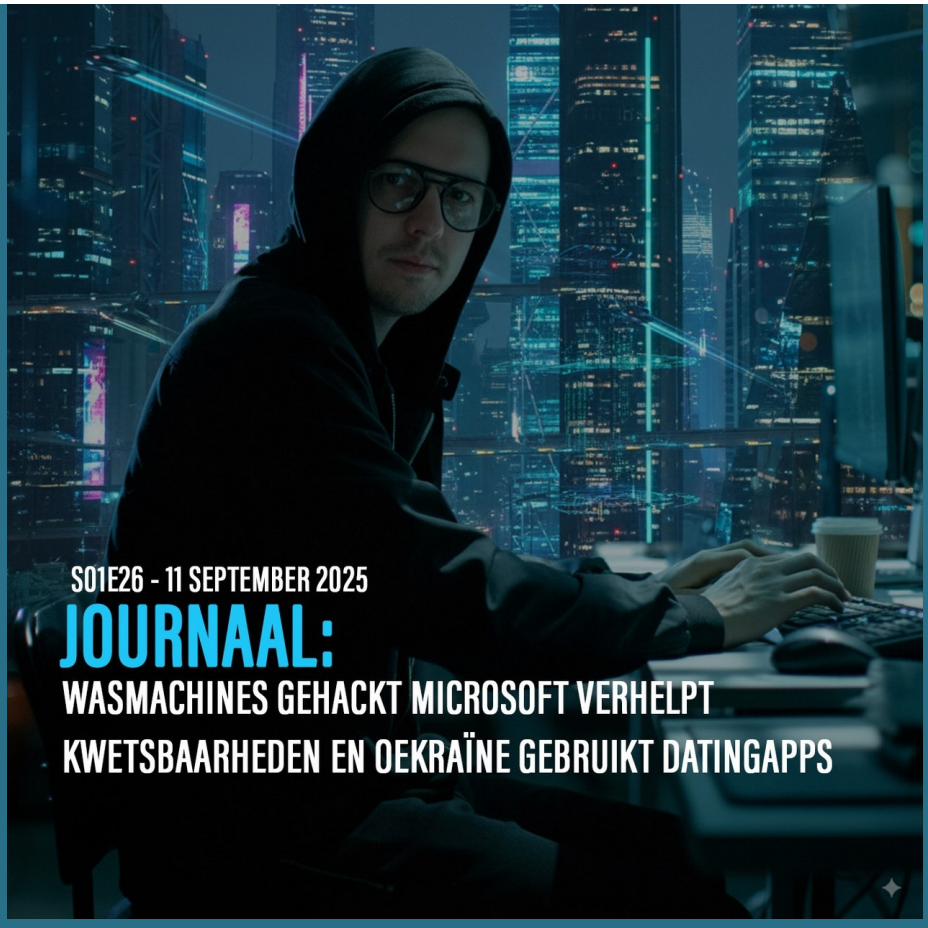
LunaLock ransomware richt zich op digitale artiesten en illustratoren via phishingaanvallen, waarbij slachtoffers misleid worden om besmette bestanden te openen. Na infectie worden belangrijke bestanden versleuteld en eisen de aanvallers losgeld in cryptocurrency. Tegelijkertijd zijn er ernstige kwetsbaarheden ontdekt in populaire software zoals WinRAR en Apache Jackrabbit, die bedrijven in gevaar brengen. Hackers kunnen deze kwetsbaarheden misbruiken om systemen binnen te dringen, waardoor de beveiliging van zowel kunstenaars als bedrijven onder druk komt te staan.

Lees verder

OM herstel, Adobe kwetsbaarheden en de groeiende dreigingen door militarisering van de ruimte

Het Openbaar Ministerie in Nederland heeft zijn systemen hersteld na een cyberaanval in juli, waarbij de communicatie met advocaten tijdelijk werd verstoord. Jaguar Land Rover kampt nog met de nasleep van een aanval die de productie en verkoop stillegde. Daarnaast hebben Adobe en SAP kwetsbaarheden ontdekt in hun software, waardoor hackers toegang kunnen krijgen tot gevoelige informatie. Geopolitieke spanningen rondom de militarisering van de ruimte en de groeiende invloed van landen als de VS, China en Rusland zorgen voor verdere zorgen over de wereldwijde cyberspaceveiligheid.

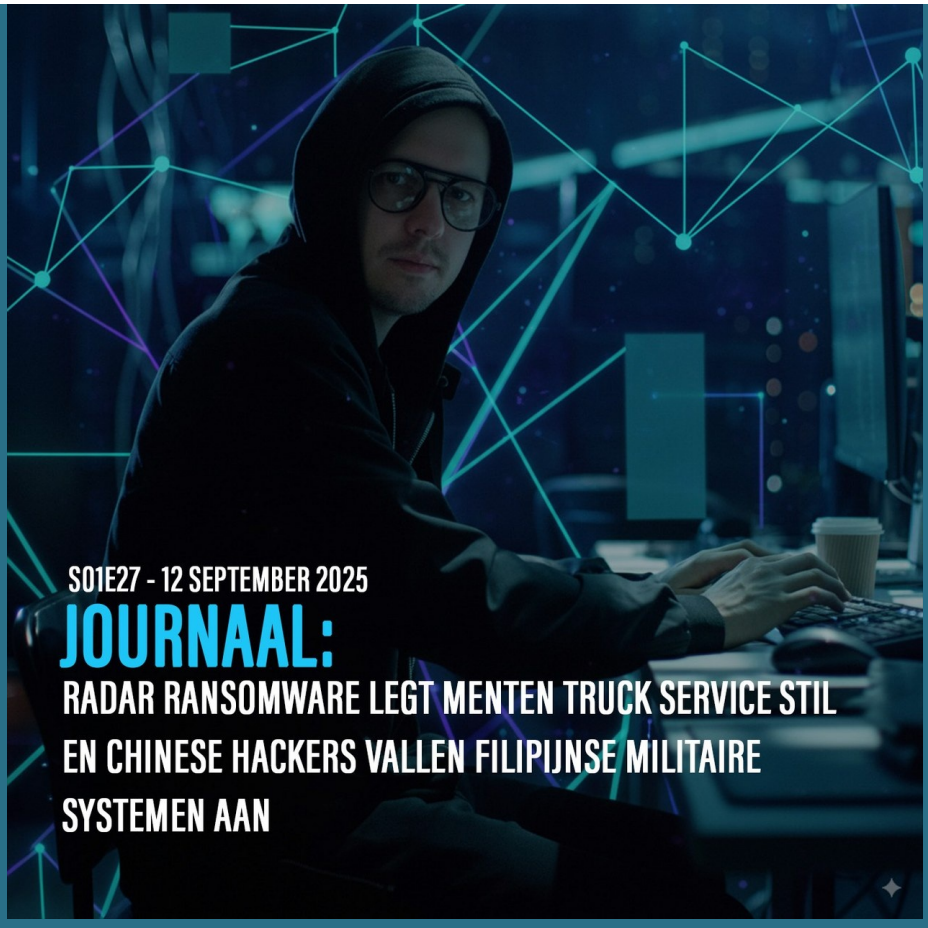
Lees verder



Wasmachines gehackt Microsoft verhelpt kwetsbaarheden en Oekraïne gebruikt datingapps

Een hack op de wasmachines van de Universiteit van Amsterdam liet zien hoe kwetsbaar zelfs eenvoudige apparaten kunnen zijn. Hackers manipuleerden het betaalsysteem zodat studenten gratis gebruik konden maken van de machines. Microsoft loste 81 kwetsbaarheden in populaire software met een belangrijke update, waarvan twee ernstige zero-day zwaktes. In de geopolitieke sfeer gebruikt Oekraïne datingapps voor spionage, waarbij valse profielen Russische soldaten misleiden. Deze incidenten tonen de groeiende dreiging van ransomware, kwetsbaarheden en digitale spionage.

Lees verder



Radar ransomware legt Menten Truck Service stil en Chinese hackers vallen Filipijnse militaire systemen aan

Menten Truck Service werd getroffen door een ransomware-aanval van de Radar-groep, die de bedrijfsvoering ernstig verstoorde. Tegelijkertijd voerden Chinese hackers een digitale aanval uit op de Filipijnse militaire systemen, waarbij ze geavanceerde malware gebruikten voor langdurige spionage. Deze aanvallen benadrukken de kwetsbaarheid van zowel bedrijven als overheden voor cyberdreigingen. Ook werd er een toenemende dreiging van politiek gemotiveerd hacktivisme zichtbaar, met groepen die zich richten op organisaties met politieke doelstellingen. De groeiende rol van cyberspace in geopolitieke conflicten werd verder onderstreept.

Lees verder

Bevolkingsonderzoek datalek, hacktivistische allianties en kwetsbaarheden in Android en videobewaking bedreigen digitale veiligheid

Bevolkingsonderzoek Nederland heeft aangekondigd dat 621.000 mensen slachtoffer zijn van een datalek, waarbij gegevens van medische onderzoeken onbedoeld zijn gelekt. Hacktivistische allianties, zoals de samenwerking tussen OverloadX Team Hacker en TEAM FEARLESS, richten zich op digitale aanvallen om politieke doelen te ondersteunen. Daarnaast zijn er kwetsbaarheden in zowel Android-telefoons van Samsung als videobewakingsoftware van AxxonSoft, die bedrijven in gevaar brengen. Phishingaanvallen en de verspreiding van malware blijven een groeiende bedreiging vormen voor zowel organisaties als gebruikers.

Lees verder

Bankhelpdeskfraude in Montfoort slachtoffer verliest 1250,- euro bij pinautomaat

In Montfoort werd een oudere persoon slachtoffer van bankhelpdeskfraude. De

oplichter, die zich voordeed als bankmedewerker, belde het slachtoffer en beweerde dat diens bankrekening in gevaar was. Na het verkrijgen van de pincode werd een koerier gestuurd om de pinpas op te halen. Later werd er 1250 euro gepind bij een automaat. De vrouwelijke verdachte, die de pinpas gebruikte, wordt omschreven als slank, met licht getinte huidskleur en halflang bruin haar, gekleed in een zwarte blouse en broek. De politie vraagt getuigen zich te melden.

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.

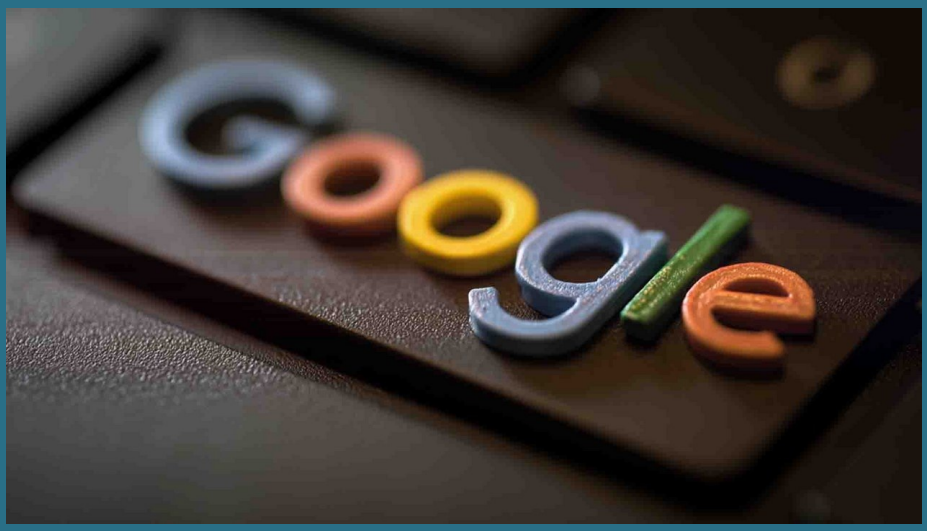
Met vriendelijke groet,
Het team van Cybercrimeinfo

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