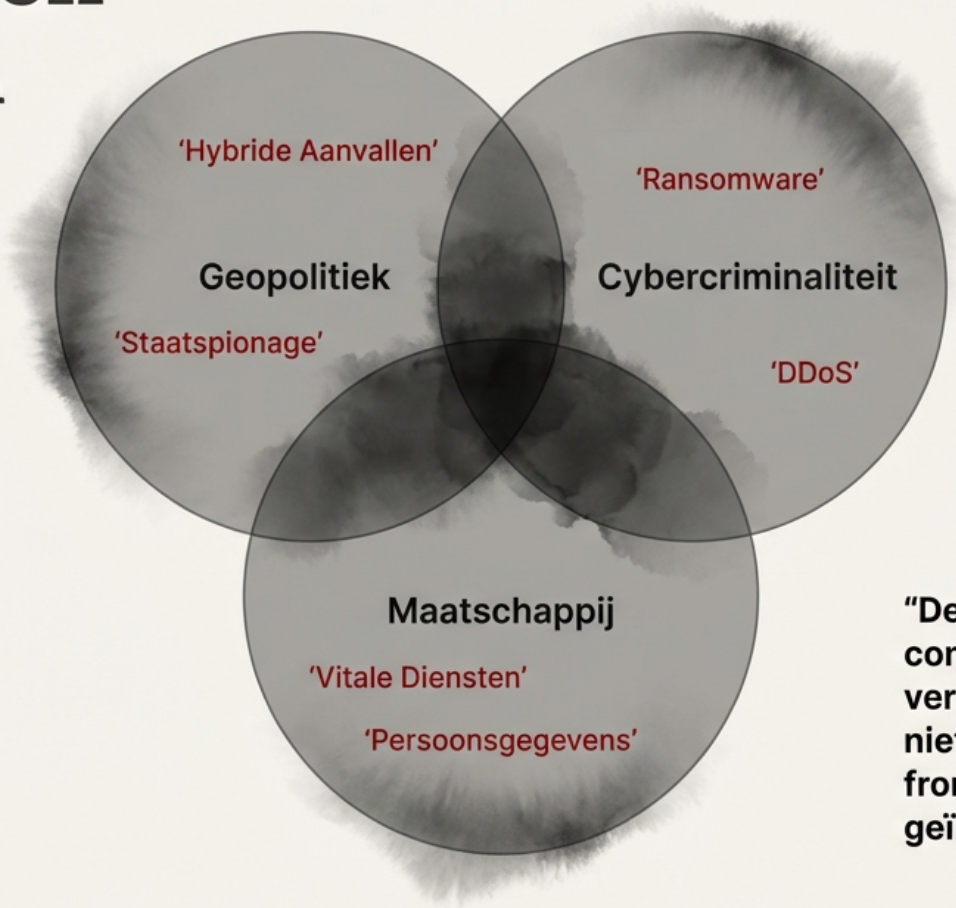

Het Digitale Slagveld
Een 24-uurs Analyse van een Geïntegreerde Dreiging | 10-12-2025
Cybercrimeinfo

De Grenzen Vervagen



“De grens tussen geopolitiek conflict en cybercriminaliteit vervaagt verder. De strijd wordt niet langer op geïsoleerde fronten gevoerd, maar in één geïntegreerde realiteit.”

Drie Fronten, Eén Realiteit

Om de complexiteit van vandaag te begrijpen, analyseren we de strijd op drie cruciale, met elkaar verweven fronten:

1. Het Nationaal Niveau:
Geopolitiek & Vitale Infrastructuur

2. Het Corporate Niveau:
De Onderneming onder Vuur

3. Het Persoonlijk Niveau:
Het Individu als Doelwit & Wapen

Front 1: Vitale Diensten als Direct Doelwit

Gecoördineerde DDoS-aanvallen leggen de kwetsbaarheid van de academische, logistieke en publieke sector in de Benelux bloot.

Case Details
Aanvaller: Hackerscollectief NoName

Doelwitten: KU Leuven, regio Wallonië, Bruxelles-Propreté, luchtvaartspeler SABCA, logistiek dienstverlener AGZ Port Services.

Front 1: Commerciële Software als Poort voor Staatspionage

Door China gesteunde actoren infiltreren vitale sectoren door misbruik te maken van bekende kwetsbaarheden in enterprise software.

Aanvaller:
China-backed Group

Methode:
Exploitatie van Ivanti Connect Secure (CVE-2024-21893)

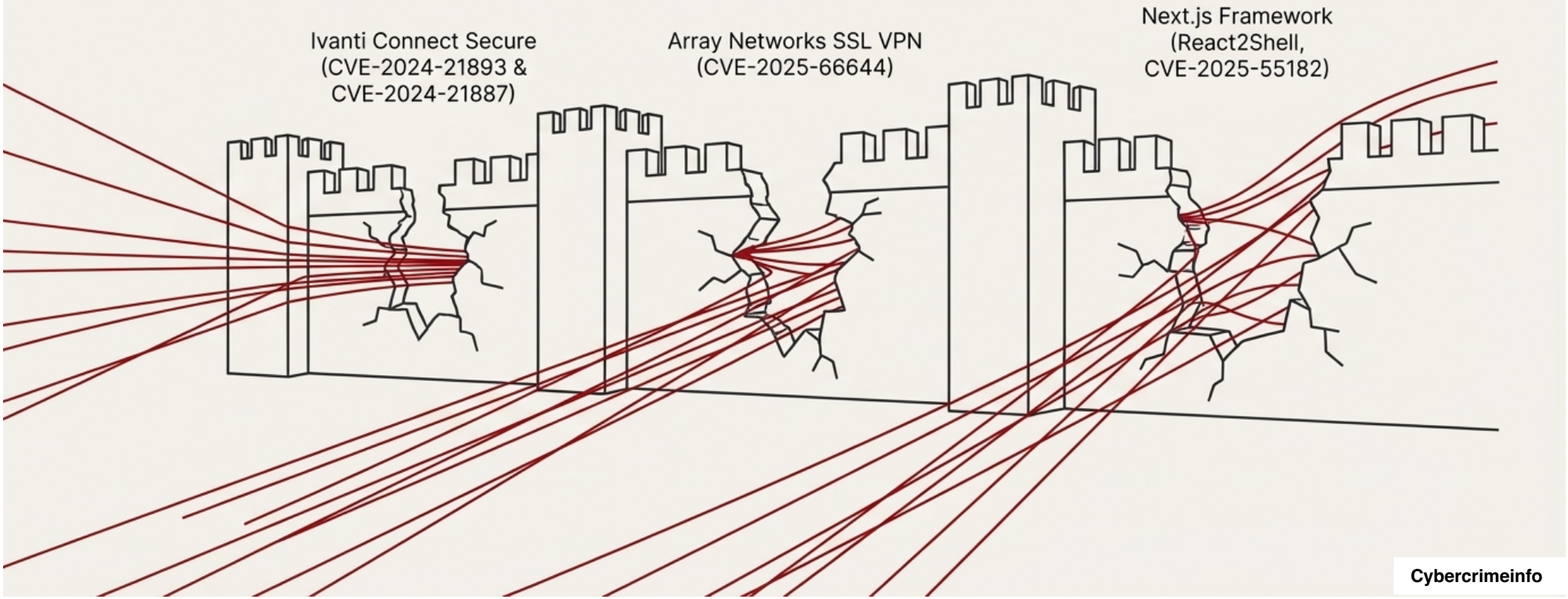
Doelwit:
Japanse transportbedrijven

Payload:
Installatie `MetaRAT`-malware

Context: Dit illustreert het dilemma waar de Nederlandse overheid voor staat (besluit om geen specifieke scan naar Chinese apparatuur uit te voeren).

Front 2: De Poorten van de Onderneming Staan Open

Kernboodschap: Kritieke lekken in netwerkinfrastructuur en enterprise software worden niet alleen ontdekt, maar ***actief en op grote schaal*** misbruikt.



Front 2: Een Arsenaal van Geavanceerde Malware

Aanvallers gebruiken een divers en steeds geavanceerder arsenaal om detectie te omzeilen en diepe toegang te verkrijgen.

MetaRAT

Geavanceerde PlugX-variant, verspreid via Ivanti-lek.

EtherRAT

Verspreid door Lazarus (Noord-Korea) via React2Shell, gebruikt blockchain voor C2.

GhostPenguin

Onzichtbare Linux-backdoor die via versleutelde UDP-pakketten communiceert.

Broadside

Mirai-botnet variant die videorecorders op schepen infecteert, compromitteert fysieke beveiliging.

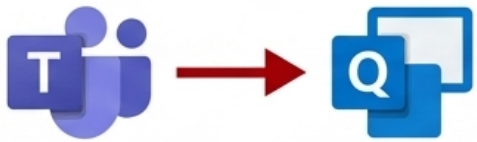
QWCrypt

Ransomware ingezet door STAC6565 via legitieme sollicitatieplatforms.

Front 3: Vertrouwen als Wapen

Kernboodschap: Social engineering evolueert van simpele phishing naar complexe, multikanaals aanvallen die legitieme tools en vertrouwde merken misbruiken.

Vishing 2.0



Aanvallers doen zich voor als IT-support via Microsoft Teams, overtuigen slachtoffer QuickAssist te gebruiken om fileless malware te laden.

Platform Hijacking

Officieel X-account van SimpleX Chat gekaapt via 'delegate'-functie om frauduleuze cryptoverkoop te promoten.

Klassieke Fraude

Bankhelpdeskfraude in IJsselstein resulteert in duizenden euro's schade.

Front 3: Het Individu als Risico en Ideologisch Slagveld

Onze digitale voetafdruk en online gedrag creëren risico's en vormen een voedingsbodem voor radicalisering.

Datalekken: 30 miljoen persoonsgegevens gelekt bij retailgigant Coupang (Zuid-Korea). De 'brandstof' voor toekomstige aanvallen.

Privacy vs. Veiligheid: Kritiek van BSI op Google Chrome's wachtwoordmanager en waarschuwingen van EFF tegen verplichte online leeftijdsverificatie.

Radicalisering: NCTV waarschuwt voor individualisering van terrorisme; radicalisering vindt plaats via online gamingplatforms en chatgroepen.

De Tegenbeweging

Terwijl de dreigingen **escaleren**, intensiveren overheden, opsporingsdiensten en de tech-gemeenschap hun inspanningen op het gebied van opsporing, regulering en werving.

Terugslaan: Arrestaties, Werving en Regulering

Concrete acties tonen de veelzijdigheid van de verdediging.

Opsporing & Arrestaties

- Drie Oekraïners gearresteerd in Polen met geavanceerde hackapparatuur (incl. Flipper Zero).
- Oplichters bankhelpdeskfraude aangehouden in IJsselstein.

Werving & Bewustwording

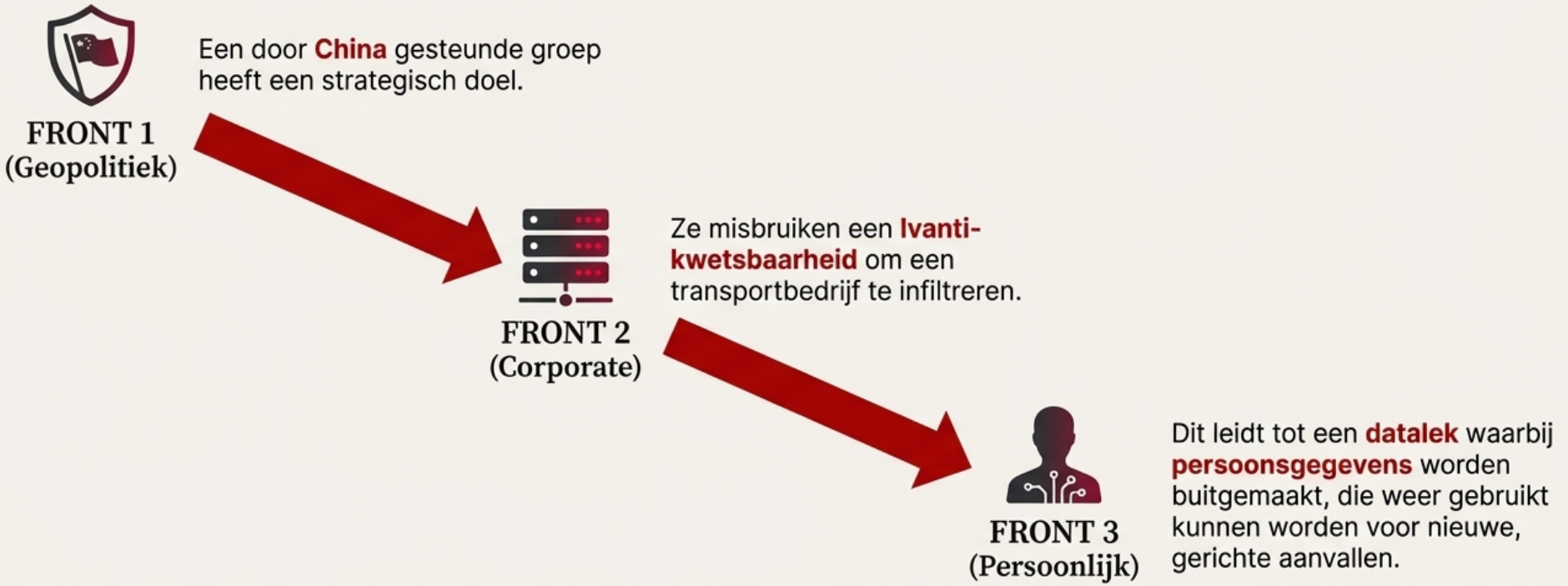
- Politie en Tweakers lanceren 'Operatie 1337' om cybertalent te werven.

Regulering & Juridische Strijd

- Google veroordeeld tot €20 miljoen boete aan Belgische uitgever Rossel.
- Belgische GBA dwingt Freedelity tot aanpassing na onrechtmatig gebruik ID-kaart.

De Synthese: Alles is Verbonden

Een enkel incident is zelden geïsoleerd. De aanvallen van vandaag weven een web door alle drie de fronten.



De Strategische Vragen voor Morgen

1. Hoe weerbaar is onze vitale én corporate infrastructuur tegen een **statelijke actor die niet primair financieel, maar disruptief of strategisch gemotiveerd is?**
2. Begrijpen we de complexiteit van onze eigen digitale supply chain, van een VPN-gateway zoals Ivanti tot een simpele Visual Studio Code-extensie die een ontwikkelaar installeert?
3. In een wereld van geavanceerde social engineering en online radicalisering, hoe maken we van onze medewerkers en klanten onze sterkste verdedigingslinie in plaats van ons grootste risico?