
Het Cyberdreigingslandschap:
Een 24-uurs Analyse
Een Executive Briefing over de meest significante incidenten, kwetsbaarheden en trends.
05-12-2025
Cybercrimeinfo

De Hoofdlijnen van de Afgelopen 24 Uur

Digitale dreigingen raakten zowel de commerciële als publieke sector diep. Terwijl organisaties reageerden op directe inbraken, werden kritieke fouten in fundamentele software blootgelegd. Tegelijkertijd verfijnden criminelen hun methoden met AI en boekten opsporingsdiensten successen in een steeds meer gepolariseerde geopolitieke arena.

Directe Aanvallen

Verstorende operaties tegen bedrijven in de automotive, financiële en erfgoedsector.

Kritieke Kwetsbaarheden

Fundamentele lekken in webtechnologie (React) en industriële systemen leggen talloze applicaties bloot.

Evoluerende Technieken

Aanvallers misbruiken AI, legitieme IT-tools en omzeilen de nieuwste browser-encryptie.

Geopolitieke Spanningen

Sancties tegen statelijke actoren (GRU) en toenemende digitale censuur markeren een verharding van de online confrontatie.

Bedrijfsleven Onder Vuur: Van Automotive tot Erfgoed

Van Mossel

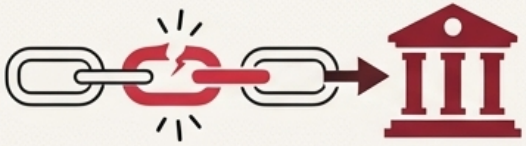
Grootste dealerholding van Nederland getroffen.

- Onbevoegden kregen toegang tot de infrastructuur.
- 3 van de 259 servers werden offline gehaald.
- Onzekerheid over diefstal van klant- of bedrijfsgegevens.

Belgische Staatsarchieven

DDoS-aanval legt toegang tot nationale archieven plat.

- Opgeëist door de groepering ‘BD Anonymous’.
- Blokkade van toegang tot historische en administratieve data.



Marquis Software Solutions

Lek in firewall treft 74 Amerikaanse banken en kredietunies.

- Aanvallers misbruikten een kwetsbaarheid in een SonicWall-firewall.
- Persoonlijke klantgegevens buitgemaakt, wat de kwetsbaarheid van de toeleveringsketen aantoont.

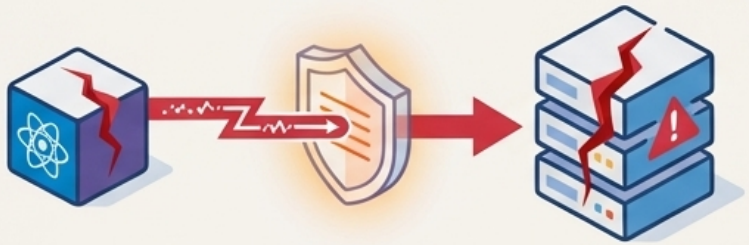
Fundamentele Scheuren in Web- en Industriële Systemen

Kritiek Lek in React Server Components (CVE-2025-55182)

Impact: Een kwetsbaarheid in een fundamentele JavaScript-library maakt Remote Code Execution (RCE) mogelijk op talloze webapplicaties.

CVSS Score: 10.0 (Kritiek)

De kwetsbaarheid, genaamd ‘React2Shell’, is eenvoudig te misbruiken. Patches zijn beschikbaar voor versies 19.x en 15.x/16.x van Next.js. 39% van de gemonitorde cloudomgevingen draaide een kwetsbare versie.



CISA Waarschuwt voor Actief Misbruikte Lekken in Industriële Controlesystemen (ICS)

Impact: Kwetsbaarheden in systemen van o.a. Mitsubishi Electric en Mirion Technologies worden actief uitgebuit. Deze systemen zijn cruciaal voor vitale infrastructuur en productieprocessen.

Dreiging: Risico’s variëren van het omzeilen van authenticatie tot RCE, wat kan leiden tot verstoring van publieke diensten.

Het Ecosysteem onder Druk: WordPress en de Dynamiek van CVE's

WordPress Plugins als Toegangspoort

Populaire plugins blijven een significant aanvalsoppervlak voor miljoenen websites.

Sneeit Framework (CVE-2025-6389)

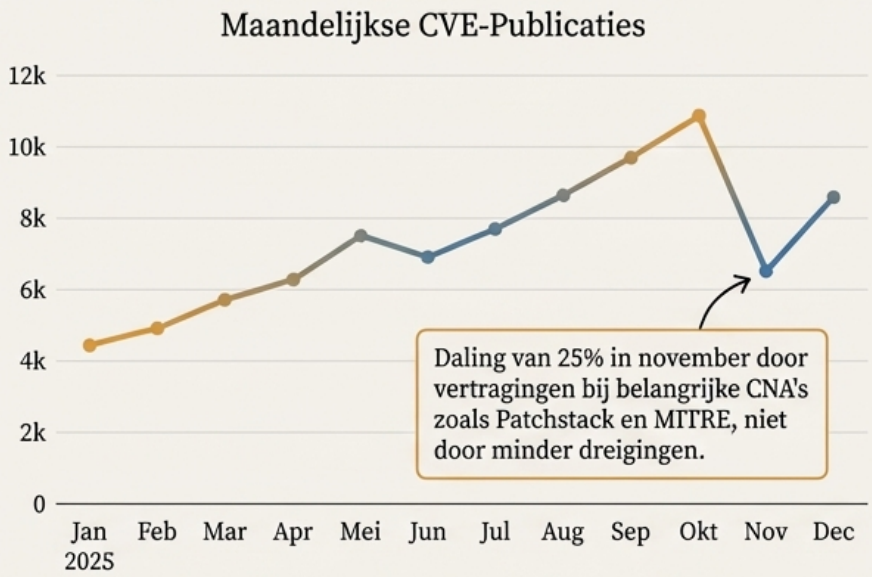
CVSS 9.8, actief misbruikt. Stelt aanvallers in staat willekeurige code uit te voeren.

Meer dan 131.000 exploitpogingen geblokkeerd door Wordfence.

King Addons for Elementor (CVE-2025-8489)

Stelt aanvallers in staat om beheerdersrechten te verkrijgen tijdens het registratieproces.
Meer dan 48.400 misbruikpogingen geregistreerd.

Analyse van CVE-Publicaties



Vertrouw niet enkel op maandelijkse CVE-aantallen voor risico-inschatting; de onderliggende trend blijft stijgend. Jaar-op-jaar stijging van 16,9%.

De Gereedschapskist van de Aanvaller: AI, Malware en Gekidnapte Software

Misbruik van Kunstmatige Intelligentie

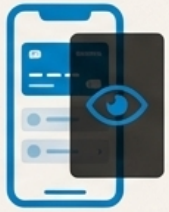
Case: De 'Claude Skills'-functionaliteit van Anthropic kan worden gemanipuleerd om ransomware zoals MedusaLocker te installeren.

Methode: Een ogenschijnlijk onschuldige 'Skill' (zoals een GIF Creator) voert op de achtergrond kwaadaardige code uit na eenmalige toestemming van de gebruiker.

Supply Chain Aanval op Ontwikkelaars

Case: Een vervalste Visual Studio Code (VSCode) extensie, vermomd als de populaire 'Prettier' vermomd als de populaire 'Prettier' formatter.

Payload: De extensie installeert ongemerkt de OctoRAT-malware, die aanvallers volledige controle geeft over de ontwikkelomgeving.



Geavanceerde Mobiele Malware

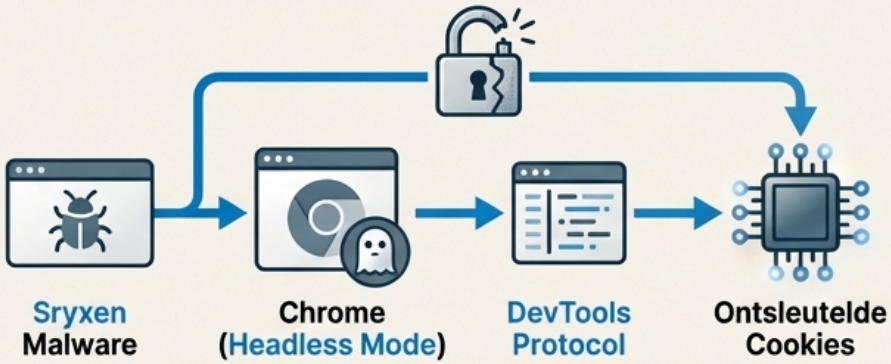
Case: De 'GoldFactory' groep gebruikt
Case: De 'GoldFactory' groep gebruikt uiterst realistische namaakversies van bankapps.

Payload: De malware behoudt de legitieme functionaliteit van de app, maar injecteert kwaadaardige code om beveiligingscodes en bankgegevens te onderscheppen.

Technologische Wedloop: Encryptie Omzeilen en Forensische Tools Misbruiken

Case Study: 'Sryxen' Stealer omzeilt Chrome Encryptie

- **De Uitdaging:** Google's nieuwe 'App-Bound Encryption' in Chrome 127+ moet cookies beschermen.
- **De Oplossing van de Aanvaller:** Sryxen kraakt de encryptie niet, maar omzeilt deze. De malware start Chrome in een onzichtbare 'headless' modus en gebruikt het DevTools Protocol om de reeds ontsleutelde cookies direct uit het geheugen op te vragen.
- **Impact:** Een slimme methode die de nieuwste beveiligingsmaatregelen van een grote browser-leverancier ondermijnt.



Case Study: Legitieme DFIR-tool wordt Aanvalswapen

- **De Tool:** Velociraptor is een gerespecteerde open-source tool voor Digital Forensics and Incident Response (DFIR).
- **Het Misbruik:** Aanvallers installeren Velociraptor op gecompromitteerde systemen (via SharePoint-kwetsbaarheden) om zich te verbergen.
- **De Tactiek:** Beveiligingssystemen negeren de activiteit van de tool omdat deze als legitiem wordt beschouwd. Dit geeft aanvallers een 'stealthy' Command & Control (C2) kanaal en een platform om ransomware zoals Warlock te verspreiden.

De Psychologie van de Aanval: Social Engineering op Industriële Schaal

Tactiek 1: Smishing voor de Feestdagen

Methode: SMS-phishing groepen (vermoedelijk uit China) gebruiken lokkertjes zoals belastingteruggaven, ongebruikte beloningspunten (T-Mobile) en nepwebwinkels.

Doel: Betaalkaartgegevens stelen om deze te koppelen aan Apple/Google Pay op een toestel van de oplichter.

Tactiek 2: DLL Side-Loading via Sollicitaties

Methode: De ValleyRAT-campagne richt zich op werkzoekenden met nep-vacatures in ZIP-bestanden.

Techniek: Een legitiem lijkend uitvoerbaar bestand van de Foxit PDF Reader laadt een kwaadaardige DLL, waardoor de RAT ongemerkt wordt geïnstalleerd.

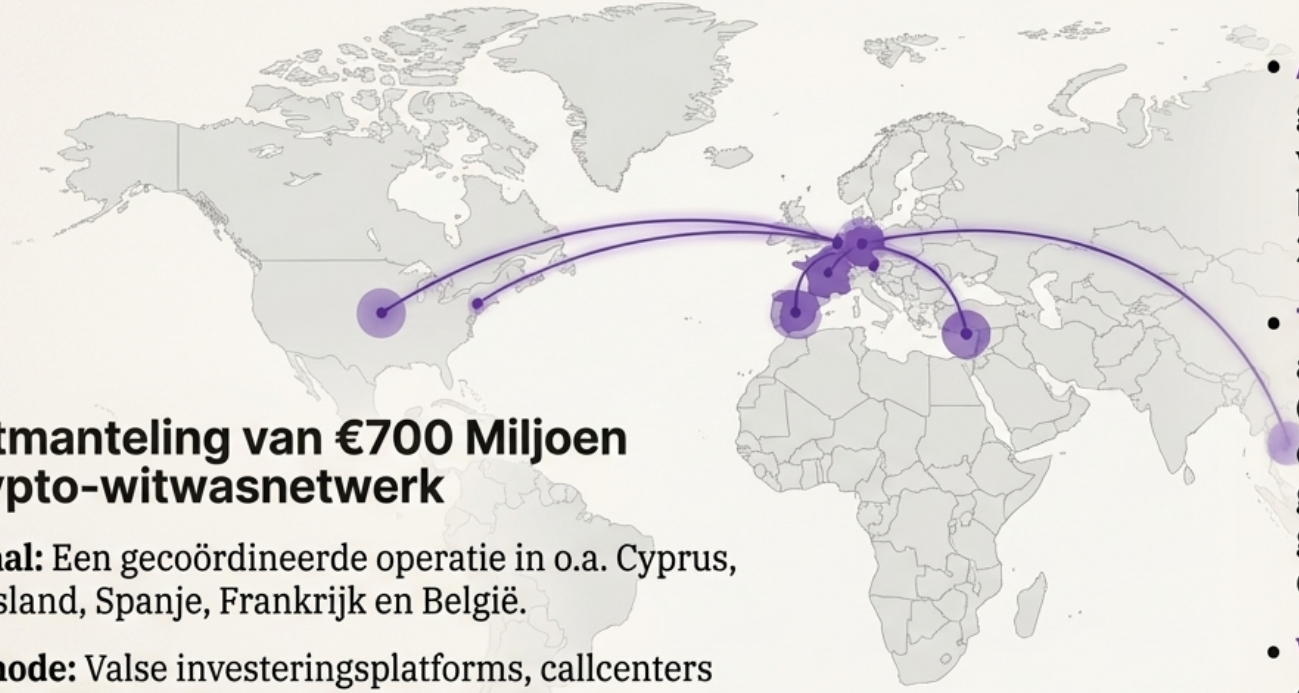
Infrastructuur: De Rol van Cloudflare

68%

van de actieve phishingkits wordt beschermd door de infrastructuur van Cloudflare

Een onderzoek onthult dat 68% van de actieve phishingkits wordt beschermd door de infrastructuur van Cloudflare. De gratis en robuuste DDoS-bescherming van Cloudflare maskeert de werkelijke locatie van de malafide servers en bemoeilijkt detectie.

Internationale Opsporing Slaat Terug: Fraudenetwerken Ontmanteld



Ontmanteling van €700 Miljoen Crypto-witwasnetwerk

Schaal: Een gecoördineerde operatie in o.a. Cyprus, Duitsland, Spanje, Frankrijk en België.

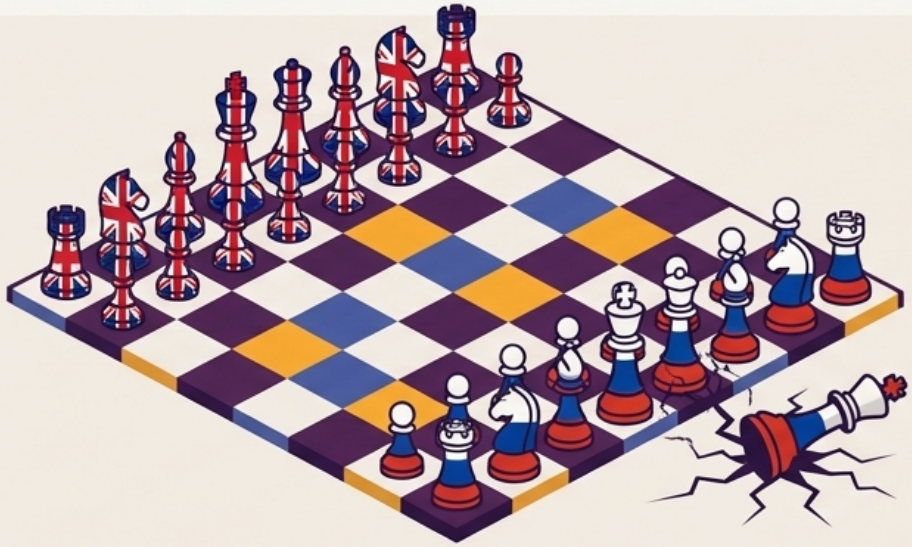
Methode: Valse investeringsplatforms, callcenters en misleidende advertenties met deepfakes.

Resultaat: Negen arrestaties en miljoenen aan activa (banktegoeden, crypto) in beslag genomen.

- **Amsterdam:** Drie 'katvangers' gearresteerd voor het witwassen van geld afkomstig van bankhelpdeskfraude. Minstens 24 fraudegevallen gekoppeld.
- **Thailand:** $300 miljoen aan activa van de 'Prince Holding Group' in beslag genomen, een organisatie gelinkt aan grootschalige elinlt grootschalige oplichting en dwangarbeid.
- **VS:** Twee broers (ex-overheidscontractors) aangeklaagd voor het proberen te wissen van 96 overheidsdatabases.

Cybercrimeinfo

De Digitale Koude Oorlog: Sancties, Censuur en Spionage



Conflict: Verenigd Koninkrijk vs. Rusland

- **Actie:** Het VK legt **sancties** op aan de Russische militaire inlichtingendienst GRU en acht cyberofficieren.
- **Aanleiding:** Vergelding voor de Novichok-zenuwgasaanval en **spionageactiviteiten** (waaronder pogingen om Yulia Skripal met malware te infecteren).
- **Reactie:** Rusland **verscherpt de controle** over het binnenlandse internet, legt beperkingen op aan FaceTime en Snapchat, en blokkeert Roblox wegens 'propaganda'.

Spionage en Infiltratie

Noord-Korea: Een **hackersgroep**, verantwoordelijk voor de miljardenroof bij cryptobeurs Bybit, werd onbedoeld blootgelegd. Een van hun eigen machines raakte geïnfecteerd met de LummaC2-infostealer, waardoor hun operatie zichtbaar werd.

Operation DupeHike: Een campagne die zich richt op administratieve medewerkers bij Russische bedrijven via **spear-phishing** met speciaal geprepareerde documenten.

De Privacyparadox: Overheidssystemen en Slim Speelgoed onder de Loep

Slim Speelgoed en de Privacy van Kinderen

De Belgische politie waarschuwt voor AI-speelgoed. Ingebouwde microfoons en camera's kunnen constant meeluisteren en data verzamelen (namen, adressen, stemherkenning). Het advies is om deze uit te schakelen wanneer niet in gebruik.

De Nederlandse Belastingdienst

Blijft tot 2028 een omstreden systeem ('Klant Toezicht Model') gebruiken dat in strijd is met de AVG. Het systeem toont onterecht gedetailleerde en verouderde persoonsgegevens, zoals seksuele gerichtheid van partners.

Overheid stopt met Google Analytics

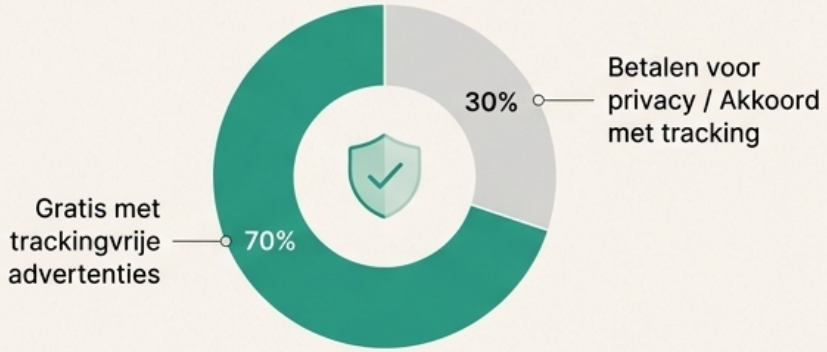
De Nederlandse overheid stopt met het gebruik van Google Analytics op vacaturesites en zoekt een Europees alternatief vanwege zorgen over doorgifte van data naar de VS.

Big Tech en Regulering: De Strijd om Data en Concurrentie

Focus: Meta (WhatsApp, Facebook, Instagram)

- **EU Onderzoek**: De Europese Commissie start een onderzoek naar het nieuwe beleid van WhatsApp dat AI-chatbots van concurrenten vanaf 15 januari 2026 blokkeert.
- **Australische Wetgeving**: Meta schakelt proactief 500.000 Facebook- en Instagram-accounts van gebruikers onder de 16 uit, vooruitlopend op een nieuw Australisch socialmediaverbod.

De Keuze van de Gebruiker: 'Pay or Okay'



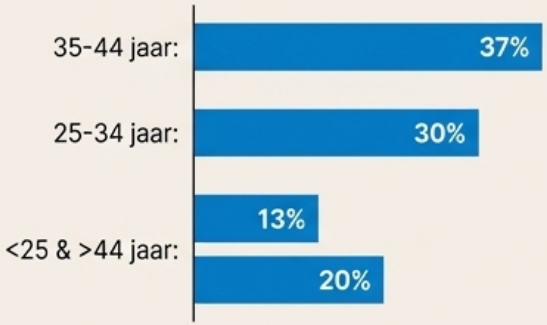
- **Onderzoek Noyb**: Privacyorganisatie toont aan dat 7 op de 10 gebruikers de voorkeur geven aan een gratis dienst met trackingvrije advertenties, boven de keuze tussen betalen voor privacy of gevolgd worden.
- **Conclusie Noyb**: Het 'Pay or Okay'-model dwingt gebruikers een 'privacybelasting' te betalen en ondermijnt de vrije toestemming die de AVG vereist.

De Anatomie van de Cybercrimineel: Een Profielschets

Het stereotype van de jonge hacker is achterhaald. De gemiddelde cybercrimineel is een volwassene van middelbare leeftijd. (Bron: Analyse van 418 zaken door Orange Cyberdefense, 2021-2025)

Demografie

Leeftijdsverdeling



90% mannelijk

Geografie & Carrière

Carrièrepad

Jongere daders beginnen vaak met hacking of DDoS, maar verschuiven naarmate ze ouder worden naar financieel gemotiveerde misdaden zoals afpersing en malwareontwikkeling. De groep 35–44 is het meest strategisch actief.

Cybercrimeinfo

Belangrijkste Inzichten & Trends

1 

Toeleveringsketens zijn het nieuwe front.
Aanvallen richten zich niet langer alleen op het einddoel, maar op de zwakste schakel. Voorbeelden: Marquis Software (via SonicWall) en ontwikkelaars (via VSCode-extensies).

2 

Fundamentele technologie als hefboom voor impact.
Een enkele kwetsbaarheid in een wijdverspreide library (React) of systeem (ICS) kan een cascade-effect hebben en duizenden organisaties tegelijk kwetsbaar maken.

3 

Aanvallers innoveren door legitieme tools te misbruiken.
De grens tussen legitiem en kwaadaardig verkeer vervaagt. Aanvallers gebruiken AI (Claude), forensische software (Velociraptor) en betrouwbare infrastructuur (Cloudflare) om detectie te ontlopen.

4 

De grens tussen cybercrime en geopolitiek vervaagt verder.
Statelijke actoren (GRU) worden direct gesanctioneerd voor cyber-fysieke operaties, terwijl censuur (Rusland) een standaard instrument wordt in de digitale confrontatie.

5 

Privacy en regulering worden centrale thema's.
De strijd gaat niet alleen over beveiliging, maar ook over data, concurrentie en de digitale rechten van burgers, wat leidt tot toenemende overheidsingrijpen (EU, Australië).

Strategische Imperatieven: Wat Vereist Onze Aandacht?

1. Proactieve Verdediging van de ‘Core’

De focus moet liggen op het verharden van fundamentele bouwstenen. Onmiddellijke patching van kritieke bibliotheken (zoals React) en het segmenteren van industriële netwerken is niet optioneel, maar essentieel.

2. De Menselijke Firewall Versterken tegen Slimme Misleiding

Traditionele bewustwording volstaat niet meer. Organisaties moeten anticiperen op zeer geavanceerde social engineering die gebruikmaakt van AI, gekaapte legitieme tools en psychologische druk.

3. Begrijp de Geopolitieke Context van Dreigingen

Analyseer dreigingen niet in een vacuüm. De herkomst van een aanval, de politieke spanningen en de doelen van statelijke actoren bepalen steeds vaker het risicoprofiel.

4. Bereid je voor op een Geregeuleerd Digitaal Domein

Compliance met privacy- en concurrentiewetgeving is nu een kernonderdeel van cyberstrategie. De keuzes van Big Tech en overheden hebben directe gevolgen voor de inzet van technologie.