Briefing Cyberspace

Cyberdreigingsrapport

10 maart 2026

TLP:AMBER

Executive Summary - Top 3 Kritieke Dreigingen

1 Russische staatshackers richten zich op Signal en WhatsApp KRITIEK

MIVD en AIVD waarschuwen dat Russische hackers actief accounts van Nederlandse overheidsfunctionarissen, militairen en journalisten proberen over te nemen via social engineering. Geen technische aanval op de apps zelf.

2 Hikvision CVSS 10.0 breed misbruikt KRITIEK KEV

CVE-2017-7921 maakt volledige authenticatie bypass mogelijk. EPSS 94,3%. Wijdverspreid in NL/BE. CISA deadline 26 maart 2026.

3 Supply chain risico via macOS malware en valse AI extensies HOOG

SHub Stealer vervangt cryptowallet bestanden op macOS. Valse AI browserextensies compromitteren 20.000+ bedrijfsomgevingen en stelen AI chatgeschiedenissen.

Patchoverzicht + Trending CVE's + Misbruikte Kwetsbaarheden

Directe actie vereist

Product	CVE	CVSS	Misbruikt	Actie
Hikvision	CVE-2017-7921	**10.0**	**Ja (KEV)**	Firmware update / uit dienst
Apple macOS/iOS	CVE-2023-43000	8.8	**Ja (KEV)**	Updates toepassen
Nginx UI	CVE-2026-27944	**9.8**	PoC beschikbaar	Upgraden naar 2.3.3
ExifTool (macOS)	CVE-2026-3102	Hoog	Onbekend	Updaten naar 13.50

Top 5 Trending (sociale media)

1. CVE-2024-23225 (Apple, 7.8, KEV) Hype 13
2. CVE-2025-59287 (WSUS, 9.8, KEV) Hype 12
3. CVE-2025-43300 (Apple, 10.0, KEV) Hype 11
4. CVE-2025-26399 (SolarWinds, 9.8, KEV) Hype 9
5. CVE-2025-14174 (Chrome, 8.8, KEV) Hype 9

Top 5 NL/BE Misbruikt (NCSC)

1. CVE-2026-1731 (BeyondTrust, 9.8) Ransomware
2. CVE-2026-20127 (Cisco SD-WAN, 10.0)
3. CVE-2026-1603 (Ivanti EPM, 8.6)
4. CVE-2022-20775 (Cisco SD-WAN, 7.8)
5. CVE-2026-22719 (VMware Aria, 8.1)

Datalekken en Incidenten

Ericsson US - Supply chain datalek via serviceprovider

Data van werknemers en klanten gestolen (17-22 april 2025, pas maart 2026 gemeld). Blootgesteld: namen, adressen, BSN, rijbewijsnummers, financiele en medische gegevens. 4.377 personen in Texas bevestigd. Geen ransomwaregroep heeft de aanval opgeist.

Spaanse belastingdienst (AEAT) - Personeelsgegevens gelekt

Dreigingsactor lekte persoonlijke gegevens van medewerkers van alle rangen. Risico op intimidatie en gerichte social engineering.

Yummy Rides Venezuela - 30.000 chauffeurfoto's gelekt

Database met foto's en volledige namen gratis beschikbaar op het darkweb.

Benelux impact

Het Ericsson incident betreft een supply chain aanval. Nederlandse en Belgische telecomklanten van Ericsson kunnen geraakt zijn. Dit onderstreept het belang van third party risk management conform NIS2 Artikel 21.

Dreigingsactoren - Wie is actief

Staatshackers

Rusland - Signal/WhatsApp kapingen
Social engineering gericht op NL overheid, militairen, journalisten. QR code misbruik en nep support. (MIVD/AIVD)

Iran - Bewakingscamera's als wapen
Honderden hackpogingen op camera's in Midden-Oosten, getimed rond raketaanvallen. (Check Point)

Iran/MuddyWater - VS infrastructuur
Actief bij Amerikaanse bank, luchthaven en defensie. Nieuwe backdoors Dindoor en Fakeset. (Symantec)

Cybercriminelen

SHub Stealer - macOS supply chain
Nep CleanMyMac site, ClickFix, vervangt cryptowallet bestanden. CIS geofencing. (Malwarebytes)

VIP Keylogger - MaaS credential theft
Steganografie, in memory executie, modulair product voor tientallen browsers. (K7 Labs)

ScamAgent - AI oplichtingsframework
Rutgers University toont hoe LLM's autonome scam gesprekken kunnen voeren. Omzeilt veiligheidsfilters.

Awareness - Doorstuurbaar naar teams

Valse SMS uit naam van MijnOverheid

Sms vraagt om gegevens bij te werken via een link. Daarna belt een "bankmedewerker" die dreigt een wijkagent te sturen.

Advies: niet klikken, geen gegevens invullen, bij twijfel zelf uw bank bellen.

Afpersmail dreigt met publicatie op darkweb

Mail beweert persoonlijke gegevens te bezitten en eist bitcoins. Kan lijken van uw eigen adres te komen (spoofing).

Advies: bluf, niet reageren, verwijderen. Speelt in op onrust door recente datalekken.

Valse AI browserextensies stelen bedrijfsdata

900.000 installaties, 20.000+ bedrijven geraakt. Extensies verzamelen AI chatgeschiedenissen met interne code en plannen.

Advies: controleer extensies, verwijder onbekende, blokkeer deepaichats[.]com en chatsaigpt[.]com.

Signal/WhatsApp account kaping door staatshackers

Deel NOOIT verificatiecodes. Scan geen onbekende QR codes. Negeer berichten van "Signal support".

Advies: controleer regelmatig uw lijst met gekoppelde apparaten. Verwijder onbekende apparaten direct.

Sectorspecifieke Risico's

Sector	Niveau	Dreigingen vandaag
Overheid	KRITIEK	Russische staatshackers richten zich op Signal/WhatsApp van overheidsfunctionarissen (MIVD/AIVD)
Telecom	HOOG	Ericsson supply chain datalek, MuddyWater actief bij Amerikaanse telecom
Financiele dienstverlening	HOOG	Argenta phishing in Belgie, valse MijnOverheid sms + bankfraude, MuddyWater bij Amerikaanse bank
Defensie	HOOG	Signal/WhatsApp kaping gericht op militairen, Iran gebruikt camera's voor militaire doelselectie
IT/Technologie	VERHOOGD	Valse AI extensies bij 20.000+ bedrijven, ExifTool RCE op macOS, Nginx UI backup lek

Regelgeving en Compliance

Trump Nationale Cyberstrategie - Deregulering

Vier pagina's (vs. 35 pagina's Biden). Focus op offensieve cyberacties en minder regelgeving. SEC disclosure rule en CIRCIA worden "aangepakt". Impact voor internationale bedrijven aan Amerikaanse beurzen.

Kamervragen cloudrisico's - Amazon European Sovereign Cloud

D66, GroenLinks-PvdA en CDA vragen minister Van Weel om opheldering over offline gehaald rapport. Kritiek TU Delft: rapport leunt te zwaar op aannames over AWS techniek. Minister heeft drie weken reactietijd.

Privacy First vs. Europese digitale identiteit

AMLA wil gebruik verplicht stellen bij banken voor niet fysieke identificatie. Privacy First stelt dat dit in strijd is met eIDAS verordening (vrijwilligheid). Relevant voor financiele instellingen (antiwitwasverordening halverwege 2027).

NSA/Cyber Command benoeming

Luitenant-generaal Joshua Rudd passeert Senaatshorde (68-28). Definitieve stemming dinsdag verwacht. Senator Wyden noemt benoeming een "vergissing".

Aanbevolen Acties

1. **Hikvision apparaten inventariseren en patchen** - CVE-2017-7921 (CVSS 10.0, EPSS 94,3%). Deadline 26 maart. Apparaten die geen updates ontvangen uit dienst nemen.
2. **Medewerkers waarschuwen voor Signal/WhatsApp kaping** - Deel geen verificatiecodes, scan geen onbekende QR codes, controleer gekoppelde apparaten. Bijzondere aandacht voor management en bestuur.
3. **Browserextensies auditen** - Controleer alle Chromium extensies op onbekende AI tools. Blokkeer domeinen deepaichats[.]com en chatsaigpt[.]com. Overweeg allowlisting beleid.
4. **Apple en Cisco patches uitrollen** - Drie Apple CVE's in KEV (macOS/iOS). Cisco SD-WAN CVE-2026-20127 (CVSS 10.0). BeyondTrust CVE-2026-1731 (ransomware badge).
5. **Third party risk assessment voor serviceproviders** - Het Ericsson incident toont het risico van supply chain aanvallen. Controleer contractuele afspraken over meldplicht en beveiligingseisen bij leveranciers.