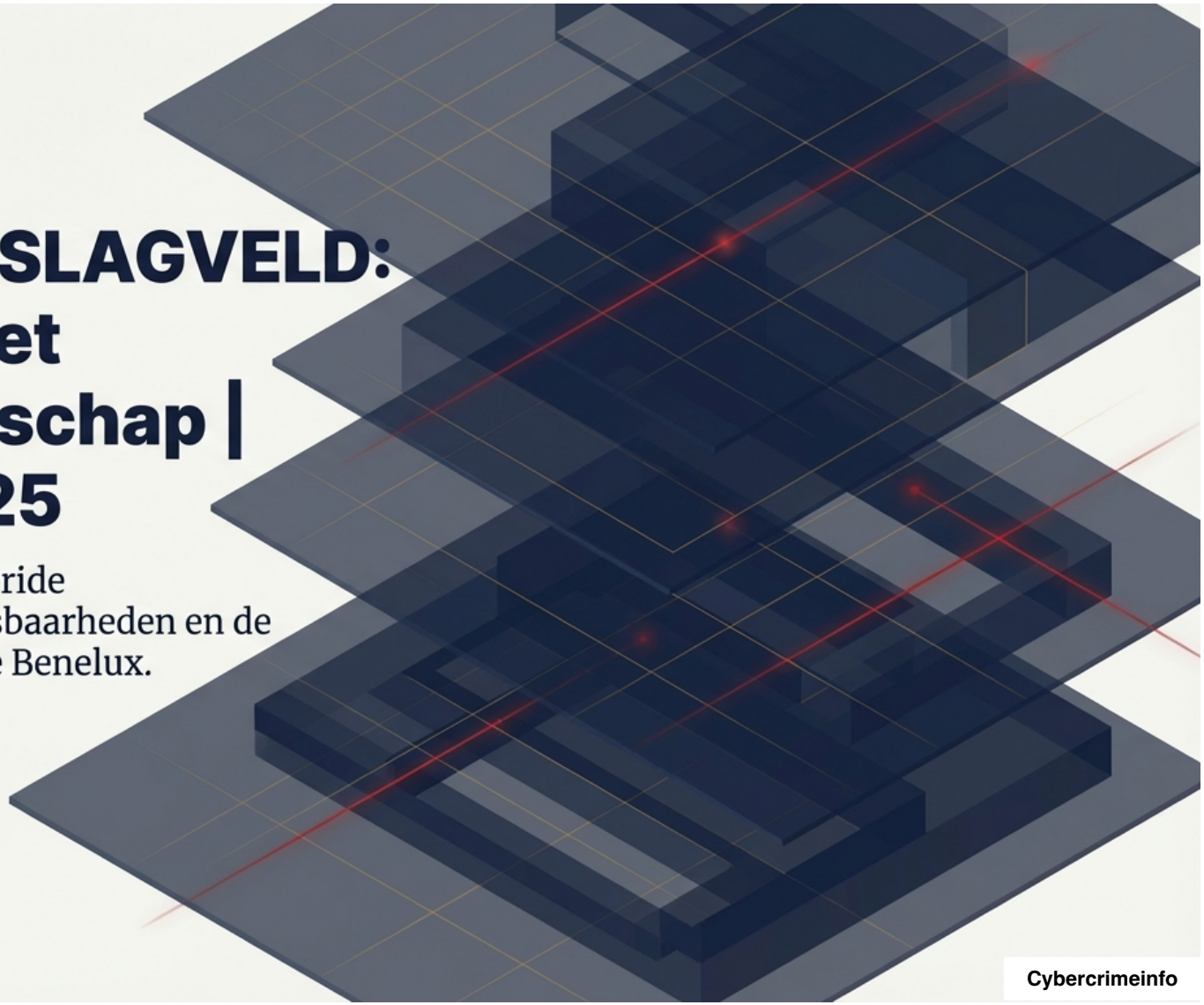
HET DIGITALE SLAGVELD: Analyse van het Dreigingslandschap | December 2025

Een gelaagd overzicht van hybride oorlogsvoering, kritieke kwetsbaarheden en de maatschappelijke impact in de Benelux.

Cybercrimeinfo



De Eerste Week van December: Een Gelaagde Crisis

De digitale veiligheid wordt niet door één type dreiging bepaald, maar door een ecosysteem van samenhangende risico's. Van geopolitieke strategie tot de software op onze servers en de fraude in onze inbox.

1. De Strategische Arena
Geopolitieke spanningen drijven de meest geavanceerde aanvallen.

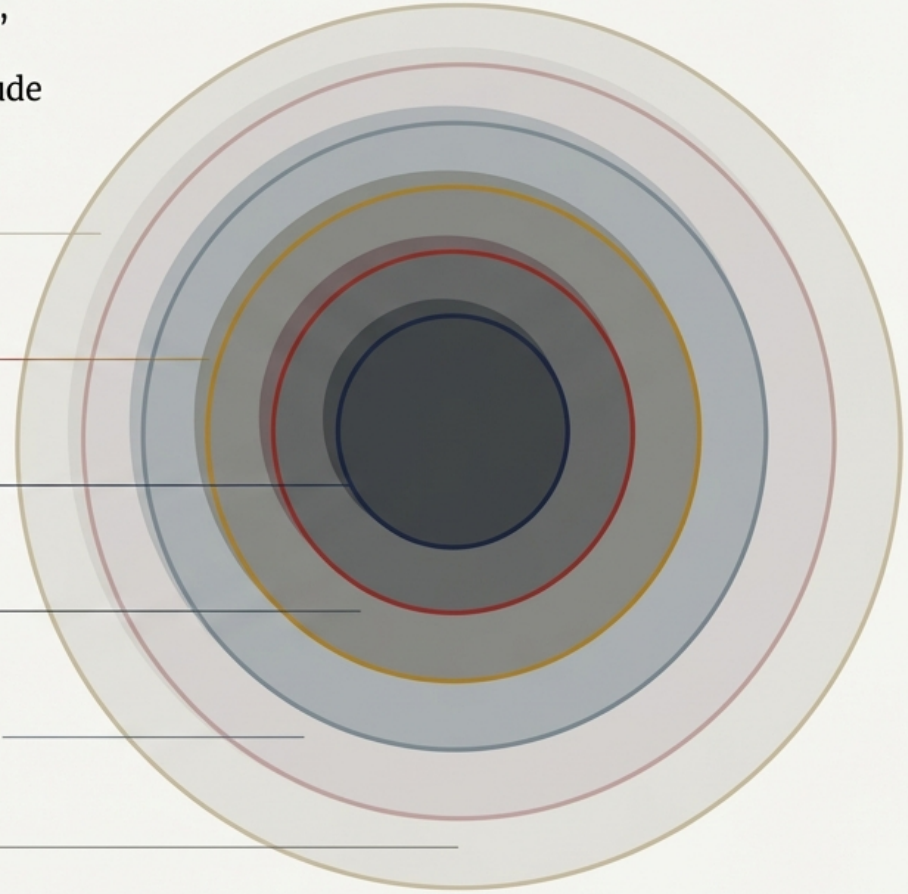
2. Het Commerciële Front
Vitale infrastructuur en bedrijven in de Benelux zijn directe doelwitten.

3. De Technische Fundering
Een golf van kwetsbaarheden vormt de basis voor exploits.

4. Het Aanvallersarsenaal
Nieuwe, gespecialiseerde malware en tactieken worden continu ontwikkeld.

5. De Maatschappelijke Impact
Burgers worden direct geraakt door fraude en privacy-inbreuken.

6. De Tegenreactie
Een overzicht van handhaving en beleidsmaatregelen.



Cybercrimeinfo

LAAG 1: DE STRATEGISCHE ARENA

Geopolitiek als Digitale Brandversneller

NAVO en EU overwegen offensieve cyberoperaties tegen Russische agressie.

De aanhoudende hybride dreiging vanuit Rusland (sabotage, GPS-storingen, desinformatie) dwingt tot een strategische koerswijziging.

Concrete voorstellen van Letland en Italië voor een gezamenlijke Europese cybermacht en een permanent centrum for hybride dreigingen.

VK legt sancties op aan de Russische inlichtingendienst GRU en individuele cyberofficieren na het onderzoek naar de Novichok-zenuwgasaanval in Salisbury.

> **NAVO onderzoekt mogelijkheid van *preventieve aanvallen* op Russische doelen om incidenten voor te zijn.**
>
> — Admiraal Giuseppe Cavo Dragone

Cybercrimeinfo

Wereldmachten Intensiveren Digitale Spionage en Controle

LAAG 2: DE STRATEGISCHE ARENA – GESTAAGDE SPIONAGE

NOORD-KOREA

Voert grootschalige operaties uit met gestolen identiteiten en AI-tools (AIApply, Final Round AI) leectorcs (AIApply, Final Round AI) om westerse bedrijven te infiltreren en fondsen te werven (Chollima/Lazarus-groep).

IRAN

Zet nieuwe backdoor 'MuddyViper' en loader 'Fooder' in tegen Israëlische kritieke kritieke sectoren (lokaal bestuur, telecommunicatie). Zet ook 'UDPGangster' in om detectie te omzeilen.

CHINA

Voert spionagecampagnes uit zoals 'Operation Hanoi Thief' tegen IT-professionals in Vietnam. Levert via frontbedrijven (BIETA, CIII) geavanceerde steganografische tools aan de staatsveiligheidsdienst. Verspreidt ValleyRAT via getrojaniseerde apps.

OEKRAÏNE

Hackers intensiveren aanvallen op de Russische luchtvaart- en defensiesector om productieketens en productieketens en logistieke zwaktes bloot te leggen.

LAAG 2: HET COMMERCIËLE FRONT

Vitale Infrastructuur in de Benelux Geraakt door Gerichte Aanvallen

bpost

Getroffen door Tridentlocker ransomware. 30GB aan data, waaronder persoonlijke en zakelijke informatie van klanten, buitgemaakt en gepubliceerd.

Van Mossel

Serveraanval op de grootste dealerholding. Drie van de 259 servers getroffen; systemen preventief offline gehaald, onzekerheid over datadiefstal.

ODIDO

Grootschalige storing legde spraak- en dataverkeer plat. Oorzaak was een intern netwerkprobleem, maar de impact op de beschikbaarheid was significant.

kpn

Onderzoek naar een mogelijk datalek, met vrees voor compromittering van gevoelige klantinformatie en communicatiegeschiedenis.

Website onbereikbaar gemaakt door een DDoS-aanval opgeëist door de groepering 'BD Anonymous'.

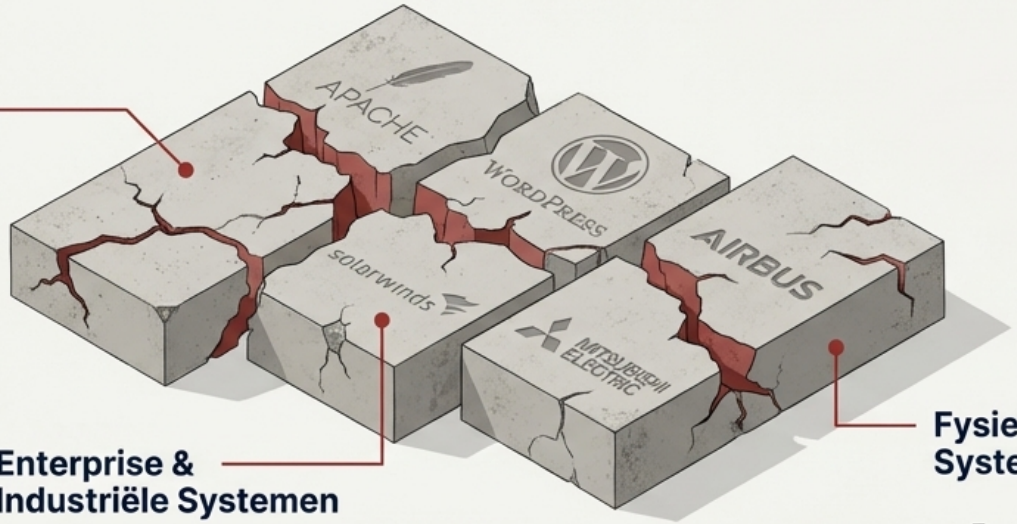
LAAG 3: DE TECHNISCHE FUNDERING

Een Fundament vol Kritieke Lekkages

Actief misbruikte kwetsbaarheden in essentiële software.

Web Ecosystemen

- **Apache Tika** (CVE-2025-66516): XXE-kwetsbaarheid met maximale risicoscore (CVSS 10.0, highlighted in red), systemen over te nemen via gemanipuleerde PDF's.
- **React Server Components** (CVE-2025-55182): Kritieke RCE-kwetsbaarheid (CVSS 10.0, highlighted in red) in veelgebruikte library.
- **WordPress Plugins**: Privilege-escalatie en RCE in 'King Addons for Elementor' (CVE-2025-8489), 'Advanced Custom Fields: Extended' en 'Sneeit Framework' (CVE-2025-6389).



Enterprise & Industriële Systemen

- **SolarWinds Serv-U** (CVE-2024-28995): Actief misbruikt in België.
- **Metabase** (CVE-2023-38646): Exploitatiepogingen waargenomen bij 52 unieke IP's in Nederland.
- **ICS-systemen**: Waarschuwingen voor lekken in systemen van Mitsubishi Electric en OpenPLC (misbruikt door pro-Russische groep TwoNet).

Fysieke en Hardware Systemen

- Fouten in Airbus A320 cockpitsystemen, onveilige dashcams (binnen seconden over te nemen) en slimme toiletcamera's van Kohler Health.

De Software Supply Chain als Zwakste Schakel

- **GitLab**: Meer dan 17.000 geheimen (API-keys, tokens, GCP-credentials) blootgelegd in publieke repositories na een scan van 5,6 miljoen repositories.
- **NPM Register**: De Shai-Hulud 2.0 malware infecteert honderden pakketten, lekt tot 400.000 ontwikkelaarsgeheimen en bevat een destructieve wiper-functie. Stortvloed van "elf-stats" spam-pakketten.
- **Visual Studio Code**: Kwaadaardige extensies (Glassworm, valse 'Material Icon Theme') die ongemerkt malware installeren zoals OctoRAT en Rust-implants.
- **AI-misbruik**: Manipulatie van Anthropic's Claude Skills voor installatie van MedusaLocker-ransomware; npm-pakketten die AI-scanners misleiden met verborgen prompts.

LAAG 4: HET ARSENAAL VAN DE AANVALLER

Spotlight op Nieuwe Malwarefamilies

BrickStorm (China/Warp Panda)

Geavanceerde malware voor diepe infiltratie in VMware vSphere-servers. Creëert verborgen virtuele machines om detectie te vermijden.

Arkanix Stealer

Focust specifiek op het stelen van VPN-inloggegevens en wifi-profielen, ideaal voor toegang tot bedrijfsnetwerken van thuiswerkers.

KimJongRAT (Kimsuky)

Verspreidt zich via valse belastingaanslagen (.hta-bestanden) om cryptovaluta en communicatiegegevens (Telegram, Discord) te stelen.

Albiriox (MaaS)

Richt zich op meer dan 400 financiële en crypto-apps op Android via geavanceerde overlay-aanvallen.

ClayRat

Android-malware die SMS-berichten, oproepgeschiedenis steelt en heimelijk foto's maakt van slachtoffers.

CastleRAT

Nieuwe RAT voor Windows die klembordgegevens monitort om crypto-adressen en inloggegevens te s

Geavanceerde Tactieken: Van MFA-Bypass tot Zero-Click Infecties

- **MFA Omzeilen**: De **Evilginx** toolkit wordt ingezet voor 'adversary-in-the-middle' (AiTM) aanvallen om sessiecookies te stelen en Multi-Factor Authenticatie te omzeilen.
- **Verdediging Uitschakelen**: Commerciële **AV/EDR 'killer tools'** worden verkocht op het darkweb. De **TangleCrypt packer** gebruikt de ABYSSWORKER-driver om EDR-processen te beëindigen.
- **Onzichtbare Infecties**: **Predator spyware** gebruikt de 'Aladdin'-vector voor 'zero-click' infecties via advertentienetwerken. De gebruiker hoeft alleen de advertentie te zien.
- **Linux Rootkits**: **BPFDoor** en **Symbiote** gebruiken eBPF-technologie in de Linux-kernel om zich diep in systemen te nestelen en bijna ondetecteerbaar te zijn.
- **AI-gestuurde Aanvallen**: De **'Water Saci'**-campagne gebruikt AI om Python-scripts te optimaliseren en verspreidt banktrojans via WhatsApp Web.

LAAG 5: DE MAATSCHAPPELIJKE IMPACT

Cybercrime Raakt Iedereen: Van Fraude tot Privacyverlies

Massale Consumentenfraude

- Explosieve groei van meer dan 2.000 valse webshops die bekende merken (Apple, Samsung) imiteren rond de feestdagen om betaalgegevens te stelen.

Geraffineerde Oplichting

- Bankhelpdeskfraude: Schrijnend geval in Amerongen waarbij een kwetsbaar slachtoffer werd opgelicht; arrestaties van 'katvangers' in Amsterdam.
- Virtuele Ontvoeringen: FBI waarschuwt voor scams met bewerkte sociale mediafoto's om families af te persen.

Privacyblunders en Zorgen

- Datalek bij gemeente Dantumadiel (e-mailadressen van 100+ inwoners gelekt).
- Zorgen over heimelijke inzage in medische dossiers via het nieuwe landelijke Mitz-systeem.
- Belgische politie waarschuwt voor privacyrisico's van AI-speelgoed dat constant meeluistert.
- Belgische politie waarschuwt voor privacyrisico’s van AI-speelgoed dat constant meeluistert.

Maatschappelijke Polarisatie

- Onderzoek in *Science* toont aan dat het algoritme van platform X polarisatie versnelt, wat de vatbaarheid voor desinformatie vergroot.

DE TEGENREACTIE

Terugslaan: Successen in Internationale Handhaving

Ontmanteling van Criminele Netwerken

- Internationale operatie rolt netwerk op dat **€700 miljoen** witwaste via frauduleuze crypto-investeringsplatforms.

- Dienst **Cryptomixer** offline gehaald door Europol; **€25 miljoen** aan crypto en 12 TB aan data in beslag genomen.

Arrestaties en Veroordelingen

- **Duitsland**: Arrestatie van een man voor grootschalige verkoop van vervalste ID-bewijzen via het darkweb.

- **Nederland**: Celstraf voor 21-jarige beheerder van darkweb-marktplaats **Bohemia**; twee mannen in Baarn aangehouden voor tonnen aan retourfraude.

- **Australië**: 7 jaar celstraf voor man die **'evil twin' wifi-aanvallen** uitvoerde op luchthavens.

Aanpak van Fysieke Criminaliteit

- Zware celstraffen voor een mensensmokkelnetwerk opererend vanuit o.a. België en Frankrijk, gecoördineerd door Eurojust.

Proactieve Verdediging: Aangescherpt Beleid en Technische Versterking

Beleid & Regulering

- **EU:** Legt een **boete van €120 miljoen** op aan **platform X** voor het misleidende 'blauwe vinkje'-systeem en gebrek aan advertentietransparantie onder de Digital Services Act (DSA).
- **Nederland:** Overheid werkt aan een concept voor een eigen **'soevereine cloud'** om afhankelijkheid van niet-Europese techreuzen te verkleinen. Concept verwacht eind 2026.
- **Frankrijk:** Privacytoezichthouder legt American Express een **boete van €1,5 miljoen** op voor illegaal plaatsen van trackingcookies.
- **India:** Verplicht communicatiediensten (WhatsApp) tot SIM-binding en periodiek uitloggen om fraude tegen te gaan.

Technische & Preventieve Maatregelen

- **Let's Encrypt:** Kondigt aan de levensduur van TLS-certificaten te verkorten naar 45 dagen om misbruik van gestolen sleutels tegen te gaan.
- **VK's NCSC:** Lanceert **proef met 'Proactive Notifications'** om organisaties te waarschuwen voor kwetsbaarheden die via internetscans zichtbaar zijn.
- **Autoriteit Persoonsgegevens:** Start controles op de beveiliging van patiëntgegevens bij Nederlandse zorginstellingen.

Conclusie: Een Permanent en Gelaagd Conflict

Het digitale dreigingsbeeld is geen verzameling losse incidenten, maar een dynamisch en onderling verbonden slagveld. De grens tussen statelijke agressie, georganiseerde misdaad en alledaagse risico's vervaagt.

1. **Geopolitiek is de drijvende kracht**
   De meest geavanceerde dreigingen (APTs, sabotage) zijn direct verbonden met internationale conflicten.

2. **De supply chain is de achilleshiel**
   Aanvallen richten zich steeds vaker op de tools en platforms die we vertrouwen: code repositories (GitLab, NPM), software-updates en AI-modellen (Claude).

3. **De mens blijft een cruciaal doelwit**
   Social engineering en fraude worden steeds persoonlijker en geraffineerder, van de directiekamer (Calendly phishing) tot de huiskamer (bankhelpdeskfraude).

4. **Een gelaagde verdediging is onmisbaar**
   Bescherming vereist een aanpak die verder gaat dan technische patches en ook strategisch bewustzijn, beleid en training op alle niveaus omvat.

Waakzaamheid op alle niveaus is geen optie, maar een noodzaak.

Bronvermelding en Methodologie

Deze analyse is gebaseerd op de **openbare** en **interne publicaties** van **Cybercrimeinfo.nl**, specifiek de **Nieuwsbrieven**, **Journalen** en Dreigingsanalyses van 1 tot en met **7 december 2025**.

De **gepresenteerde informatie is een** synthese van gerapporteerde **incidenten**, technische analyses en geopolitieke observaties om een **coherent** en **gelaagd dreiging**beeld te vormen.

Cybercrimeinfo