# Het Digitale Slagveld

## Een 24-uurs Analyse van de Frontlinies

11 December 2025

CYBERCRIMEINFO INTELLIGENCE BRIEFING

# Situatie-update: De Belangrijkste Fronten van 11 December

*De afgelopen dag stond in het teken van een breed scala aan digitale incidenten die de kwetsbaarheid van zowel individuen als grote organisaties blootlegden. Van geavanceerde staatshacks tot fraude met pakketdiensten, het landschap van cyberdreigingen ontwikkelt zich in hoog tempo. Deze briefing analyseert de gebeurtenissen langs vijf cruciale fronten.*

### DE KETEN ALS WAPEN

Misbruik van vertrouwen in logistiek, software en communicatiekanalen.

### DE VOORTDURENDE WAPENWEDLOOP

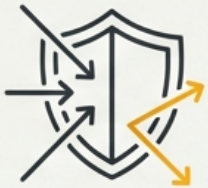
Een stortvloed aan kritieke kwetsbaarheden vereist onmiddellijke actie.

### GEAVANCEERDE AANVALSCAMPAGNES

De specialisatie en verspreiding van geavanceerd digitaal wapentuig.

### CYBER ALS GEOPOLITIEK INSTRUMENT

De inzet van digitale middelen in internationale conflicten en spionage.



### DE TEGENREACTIE

De gecoördineerde respons van rechtshandhaving en beleidsmakers.


Front 1: De Keten als Wapen
Aanvallers misbruiken vertrouwde systemen en merken om verdedigingslinies te omzeilen.
Cybercrimeinfo

# Analyse: Misbruik van Vertrouwen in de Praktijk

## Logistieke Fraude

**Case:** Amazon / PostNL Oplichting

**Methode:** Klonen van PostNL-terminal om retourzendingen te simuleren en goederen te behouden.

**Impact:** €260.000 schade voor Amazon. Celstraffen opgelegd.

amazon postnl

## Phishing via Beveiligingsdienst

**Case:** Mimecast Phishing Campagne

**Methode:** Misbruik van 'secure-link rewriting' functionaliteit om phishing-URL's achter een vertrouwd Mimecast-domein te verbergen. Nabootsing van SharePoint en DocuSign.

**Impact:** 40.000+ phishingmails verstuurd naar 6.000+ organisaties.

mimecast

## Compromittering via Beheersoftware

**Case:** NetSupport Toegangsmisbruik

**Methode:** Meldingen van een incident waarbij legitieme remote support software (NetSupport) is ingezet voor ongeautoriseerde toegang tot een bedrijfsnetwerk in België.

**Impact:** Potentiële spionage en datadiefstal via een vertrouwd IT-instrument.

NetSupport

# Front 2: De Voortdurende Wapenwedloop

*De stroom van kritieke kwetsbaarheden in bedrijfssoftware en hardware-protocollen versnelt.*

# Kwetsbaarheden in Bedrijfssoftware Vereisen Directe Actie

## Microsoft Patch Tuesday (December 2025)

**Overzicht:** 57 lekken gedicht, waarvan 3 zero-days.

### Uitgelicht (Actief Misbruikt):

CVE-2025-62221 in Windows Cloud Files Mini Filter Driver, leidt tot SYSTEM-rechten.

### Uitgelicht (Kritiek):

CVE-2025-62562 in Outlook, kan leiden tot Remote Code Execution (RCE) door enkel te antwoorden op een e-mail.

## Ivanti Endpoint Manager

**Kwetsbaarheid:** Kritieke Cross-Site Scripting (XSS) - CVE-2025-10573.

- **Impact:** CVSS-score 9.6. Ongeauthenticeerde aanvallers kunnen willekeurige code uitvoeren.
- **Regionale Blootstelling:** 37 kwetsbare systemen in Nederland, 5 in België.

## Fortinet Producten

**Kwetsbaarheid:** Kritieke authenticatie-bypass - CVE-2025-59718 & CVE-2025-59719.

- **Impact:** CVSS-score 9.1. Aanvallers kunnen via gemanipuleerde SAML-berichten de FortiCloud SSO-login omzeilen.

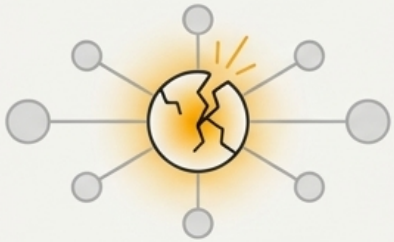
# Wapenwedloop: Van Populaire Tools tot Fundamentele Protocollen

## Case 1: WinRAR Exploit

**Kwetsbaarheid**: CVE-2025-6218 (Path Traversal).

**Status**: Actief misbruikt door diverse groepen (o.a. **Gamaredon**, **Bitter**) voor het plaatsen van backdoors. CISA waarschuwt.

WinRAR



## Case 2: SAP Systeemlekken

**Kwetsbaarheid**: Drie kritieke lekken, waaronder CVE-2025-42880 (Code Injection) met CVSS-score **9.9**.

**Impact**: Potentieel volledige overname van systemen die SAP Solution Manager draaien.

SAP

## Case 3: PCIe Encryptiefouten

**Kwetsbaarheid:** Drie fundamentele fouten (CVE-2025-9612/13/14) in het PCIe Integrity and Data Encryption (IDE) protocol.

**Impact:** Kan leiden tot verwerking van onjuiste of verouderde data, wat de integriteit van data op hardwareniveau ondermijnt.


Persistence
Evasion
C2 Comms
Payload
Front 3: Geavanceerde Aanvalscampagnes
De professionalisering van cybercrime: modulaire malware, supply chain-aanvallen en ontwijkingstechnieken
Loader
Lateral Movement
Data Exfiltration

# Het Arsenaal van de Moderne Cybercrimineel

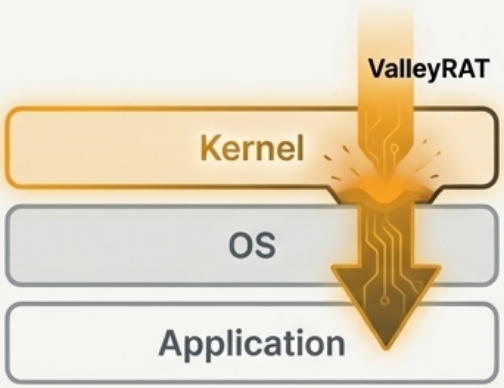
## Exhibit A: 'Spiderman' Phishing-as-a-Service

**Doelwit:** Klanten van tientallen Europese banken (ING, Deutsche Bank) en fintechs (Klarna).

**Techniek:** Modulaire kit met pixel-perfecte replica's van banksites. Onderschept realtime inloggegevens, 2FA en PhotoTAN-codes.

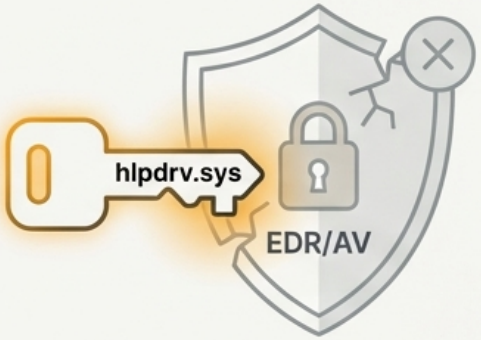
**Verspreiding:** Eén groep die de kit gebruikt telt al meer dan 750 leden.

## Exhibit B: 'ValleyRAT' Backdoor




- **Techniek:** Maakt gebruik van een kernel-mode rootkit om zich diep in Windows 11 te nestelen. Kan antivirus- en EDR-drivers geforceerd verwijderen.
- **Status:** Gelekte 'builder' leidt tot snelle toename in gebruik (85% van detecties in laatste 6 maanden)

## Exhibit C: 'Makop' Ransomware




- **Techniek:** Combineert RDP brute-force aanvallen met Bring Your Own Vulnerable Driver (BYOVD). Misbruikt legitieme, getekende drivers (bv. `hlpdrv.sys`) om EDR/AV op kernelniveau uit te schakelen.

# Aanval op de Bron: Het Developer Ecosysteem als Doelwit

## Case Study 1: Shai-Hulud 2.0 Supply Chain Aanval

- **Vector:** Honderden gemanipuleerde npm-pakketten
- **Methode:** Kwaadaardige code uitgevoerd tijdens pre-installatie fase in CI/CD pipelines, nog vóór beveiligingscontroles.
- **Resultaat:** Diefstal van credentials en configuraties van o.a. Zapier en Postman.


## Case Study 2: React2Shell Exploitatie

- **Vector:** Kritieke RCE-kwetsbaarheid (CVE-2025-55182) in React Server Components
- **Methode:** Wordt op grote schaal misbruikt voor het droppen van crypto miners (XMRig) en nieuwe backdoors (PeerBlight, CowTunnel).
- **Omvang:** Meer dan 165.000 IP-adressen met kwetsbare code gedetecteerd

## Context: De npm Token Transitie

- **Situatie:** GitHub heeft klassieke npm-tokens permanent ingetrokken en pusht ontwikkelaars naar het veiligere OIDC (Trusted Publishing).
- **Dilemma:** Experts van OpenJS waarschuwen voor kwetsbaarheden in de huidige OIDC-implementatie, wat een risico blijft voor kritieke projecten


Front 4: Cyber als Geopolitiek Instrument
Spionage, ondermijning en sanctie-ontduiking: de inzet van digitale middelen door statelijke actoren.
Cybercrimeinfo

# Staten Gebruiken Cyber voor Spionage en Destabilisatie

## Aanval op Persvrijheid

**Doelwit:** "**Reporters Without Borders (RSF).**"
**Aanvaller:** "De aanval wordt gelinkt aan de **Russische FSB-groep Calisto** (ook bekend als ColdRiver)."
**Doel:** "Het ondermijnen van de organisatie die zich inzet for journalisten, nadat RSF in Rusland als 'ongewenste organisatie' werd bestempeld."

## Informatieoorlogvoering & Sancties

**Actie:** "Het **Verenigd Koninkrijk** legt sancties op tegen Russische (o.a. Telegramkanaal Rybar) en Chinese (o.a. i-Soon) actoren."
**Reden:** "Beschuldigingen van het verspreiden van desinformatie en cyberaanvallen gericht op het ondermijnen van westerse democratieën en de steun voor Oekraïne."

## Vervaging van Grenzen

**Actie:** "De **VS** klaagt een Oekraïense vrouw aan voor het ondersteunen van Russische hackergroepen (**CyberArmyofRussia_Reborn** en **NoName057(16)**)."
**Context:** "De aanvallen waren gericht op vitale infrastructuur (o.a. watersystemen) in de VS en NAVO-landen, als onderdeel van Ruslands hybride oorlogsvoering."

# Front 5:
# De Tegenreactie

*De gecoördineerde respons van rechtshandhaving, justitie en internationale samenwerking.*

# Opsporing, Vervolging en Preventie

## Juridische Verantwoording

- **Case 112 DDoS-aanval:** Eis van **8 maanden celstraf** tegen een man die met simboxen het alarmnummer 112 platlegde.
- **Case Amazon Fraude: Celstraffen** en een terugbetalingsplicht van €260.000 opgelegd aan de daders.
- **Case Bitvavo Fraude:** Verdachten van miljoenenroof via helpdeskfraude blijven langer vastzitten.

## Internationale Arrestaties

- **Spanje:** Een 19-jarige hacker gearresteerd voor de diefstal en verkoop van **64 miljoen** persoonsgegevens van 9 verschillende bedrijven.

## Proactief Beleid

- **Wereldwijde Oproep:** Een internationale coalitie (o.a. FBI, NSA, Europol) roept op tot een **verbod op standaardwachtwoorden** in vitale sectoren om de 'digitale deuren' voor aanvallers te sluiten.

# Strategische Implicaties: De Rode Draden op het Slagveld

## Vertrouwen is het Nieuwe Doelwit

Aanvallers focussen niet langer alleen op het doorbreken van perimeters, maar op het misbruiken van inherente vertrouwensrelaties in logistiek (PostNL), beveiliginging (Mimecast) en software (NetSupport).

## De Snelheid van Patching is Cruciaal maar Onvoldoende

De stortvloed van zero-days en kritieke lekken (Microsoft, Ivanti) maakt snelle patching essentieel. Echter, aanvallen op de supply chain (Shai-Hulud) en fundamentele protocollen (PCIe) tonen aan dat een diepere, structurele verdediging nodig is.

## Geopolitiek Bepaalt de Digitale Dreiging

Statelijke actoren (Rusland, China) gebruiken cyberaanvallen als een integraal onderdeel van hun buitenlandbeleid (RSF aanval, desinformatie), wat directe gevolgen heeft voor bedrijven en maatschappelijke organisaties.

## De Grens Tussen Crimineel en Staat Vervaagt

Geavanceerde tools (ValleyRAT kernel rootkits) en technieken (BYOVD) die ooit voorbehouden waren aan staten, zijn nu toe-gankelijk voor criminele groepen. Tegelijkertijd gebruiken staten 'hacktivisten' als dekmantel (CARR/NoName057).