Cyberdreigingsrapport - Week 10, 2026

Briefing Cyberspace | Digiweerbaar BV

Datum: zondag 8 maart 2026 | Periode: 1 t/m 7 maart 2026 | Classificatie: TLP:AMBER

5. EXECUTIVE SUMMARY - Top 3 kritieke dreigingen van de week

1. Odido, het grootste datalek in de Nederlandse geschiedenis (6,5 miljoen klanten)

Het datalek bij Odido domineerde deze week het dreigingslandschap. De groep ShinyHunters publiceerde de volledige dataset op een criminele website, met daarin namen, adressen, telefoonnummers, bankrekeningen, geboortedata en kopieen van identiteitsbewijzen. Bijzonder zorgwekkend is dat 16.300 e-mailadressen van medewerkers bij vitale bedrijven zijn aangetroffen, waaronder NXP, Philips, Rabobank, ProRail, TenneT, Alliander, politie, Schiphol, ASML en het Europees Ruimteagentschap.

Implicatie NIS2: Vitale sectoren zijn direct geraakt. Organisaties moeten hun medewerkers waarschuwen voor gerichte phishing op basis van gelekte gegevens.

Implicatie AVG: Meldingsplicht bij de Autoriteit Persoonsgegevens is geactiveerd. De Check je hack dienst van de politie was nog niet operationeel voor Odido.

2. Ransomware treft drie Nederlandse en Belgische bedrijven

Vier ransomwaregroepen sloegen deze week toe in de Benelux. Akira trof BK Group in Amsterdam (trustkantoor, geregistreerd bij DNB). Qilin claimde het Belgische industriebedrijf Abutriek Service NV in Anzegem. AiLock publiceerde data van Netwerk NV uit Dordrecht (afvalinzameling). Anubis claimde 170 GB aan gestolen data bij AkzoNobel, hoewel dit niet bevestigd is door het bedrijf.

Implicatie NIS2: Financiele dienstverleners en industriele bedrijven vallen onder NIS2 rapportageverplichtingen. Aanval op BK Group raakt de vertrouwenssector.

3. Staatshackers op alle fronten actief, van Rusland tot China en Iran

APT28 (Rusland) misbruikt actief twee Microsoft kwetsbaarheden (CVE-2026-21513 en CVE-2026-21509) via kwaadaardige LNK bestanden. APT36 (Pakistan) zet AI in voor massaproductie van malware in ongewone programmeertalen. Silver Dragon/APT41 (China) richt zich op Europese overheden via Cobalt Strike met Google Drive als commandoserver. CL-UNK-1068 (China) bespioneert telecom en energiesectoren in Azie. Iraanse groepen verhogen hun activiteit met DDoS en ICS aanvallen.

Implicatie NIS2: Organisaties in vitale sectoren moeten hun detectiecapaciteit verhogen voor de genoemde indicators of compromise.

1. PATCHOVERZICHT - Directe actie vereist

Product	CVE	CVSS	Actief misbruikt	Actie
Microsoft MSHTML	CVE-2026-21513	8.8	JA (APT28)	Patch Tuesday februari toepassen
Microsoft Office	CVE-2026-21509	7.8	JA (APT28)	Patch Tuesday februari toepassen
Cisco Secure Firewall MC	CVE-2026-20079	10.0	JA	Direct patchen
Cisco Secure Firewall MC	CVE-2026-20131	10.0	Onbekend	Direct patchen
Cisco SD-WAN Controller	CVE-2026-20127	10.0	JA (CISA KEV)	Direct patchen
BeyondTrust Remote Support	CVE-2026-1731	9.8	JA (ransomware)	Direct patchen, wordt gebruikt in ransomware
Ivanti Endpoint Manager Mobile	CVE-2026-1281	9.8	Onbekend	Direct patchen
WordPress plugin	CVE-2026-1492	9.8	JA (200+ pogingen/24u)	Plugin updaten

Android (Qualcomm)	CVE-2026-21385	Hoog	JA	Android updates installeren
Android 16 System	CVE-2026-0006	Kritiek	Onbekend	Android updates installeren
MongoDB	CVE-2026-25611	7.5	Onbekend	Update naar 8.2.4+
Broadcom VMware Aria Ops	CVE-2026-22719	8.1	JA (CISA KEV)	Direct patchen
Apple iOS/macOS	CVE-2026-20700	7.8	JA (CISA KEV)	Updates installeren
Google Chromium	CVE-2026-2441	8.8	JA (CISA KEV)	Chrome updaten
Microsoft Office Word	CVE-2026-21514	7.8	JA (CISA KEV)	Patch Tuesday toepassen

Weektrend: 90 zeroday kwetsbaarheden werden actief misbruikt in 2025, een stijging van 15% ten opzichte van 2024. Microsoft was het vaakst getroffen (25 zerodays), gevolgd door Google (11) en Apple (8). In 2025 werden 48.196 CVE's gepubliceerd, gemiddeld 132 per dag. Het aantal Known Exploited Vulnerabilities steeg met 30% naar 241, waarvan 39% oorspronkelijk uit 2024 of eerder stamt.

1b. Trending CVE's op Sociale Media

- CVE-2024-23225 - Apple iOS/iPadOS (CVSS 7.8, KEV: JA, Hype Score: 11)
- CVE-2024-23296 - Apple iOS/iPadOS (CVSS 7.8, KEV: JA, Hype Score: 11)
- CVE-2024-50629 - Synology BeeStation/DiskStation (CVSS 5.3, Hype Score: 11)
- CVE-2025-38617 - Linux kernel (CVSS 4.7, Hype Score: 8)
- CVE-2025-14174 - Google Chrome Mac (CVSS 8.8, KEV: JA, Hype Score: 7)

Opvallend: CVE-2025-59287 (Windows Server Update Service, CVSS 9.8, EPSS 75.9%) staat op positie 8 in de trending lijst en verdient extra aandacht vanwege de extreem hoge exploitatiekans.

1c. Actief Misbruikte Kwetsbaarheden (CISA KEV / NCSC)

NL/BE Top 5:

- CVE-2026-1731 - BeyondTrust Remote Support/PRA (CVSS 9.8, EPSS 64.6%, NCSC H/H, RANSOMWARE)
- CVE-2026-20127 - Cisco Catalyst SD-WAN (CVSS 10.0, EPSS 2.6%, NCSC H/H)
- CVE-2022-20775 - Cisco SD-WAN (CVSS 7.8, EPSS 0.5%, NCSC H/H)
- CVE-2026-22719 - VMware Aria Operations (CVSS 8.1, EPSS 7.4%, NCSC M/H)
- CVE-2026-2441 - Google Chromium (CVSS 8.8, EPSS 0.1%, NCSC M/H)

CVE-2026-1731 (BeyondTrust) is bijzonder kritiek: EPSS van 64.6% EN actief gebruikt in ransomware campagnes. Overlap met patchoverzicht hierboven.

Wereldwijd Top 5:

- CVE-2017-7921 - Hikvision producten (CVSS 10.0, EPSS 94.3%)
- CVE-2020-7796 - Zimbra Collaboration Suite (CVSS 9.8, EPSS 93.5%)
- CVE-2025-49113 - Roundcube Webmail (CVSS 9.9, EPSS 90.4%)
- CVE-2024-43468 - Microsoft Configuration Manager (CVSS 9.8, EPSS 85.1%)
- CVE-2026-1731 - BeyondTrust Remote Support/PRA (CVSS 9.8, EPSS 64.6%, RANSOMWARE)

Opvallend: Hikvision CVE-2017-7921 (uit 2017) blijft met EPSS 94.3% de meest misbruikte kwetsbaarheid wereldwijd. Organisaties met Hikvision of Dahua camera's moeten firmware direct updaten.

2. DATALEKKEN & INCIDENTEN

- Odido (NL) - Volledige dataset gepubliceerd door ShinyHunters. Impact: 6,5 miljoen klanten. ID nummers, bankrekeningen, adressen. 16.300 medewerkers vitale bedrijven betrokken
- BK Group (NL, Amsterdam) - Ransomware Akira, trustkantoor bij DNB. Impact: financiele diensten, corporate/private wealth
- SkiWebShop (NL) - Klantgegevens op darkweb te koop. Impact: 81.000 klantgegevens
- AkzoNobel (NL) - Claim door Anubis ransomware. Impact: 170 GB, 169.000 bestanden. Niet bevestigd door bedrijf
- Mall of the Netherlands (NL) - Ongeautoriseerde databasetoegang loyaliteitsprogramma. Impact: namen, e-mail, telefoon, postcode, geboortedatum. AP geinformeerd
- Netwerk NV (NL, Dordrecht) - AiLock ransomware, afvalbedrijf (Korevaar Group). Impact: omvang onbekend
- Abutriek Service NV (BE, Anzegem) - Qilin ransomware, industrieel installatiewerk. Impact: dubbele afpersing (data en versleuteling)
- Brussels Airlines (BE) - Cyberaanval halveerde de winst in 2025. Impact: 68.500 vluchten, 9,1 miljoen passagiers, 1,6 miljard omzet
- Cognizant TriZetto (VS) - Ongeautoriseerde toegang november 2024, pas november 2025 ontdekt. Impact: 3,4 miljoen patienten, detectietijd meer dan 1 jaar
- University of Hawaii (VS) - Ransomware op epidemiologie afdeling. Impact: 1,2 miljoen personen, universiteit betaalde losgeld
- EU politieaccounts (EU) - Verkoop op darkweb voor 900 euro per stuk. Impact: frauduleuze verzoeken aan Meta, Google, Telegram, WhatsApp, TikTok, X

Weektrend: Nederland werd deze week onevenredig hard getroffen met 6 incidenten. Het Odido incident is het grootste datalek in de Nederlandse geschiedenis en zal de komende weken nasleep hebben via gerichte phishing.

3. DREIGINGSACTOREN - Wie was actief

- APT28 (Rusland) - Staatshacker - Doelwit: VS/EU overheden, Oekraine - CVE-2026-21513/21509 exploitatie. Nieuwe malware: BadPaw loader + MeowMeow backdoor
- Silver Dragon/APT41 (China) - Staatshacker - Doelwit: Europese/Aziatische overheden - Cobalt Strike, Google Drive C2, DLL sideloading
- APT36/Transparent Tribe (Pakistan) - Staatshacker - Doelwit: Indiase overheid - AI gegenereerde malware in Nim, Zig, Crystal. Massaproductie
- APT37/ScarCruft (Noord-Korea) - Staatshacker - Doelwit: Air gapped systemen - USB malware via RECYCLE.BIN verstopping
- CL-UNK-1068 (China) - Staatshacker - Doelwit: Telecom, energie, overheid Azie - Xnote malware (sinds 2014), DLL sideloading
- UAT-9244/FamousSparrow (China) - Staatshacker - Doelwit: Zuid-Amerika telecombedrijven - TernDoor, PeerTime (Linux P2P), brute force
- Dust Specter (Iran) - Staatshacker - Doelwit: Iraakse overheid - Nieuwe malware: SPLITDROP, GHOSTFORM
- Iraanse groepen - Staatshacker - Doelwit: Midden-Oosten infrastructuur - DDoS, phishing, ICS aanvallen (NCSC VK waarschuwing)
- ShinyHunters - Crimineel - Doelwit: Odido (NL) - Datalek publicatie, 1-10 miljoen geeist als losgeld
- Akira - Ransomware - Doelwit: BK Group (NL) - Meer dan 620 organisaties sinds maart 2023, ~$244M losgeld
- Qilin - Ransomware - Doelwit: Abutriek (BE) - 1.500+ slachtoffers sinds juli 2022, productie is primair doelwit
- AiLock - Ransomware - Doelwit: Netwerk NV (NL) - Nieuwe groep sinds begin 2025
- Anubis - Ransomware - Doelwit: AkzoNobel (NL, niet bevestigd) - Actief sinds december 2024
- Velvet Tempest - Ransomware - Doelwit: VS non-profit - ClickFix + DonutLoader + CastleRAT. Historisch: Ryuk, Conti, BlackCat
- Funnull CDN - Crimineel - Doelwit: Wereldwijd - 10.748 geinfecteerde IP's, meer dan 1 miljoen gebruikers/dag blootgesteld

Weektrend: Acht staatshackergroepen uit vijf landen waren gelijktijdig actief. China domineert met vier groepen. De convergentie van AI gegenereerde malware (APT36) en klassieke technieken (APT28) maakt detectie complexer.

4. AWARENESS AANDACHTSPUNTEN - Doorsturen naar teams

Odido phishing (NL, actief)

Na het datalek circuleren valse compensatieformulieren en neptelefontjes van "Odido klantenservice". Medewerkers die Odido klant zijn, kunnen gericht benaderd worden met hun echte naam en adres.

Advies: Waarschuw alle medewerkers. Odido stuurt geen compensatieformulieren per e-mail. Bij twijfel bel zelf het officiele nummer van Odido.

ClickFix campagnes (wereldwijd, actief)

Malvertising via zoekmachines leidt naar valse CAPTCHA pagina's die gebruikers vragen een Windows Run commando uit te voeren. Dit installeert malware waaronder Lumma Stealer en CastleRAT. Ook valse installatiepagina's voor Claude Code en andere AI tools zijn waargenomen.

Advies: Blokkeer uitvoering van commando's via Windows Run. Gebruik alleen officiele downloadpagina's voor software.

Valse software updates (wereldwijd, actief)

Neptverzoeken voor Zoom, Teams en Adobe updates verspreiden malware via gestolen Extended Validation certificaten. De updates lijken legitiem en passeren standaard beveiligingscontroles.

Advies: Centraliseer software updates via een patch management systeem. Sta handmatige updates door eindgebruikers niet toe.

Fake tech support (VS/EU, actief)

Voice phishing leidt tot installatie van Microsoft Quick Assist, waarna aanvallers Remote Monitoring tools (Level RMM, XEOX) en Havoc C2 installeren voor volledige toegang.

Advies: Beperk Microsoft Quick Assist via groepsbeleid. Train medewerkers om onverwachte supportverzoeken te herkennen.

Watergroep phishing (BE, actief)

In Zelzate circuleren valse e-mails namens De Watergroep met een compensatie van 124 euro. Dit volgt op echte compensatie door Farys voor bruin water. De echte vergoeding wordt automatisch verstrekt.

Advies: Herinner Belgische medewerkers dat nutsbedrijven nooit bankgegevens opvragen per e-mail.

Browser als aanvalsoppervlak

Onderzoek toont dat 41% van medewerkers AI webtools gebruikt, waarvan 46% gevoelige data invoert via persoonlijke accounts. Phishing domeinen zijn gemiddeld 18 jaar oud, waardoor blokkering op basis van domeinleeftijd niet werkt.

Advies: Implementeer browser isolatie en DLP beleid voor AI tools. Blokkeer persoonlijke accounts op zakelijke apparaten.

6. SECTORSPECIFIEKE RISICO'S

- Telecom (KRITIEK) - Odido datalek (6,5M NL), Chinese APT's (UAT-9244 op Zuid-Amerika telecom)
- Financiele diensten (HOOG) - BK Group ransomware (Akira), BeyondTrust KEV (ransomware)
- Industrie/productie (HOOG) - AkzoNobel (Anubis claim), Abutriek (Qilin), Netwerk NV (AiLock). Qilin richt 39% van aanvallen op productiesector
- Overheid/defensie (HOOG) - EU politieaccounts op darkweb, APT28 actief, DigiD afhankelijkheid
- Retail (VERHOOGD) - Mall of the Netherlands (databasetoegang), SkiWebShop (81K op darkweb)
- Luchtvaart (VERHOOGD) - Brussels Airlines winst gehalveerd door cyberaanval
- Gezondheidszorg (VERHOOGD) - Cognizant TriZetto (3,4M patienten), University of Hawaii (1,2M)

- Cloud/infrastructuur (VERHOOGD) - AWS ME datacenters fysiek getroffen door drone aanvallen (109 diensten)
- Gebouwautomatisering (VERHOOGD) - Honeywell BMS controllers: authenticatie bypass in IQ4E, IQ412, IQ422 en andere modellen

7. OPERATIONELE VERSTORINGEN

- AWS ME-CENTRAL-1 - Drone aanvallen op datacenters VAE/Bahrein. 109+ diensten uitgeschakeld, meerdere dagen. Status: noodtoestand
- Wikipedia/MediaWiki - JavaScript worm via User scripts. 3.996 pagina's gewijzigd, 85 accounts gecompromitteerd. Status: hersteld (23 min actief)
- Brussels Airlines - Cyberaanval op systemen. Operationele verstoringen vluchten. Status: onder onderzoek
- Iran nationaal internet - Staatsingrijpen tijdens luchtaanvallen. Netwerkverkeer daalde tot 4% van normaal. Status: tijdelijk

8. REGELGEVING & COMPLIANCE

Nederland, Kamermotie datalekken

Naar aanleiding van het Odido incident heeft de Tweede Kamer een motie ingediend voor een handelingskader voor slachtoffers van datalekken. Partijen VVD, CDA, ChristenUnie, D66 en JA21 steunen de motie.

Nederland, DigiD soevereiniteit

De Tweede Kamer heeft een motie aangenomen die vereist dat servers, opslag en beveiliging van DigiD in Nederlandse handen blijven. Dit volgt op zorgen over een mogelijke overname door Solvinity.

Nederland, Belastingdienst en buitenlandse software

Kamervragen zijn gesteld over de keuze van de Belastingdienst voor het Amerikaanse bedrijf Fast Enterprises. Zorgen betreffen spionagerisico's en datasoevereiniteit.

Autoriteit Persoonsgegevens, AI waarschuwing

De AI Impactbarometer van de AP toont een verdubbeling van rode markers (van 2 naar 4). De AP waarschuwt dat de implementatie van de AI Verordening achterblijft en dat lessen van het toeslagenschandaal niet worden geleerd. Specifiek benoemd: discriminerende algoritmes, deepfakes en AI gestuurde fraude.

Internationaal, leeftijdsverificatie

300+ wetenschappers uit 30 landen, waaronder Nederland, waarschuwen in een open brief tegen online leeftijdsverificatie vanwege privacy en datalekrisico's.

Verzekeringsmarkt, cyberrisico

Europees cyberverzekeraar Stoik rapporteert een stijging van claimfrequentie met 150% (van 4,3% naar 10,6% in 2024-2025). E-mail incidenten vormen 59,4% van alle claims. Ransomware werd 60% impactvoller.

9. VOORUITBLIK - Week 11

Odido nasleep

De komende week is verhoogde waakzaamheid geboden voor gerichte phishing op basis van gelekte Odido data. Medewerkers van vitale organisaties (NXP, Philips, ProRail, TenneT, politie, Schiphol, ASML) lopen extra risico. Monitor inkomende e-mail op spear phishing met persoonlijke gegevens.

Patch Tuesday maart (11 maart)

Microsoft Patch Tuesday staat gepland voor dinsdag 11 maart. Gezien de actieve exploitatie van CVE-2026-21513 en CVE-2026-21509 door APT28, is snelle toepassing van nieuwe patches essentieel. Bereid het patchproces voor.

Ransomware druk houdt aan

Met vier Benelux slachtoffers in een week is de ransomwaredruk uitzonderlijk hoog. Qilin, Akira en AiLock zijn alle drie actief in de regio. Test uw backups en incident response plan.

AI als aanvalstool

De inzet van AI voor malwareproductie (APT36) en de opkomst van AI gestuurde aanvalstools signaleren een structurele verschuiving. Traditionele signature based detectie wordt minder effectief tegen polymorphe, AI gegenereerde malware.

Aanbevelingen voor de komende week:

- Communiceer het Odido risico naar alle medewerkers
- Controleer of Patch Tuesday februari volledig is uitgerold (APT28 kwetsbaarheden)
- Verifieer BeyondTrust, Cisco en Ivanti patchstatus (CISA KEV)
- Test backup en recovery procedures
- Evalueer browser isolatie en DLP beleid voor AI tools
- Controleer Hikvision/Dahua camera firmware (CVE-2017-7921 nog steeds meest misbruikt)

Bronnen: MijnCcinfoPDF dagrapportages 1-7 maart 2026, CISA KEV database, NCSC kwetsbaarheidswaarschuwingen, CVEmon RSS, CVEDB Shodan

Rapport samengesteld door Digiweerbaar BV - Briefing Cyberspace Week 10