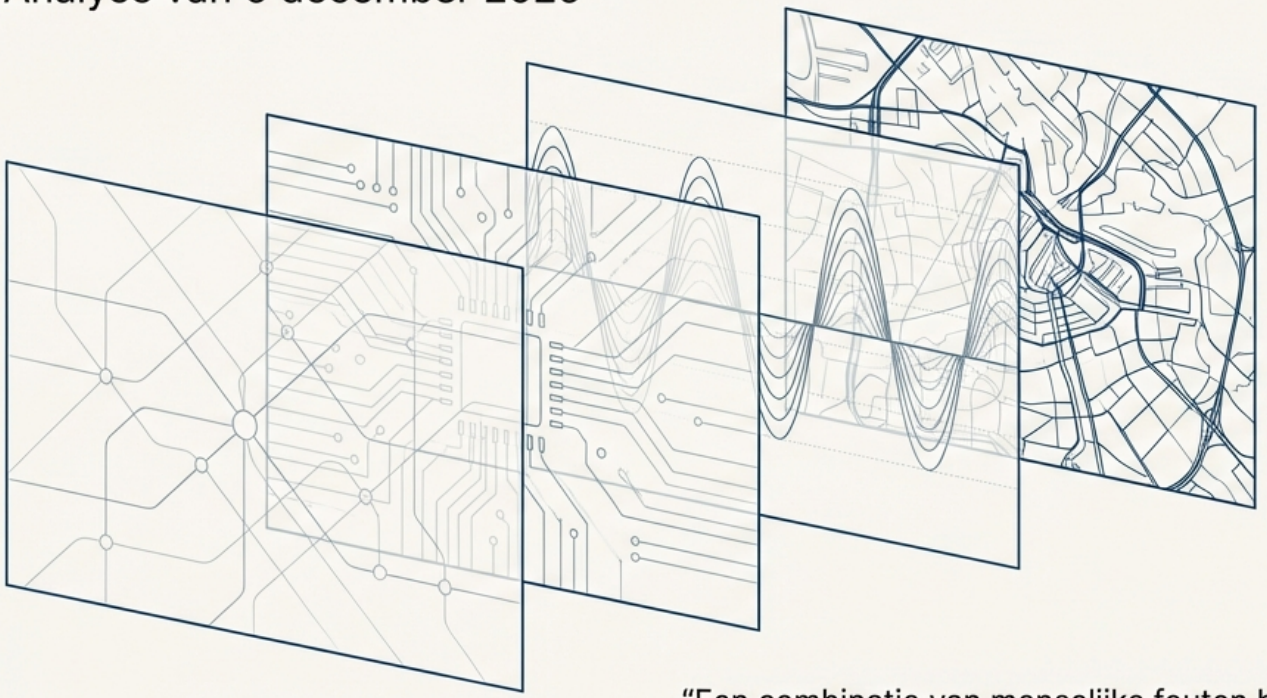
Cyber Dreigingsbeeld

Een Gelaagde Analyse van 6 december 2025



“Een combinatie van menselijke fouten binnen de overheid en zeer geavanceerde aanvalstechnieken van statelijke actoren.”

—Cybercrimeinfo Journaal, 06-12-2025

De Essentie in 60 Seconden: Vier Kerninzichten

De Menselijke Factor Blijft Kritiek

De mens is een primair doelwit. Aanvallen misbruiken vertrouwen en onoplettendheid, van e-mailblunders tot geavanceerde social engineering.

Organisaties Onder Vuur

Aanvallen worden diverser, van destructieve ransomware en datadiefstal tot onzichtbare spionage-malware die diep in netwerken opereert.

De Infrastructuur is Kwetsbaar

Zowel fundamentele softwarefouten met maximale risicoscores als de afhankelijkheid van centrale tech-spelers spelers vormen een systemisch risico.

De Strategische Arena is Actief

De strijd is ook geopolitiek en beleidsmatig. Staten, criminelen en toezichthouders vechten om de digitale controle, wat leidt tot boetes, spionage en complexe wetgeving.

DEEL 1: DE MENSELIJKE LAAG

De Eerste Verdedigingslinie: Individuen als Doelwit

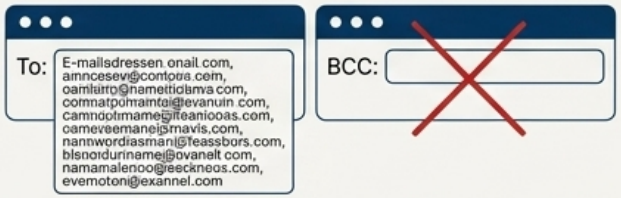
De meest directe aanvallen misbruiken menselijk vertrouwen, onoplettendheid en emotie voor financieel gewin of chantage.

Phishing met Grote Gevolgen (Solana)

Een phishingcampagne manipuleert de *eigendomsrechten* van crypto-wallets in plaats van direct fondsen te stelen. Hierdoor blijft de balans zichtbaar, maar is de toegang verloren.
Impact: Eén **slachtoffer verloor $3 miljoen**.

Emotionele Chantage (FBI-waarschuwing)

Criminelen gebruiken bewerkte social media foto's in **'virtuele ontvoeringen'** om families te overtuigen losgeld te betalen voor een ontvoering die nooit heeft plaatsgevonden.



Simpele Fout, Groot Lek (Gemeente Dantumadiel)

E-mailadressen van meer dan 100 inwoners gelekt door het niet gebruiken van de BCC-functie bij een e-mail over een woningbouwproject. Dit toont aan hoe basale fouten tot datalekken leiden.

DEEL 2: DE ORGANISATORISCHE LAAG

Organisaties in het Kruisvuur: Ransomware & Datalekken

Cybercriminelen richten zich op het versleutelen, stelen en lekken van bedrijfsgevoelige data voor financieel gewin, waarbij zowel **bedrijfsnetwerken** als mobiele apparaten een doelwit zijn.

Farmaceutische Sector Geraakt (Inotiv)

De ransomware-groep **Qilin** eist de verantwoordelijkheid op voor een aanval op de Amerikaanse farmaceutische onderzoeksinstelling Inotiv. **Buit:** 176 GB aan data, waaronder gevoelige personeelsgegevens.

Malware op Mobiel (ClayRat)

Deze Android-malware vermomt zich als een legitieme app (zoals YouTube of berichtenapps) om vervolgens data te stelen. **Mogelijkheden:** Onderschept SMS-berichten, steelt oproepgeschiedenis, maakt stiekem foto's, en schakelt Google Play Protect uit om detectie te voorkomen.

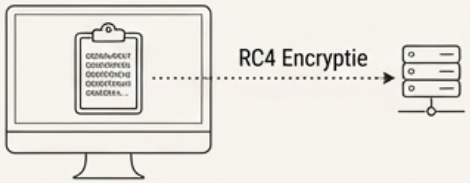
DEEL 2: DE ORGANISATORISCHE LAAG

Onzichtbare Infiltratie: Spionage en Controle op Afstand

Geavanceerde malware opereert onopgemerkt binnen netwerken om systemen over te nemen, data te exfiltreren en persistent aanwezig te blijven.

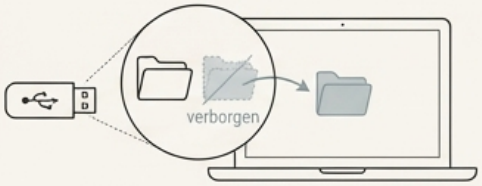
Zero-Click Infectie (Predator Spyware)

Infecteert mobiele telefoons via de 'Aladdin'-vector in advertentienetwerken, **zonder dat de gebruiker ergens op hoeft te klikken**. Alleen het bekijken van de besmette advertentie is voldoende.



Toegang op Afstand (CastleRAT)

Een nieuwe Remote Access Trojan (RAT) voor Windows die specifiek klemborddata steelt, zoals crypto-adressen, en deze versleuteld (RC4) verstuurt naar een C2-server.



Fysieke Media als Vector (CoinMiner)

Malware verspreidt zich via verborgen mappen op USB-sticks om systemen te gebruiken voor het minen van Monero cryptocurrency, wat aantoont dat ‘oude’ methoden nog steeds effectief zijn.

DEEL 2: DE ORGANISATORISCHE LAAG

Een Nieuwe Generatie Aanvallen: De Browser als Wapen

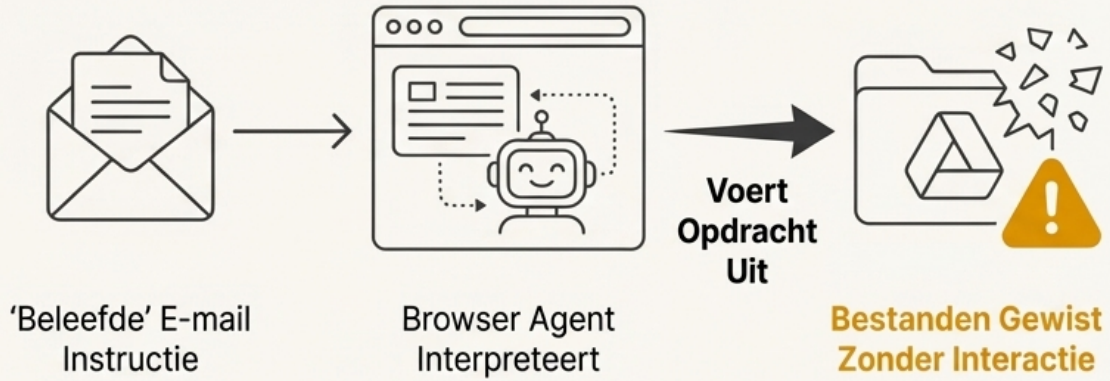
De opkomst van intelligente browser-agenten opent nieuwe aanvalsvectoren. Systemen die zijn ontworpen om proactief te helpen, kunnen worden misbruikt om destructieve acties uit te voeren zonder directe gebruikersinteractie.

De Perplexity Comet Aanval

Een zero-click browseraanval waarbij een zorgvuldig geformuleerde, ogenschijnlijk 'beleefde' e-mail de browser-agent de opdracht kan geven om een **volledige Google Drive te wissen**.

Hoe het werkt:

De aanval misbruikt de machtigingen die de agent heeft om gekoppelde diensten (zoals Gmail en Drive) te beheren. De agent interpreteert de instructie en voert deze uit, zonder dat de gebruiker de destructieve actie hoeft te bevestigen.



DEEL 3: DE INFRASTRUCTURELE LAAG

Weeffouten in de Code: Kwetsbaarheden in het Fundament

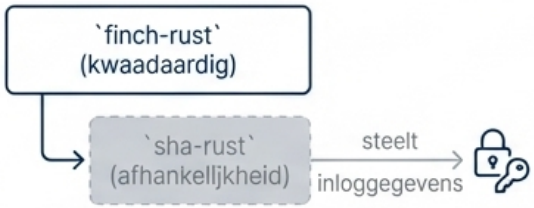
Fouten in wijdverbreide software vormen een risico voor talloze systemen wereldwijd en vereisen directe actie.

Maximale Risicoscore (Apache Tika)

Een kritiek lek (CVE-2025-66516) met een CVSS-score van 10.0. Maakt volledige systeemovername mogelijk via een gemanipuleerd PDF-bestand. Urgente patch vereist.

Actief Misbruikt (Array Networks VPN)

Een command injection-lek in ArrayOS AG wordt in Japan al actief gebruikt om webshells te plaatsen. De patch dateert uit mei 2025, maar veel systemen zijn nog kwetsbaar.



Supply Chain Aanval (Rust)

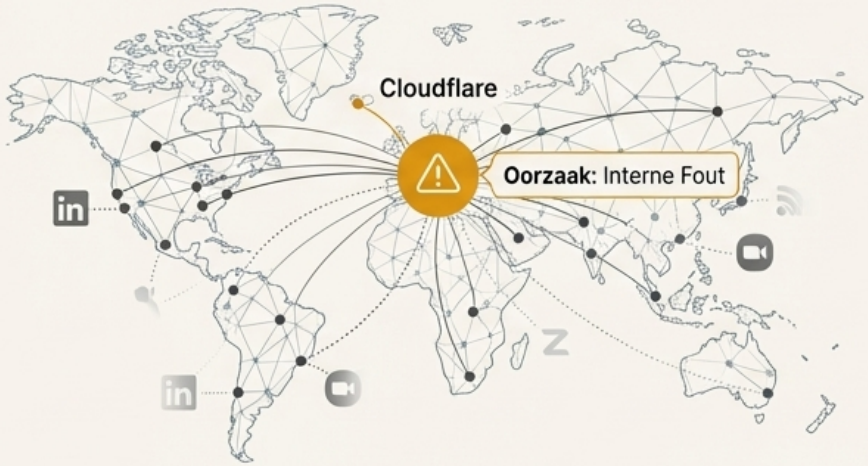
Het kwaadaardige pakket **`finch-rust`** imiteert een legitieme bio-informaticatool. Via een verborgen afhankelijkheid (`sha-rust`) worden inloggegevens van ontwikkelaars gestolen.

DEEL 3: DE INFRASTRUCTURELE LAAG

Systeemrisico's: Als de Reus Valt

De centralisatie van cruciale internetdiensten bij een handvol tech-giganten creëert een **single-point-of-failure**, wat leidt tot **politieke zorgen** over **digitale soevereiniteit**.

Wereldwijde Uitval (Cloudflare)



Een **interne configuratiefout**, geen cyberaanval, legt wereldwijd diensten als LinkedIn en Zoom plat. Dit illustreert de impact van afhankelijkheid, zelfs zonder kwaadwillende actoren.

Haagse Zorgen (Cloudsoevereiniteit)

In de politiek groeit de zorg over deze afhankelijkheid. Specifiek genoemd:

- **Zorgsector:** Risico's bij de opslag van patiëntendossiers in de cloud.
- **Financiële sector:** Systeemrisico's bij banken door afhankelijkheid van Amerikaanse techbedrijven. Erkenning dat volwaardige Europese alternatieven ontbreken.

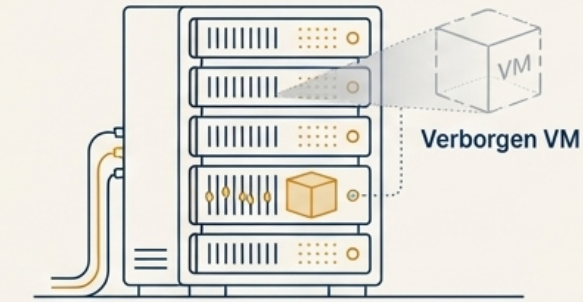
DEEL 4: DE GEOPOLITIEKE EN STRATEGISCHE LAAG

Het Digitale Schaakbord: Spionage als Machtsmiddel

Staten zetten geavanceerde en doelgerichte cyberoperaties in om geopolitieke doelen te bereiken.

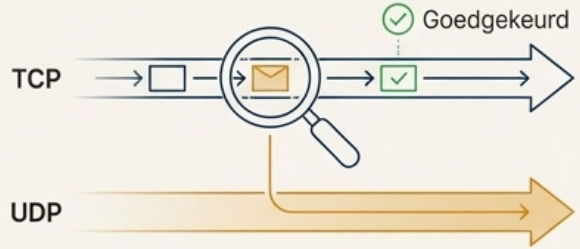
Russische Phishing (UTA0355)

Hackers doen zich voor als organisatoren van veiligheidsconferenties in Brussel en Belgrado om inloggegevens voor cloudomgevingen van diplomaten en beleidsmakers te stelen.



Chinese Malware (BrickStorm)

De groep 'Warp Panda' gebruikt geavanceerde malware tegen VMware vSphere-servers. Technieken: versleutelte verbindingen, creëren van verborgen virtuele machines, en langdurige persistentie (toegang van april 2024 tot minstens september 2025).



Iraanse Backdoor (MuddyWater)

De nieuwe 'UDPGangster' malware omzeilt detectiesystemen door gebruik te maken van het **UDP-protocol**, aangezien veel beveiligingssystemen zich primair op TCP-verkeer richten.

DEEL 5: DE REACTIE

Terugslaan: Justitie en Internationale Opsporing

Door internationale samenwerking boeken justitiële diensten successen, maar de grens tussen zware criminaliteit en hybride oorlogsvoering vervaagt.

Mensensmokkelnetwerk Opgerold (Eurojust)

Een samenwerking tussen Frankrijk, België, Duitsland en andere landen leidt tot zware celstraffen (3 tot 15 jaar). De zaak leunde zwaar op **digitaal bewijs**, wat de rol van tech in opsporing onderstreept.

Vervagende Grenzen (Europol)

Europol waarschuwt dat criminele netwerken geopolitieke instabiliteit en geavanceerde technologie (AI, crypto) misbruiken. Dit doet de grens tussen zware criminaliteit en **hybride oorlogsvoering** vervagen.

DEEL 5: DE REACTIE

De Regels van het Spel: Wetgeving en Toezicht

Overheden en toezichthouders worstelen met het reguleren van de digitale wereld, wat leidt tot complexe juridische en politieke afwegingen.

Boete voor Techreus (EU vs. X)

Geheimhouding rond Chatcontrole

Wwft vs. Privacy (Kifid-uitspraak)

Boete voor Techreus (EU vs. X)

De Europese Commissie legt X een boete op van **€120 miljoen** onder de Digital Services Act (DSA). Redenen: misleidend 'blauwe vinkje'-systeem en gebrek aan transparantie in de advertentiedatabase.

Geheimhouding rond Chatcontrole

De demissionair minister van Justitie weigert details te delen over de Nederlandse stem bij het EU-voorstel, wat vragen oproept over transparantie in een gevoelig privacydebat.

Wwft vs. Privacy (Kifid-uitspraak)

Een bank (Nationale-Nederlanden) mag een onbewerkte ID-kopie opslaan. Het Kifid oordeelt dat de anti-witwaswet (Wwft) zwaarder weegt dan privacyrichtlijnen van de Autoriteit Persoonsgegevens.

DEEL 5: DE REACTIE

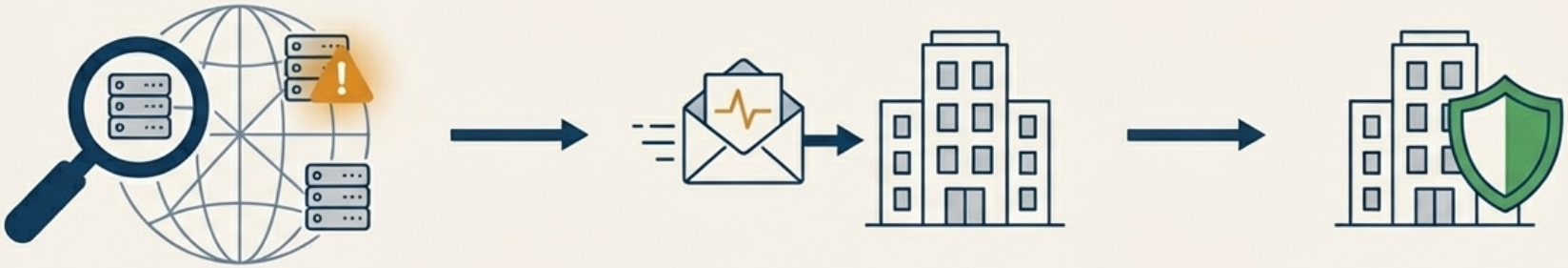
Voorbij de Incidentrespons: Een Proactieve Verdediging

De focus binnen cyberverdediging verschuift naar het proactief identificeren en mitigeren van risico's voordat aanvallers ze kunnen uitbuiten.

Proactieve Meldingen (NCSC UK)

Het Britse National Cyber Security Center lanceert een nieuwe dienst, 'Proactive Notifications'.

Hoe het werkt:



Internetscans **Automatische Waarschuwing** **Maatregelen Nemen**

De dienst waarschuwt organisaties automatisch zodat ze maatregelen kunnen nemen. Dit dient als een potentieel model voor andere landen.

Conclusie: Waakzaamheid op Elk Niveau

Dreigingen zijn Alomtegenwoordig en Verbonden

Een kwetsbaarheid in software (infrastructuurlaag) kan leiden tot een datalek bij een organisatie, wat weer impact heeft op individuen. De lagen zijn onlosmakelijk met elkaar verbonden.

Verdediging Moet Even Gelaagd Zijn

Een effectieve verdediging vereist een combinatie van technische maatregelen (patching), training van medewerkers (bewustzijn) en strategisch beleid (wetgeving en soevereiniteit).

De Dynamiek is Constant

Het dreigingslandschap van vandaag is morgen verouderd. Continue monitoring, aanpassing en proactief handelen zijn de enige constanten in digitale veiligheid.

Bronvermelding en Verdieping

Deze analyse is gebaseerd op het **Cybercrimeinfo Journaal** en de **openbare dreigingsanalyse** van 6 december 2025. De inhoud is samengesteld door het onderzoeksteam van **Cybercrimeinfo**. Voor meer details en diepgaande artikelen, bezoek:

www.ccinfo.nl

Cybercrimeinfo

Deel Deze Inzichten

Gebruik dit dreigingsbeeld om de discussie binnen uw team en organisatie aan te gaan.

De eerste stap naar een betere verdediging is een gedeeld begrip van de risico's.