200.000 Basic-Fit leden, Booking klanten en de ChipSoft kettingreactie

Bekijk de webversie

## NB414: BASIC-FIT EN BOOKING GELEKT, NIS2 OFFICIEEL VAN START

Deze week raakte de Nederlandse zorg opnieuw, de NIS2 deadline ging officieel in en twee grote datalekken bij Booking en Basic-Fit treffen honderdduizenden consumenten. We vatten de belangrijkste cyberdreigingen samen, met een achtergronddossier over de hackergroep ShinyHunters en een opsporingsoproep uit Erp en Eindhoven.


### BOOKING EN BASIC-FIT GELEKT, KAMERVRAGEN OVER CHIPSOFT

Booking.com bevestigde medio april dat onbevoegden boekingsdetails, namen en adressen hebben ingezien, met gevolgen voor Nederlandse klanten. Vrijwel gelijktijdig meldde Basic-Fit dat gegevens van ongeveer 200.000 Nederlandse leden mogelijk zijn buitgemaakt, waaronder bankgegevens. En in Den Haag stelden D66 en GroenLinks-PvdA Kamervragen over de ChipSoft ransomwareaanval, die 70 procent van de Nederlandse ziekenhuizen raakt via een leverancier.

**Zo ver reikt een hack in de zorg »**


### NIS2 DEADLINE, NGINX UI MISBRUIKT EN AI AGENTS ONDER VUUR

België zet de NIS2 wet vanaf 18 april 2026 in werking voor 2.410 essentiële entiteiten, en Nederland volgt met de Cyberbeveiligingswet voor 8.000 organisaties onder NCSC-toezicht. Tegelijk misbruiken aanvallers een kritieke Nginx UI kwetsbaarheid actief, terwijl Cisco haast heeft met een RCE-patch in Identity Services Engine. Nieuw is dat criminelen AI-coding-agents misbruiken via GitHub pull requests, en een vishing-platform automatiseert telefonische fraude met AI-stemmen.

**De dag dat NIS2 officieel begint »**

### Help Cybercrimeinfo in de lucht te houden

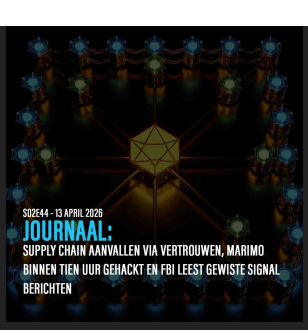
Onze tools, journalen en waarschuwingen zijn gratis voor iedereen. Maar onderzoek en hosting kosten geld. Waardeert u onze intelligence? Help ons dan met een eenmalige donatie. Elke bijdrage maakt de digitale wereld een stukje veiliger.

Ik wil graag steunen »

**Ik wil graag steunen »**

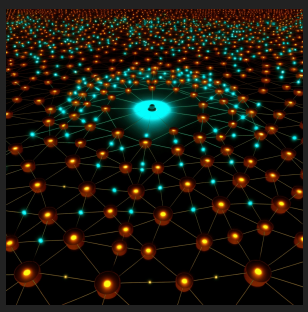
### SUPPLY CHAIN AANVALLEN, MARIMO GEHACKT EN FBI LEEST SIGNAL

De CPU-Z tool van CPUID verspreidde zes uur lang malware, en ShinyHunters stal tokens van Rockstar Games via cloudleverancier Anodot. De kritieke kwetsbaarheid in Marimo werd binnen tien uur na openbaarmaking actief misbruikt voor credential diefstal. En opvallend, de FBI toonde aan dat gewiste Signal berichten te herstellen zijn via de




notificatiedatabase van een iPhone.

**Gewiste berichten, vertrouwde leveranciers, grote gevolgen »**



### SHINYHUNTERS, DE GROEP ACHTER ODIDO, TICKETMASTER EN AMTRAK

Sinds mei 2020 is ShinyHunters een van de meest productieve cybercriminele groepen ter wereld, met Ticketmaster (560 miljoen records), AT&T (110 miljoen) en meer dan 165 Snowflake-omgevingen op hun lijst. In februari 2026 drongen ze bij Odido binnen via phishing en MFA-bypass, en publiceerden gegevens van 6,2 miljoen klanten inclusief circa 5 miljoen BSN-nummers. Recente slachtoffers van deze week zijn McGraw Hill met 13,5 miljoen e-mailadressen en Amtrak met 2,1 miljoen.

**Wie zit er achter die Odido hack »**


### PINNERS GEZOCHT NA BANKHELPDESKFRAUDE IN ERP EN EINDHOVEN

Op 18 december 2025 werd een 74-jarige vrouw uit Erp slachtoffer van bankhelpdeskfraude nadat een bedriegster zich voordeed als bankmedewerker. Dezelfde avond haalde een koerier haar pas, sieraden, telefoon en identiteitskaart op, en de volgende dag werd voor duizenden euro's gepind in Erp en Eindhoven. De politie heeft camerabeelden van twee verdachten, waarvan één vermoedelijk minderjarig, en vraagt mensen die iets herkennen om te bellen.

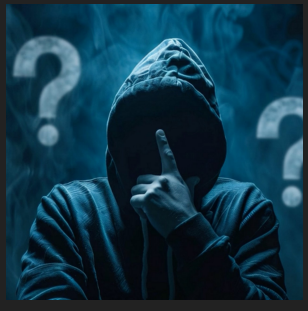
**Herkent u deze pinners »**

## Liever luisteren of kijken?

Geen tijd om te lezen? Blijf op de hoogte via uw favoriete platform. Kies voor de snelle update, de diepgaande analyse of de visuele presentatie.

**Spotify Audio »**
DAGELIJKS JOURNAAL (3 min)
DIEPTE ANALYSE (15 min)

**YouTube Video »**
VISUELE PRESENTATIE (5 min)



### CYBERCRIME QUIZ WEEK 16 - TEST JE KENNIS!

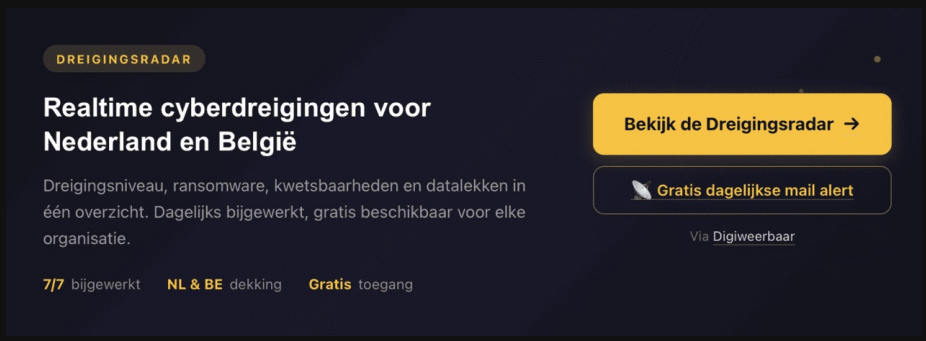
Weet jij hoeveel procent van de Nederlandse ziekenhuizen werd geraakt door de ChipSoft ransomware? Welke beruchte ransomware leider werd ontmaskerd door de Duitse politie? En hoeveel miljard dollar stalen Noord-Koreaanse hackers in 2025? Van zerodays tot Russische spionage. Test in 20 vragen of jij alles hebt meegekregen!

**Test in 20 vragen of jij alles hebt meegekregen?**

## CYBER DREIGINGSRADAR NEDERLAND & BELGIE

De Cyber Dreigingsradar van Digiweerbaar en Cybercrimeinfo is live. Als trouwe lezer van het Cyber Journaal krijg je als eerste toegang tot dit actuele dashboard dat het dreigingslandschap in Nederland en Belgie in kaart brengt.

Bekijk het actuele dreigingsniveau, ransomware activiteit, kwetsbaarheden en sectoranalyse, allemaal op basis van data die 24 uur per dag wordt verzameld uit meer dan 100 bronnen.





Bedankt voor het lezen! Deel deze nieuwsbrief gerust met vrienden, familie en collega's, samen maken we Nederland en België digitaal weerbaarder.

Tot volgende week,
Cybercrimeinfo

Share Tweet Share Pinterest Whatsapp Bluesky Mastodon