Week 04-2026

Analyserapport Bedreigingslandschap: De Evolutie van Initiële Toegang en Identiteitsfraude (Editie 2026)

1. Strategische Context: De Verschuiving in het Dreigingslandschap

In 2026 is de grens tussen digitale manipulatie en fysieke dreigingen nagenoeg verdwenen. De focus van aanvallers is definitief verschoven van het exploiteren van technische kwetsbaarheden naar het manipuleren van vertrouwde infrastructuren en menselijke processen. We zien dat initiële toegang (Initial Access) steeds vaker een bijproduct is van de Europese afhankelijkheid van niet-Europese "Big Tech" infrastructuren.

De Europese Commissie overweegt inmiddels restricties op technologie uit landen als China wegens spionagezorgen, terwijl de roep om digitale autonomie in Nederland wordt versterkt door dossiers zoals de mogelijke overname van Solvinity door Kyndryl. Het platform *Firewall* van Eric Smit waarschuwt hier terecht voor het risico op Amerikaanse overheidsinmenging (via de Cloud Act) in vitale infrastructuren zoals DigiD.

Strategische Implicaties Traditionele verdedigingsmechanismen, zoals standaard MFA en statische scanners, volstaan niet meer tegen 'Adversary-in-the-Middle' (AiTM) tactieken die tokens in real-time onderscheppen. Beveiliging is in 2026 geen kwestie meer van het dichttimmeren van de digitale voordeur, maar van het beheersen van de volledige browser- en identiteitsketen.

2. Browser-gebaseerde Aanvallen: De Casus GhostPoster

De browser is de primaire werkplek en daarmee het belangrijkste aanvalsoppervlak geworden. De GhostPoster-campagne illustreert een fundamentele vertrouwensbreuk: malafide extensies bleven tot wel vijf jaar onopgemerkt in officiële stores van Google, Microsoft en Mozilla. Dit markeert het falen van geautomatiseerde store-vetting door de grote tech-providers.

De Omvang van de Infiltratie

Onderzoek heeft 17 extensies geïdentificeerd met in totaal meer dan **840.000 installaties**:

- **Google Translate in Right Click:** 522.398 installaties
- **Translate Selected Text with Google:** 159.645 installaties
- **Ads Block Ultimate:** 48.078 installaties
- **Floating Player - PiP Mode:** 40.824 installaties
- **Convert Everything:** 17.171 installaties
- **Youtube Download:** 11.458 installaties
- **One Key Translate:** 10.785 installaties
- **AdBlocker:** 10.155 installaties
- **Save Image to Pinterest on Right Click:** 6.517 installaties
- **Instagram Downloader:** 3.807 installaties
- **RSS Feed:** 2.781 installaties
- **Cool Cursor:** 2.254 installaties
- **Full Page Screenshot:** 2.000 installaties
- **Amazon Price History:** 1.197 installaties
- **Color Enhancer:** 712 installaties
- **Translate Selected Text with Right Click:** 283 installaties
- **Page Screenshot Clipper:** 86 installaties

Technische Diepgang: Steganografie 2.0 De verfijning van GhostPoster ligt in het verbergen van kwaadaardige code. In geavanceerde varianten zoals de 'Instagram Downloader' werd de staging-logica verplaatst naar het achtergrondscript. Dit script scant de raw bytes van een gebundeld afbeeldingsbestand op een specifieke delimiter (>>>>). De data na deze delimiter wordt geëxtraheerd, opgeslagen en via Base64 gedecodeerd als JavaScript. In combinatie met een "dormancy period" van 48 uur tot 5 dagen omzeilt dit effectief sandbox-detectie.

3. Van Browser DoS naar Systeemovername: De KongTuke/CrashFix Campagne

De KongTuke-groep (ook bekend als 404 TDS) combineert technische disruptie met psychologische druk. Hun 'CrashFix' methodiek maakt misbruik van de frustratie van de gebruiker bij een haperende browser.

De Infectieketen

1. **Imitatie:** Gebruikers worden via malafide advertenties verleid tot het installeren van 'NexShield' (een kopie van uBlock Origin Lite).

2. **Geforceerde Browser DoS:** De extensie triggert een infinite loop die het geheugen uitput, waardoor de browser onbruikbaar wordt en crasht.
3. **Social Engineering:** Na herstart toont een pop-up een valse waarschuwing over een "abnormale stop" en instrueert de gebruiker om een scan uit te voeren.
4. **De ClickFix Techniek:** De gebruiker wordt gevraagd een commando in het Windows-uitvoervenster te plakken. De extensie heeft echter al een kwaadaardig PowerShell-commando naar het klembord gekopieerd dat gebruikmaakt van `finger.exe` om de uiteindelijke payload op te halen.

Operationele Impact De campagne richt zich specifiek op **domain-joined systemen**. Wanneer een zakelijk netwerk wordt herkend, wordt de **ModeloRAT** uitgerold. Deze Python-gebaseerde RAT maakt gebruik van **RC4-encryptie** voor C2-communicatie en dient als wegbereider voor ransomware-groepen zoals *Rhysida* en *Interlock*.

4. De Helpdesk als Aanvalsvector: Social Engineering & Identiteitsfraude

De helpdesk is de 'zachte onderbuik' van de organisatie geworden, waarbij aanvallers technische barrières omzeilen door menselijke emotie en behulpzaamheid te exploiteren.

Casuïstiek Analyse

- **Salarisfraude & OSINT:** Aanvallers gebruiken publieke informatie (OSINT) om verificatievragen te beantwoorden en helpdeskmedewerkers te overtuigen MFA-apparaten opnieuw te registreren. In gedocumenteerde gevallen leidde dit tot het wijzigen van bankgegevens voor salarisbetalingen.
- **De Kifid-uitspraak (SNS vs. ING):** Een cruciaal juridisch precedent in 2026. Een klant werd via **AnyDesk** opgelicht. Het Kifid stelde SNS Bank deels aansprakelijk omdat zij, na het detecteren van verdachte overboekingen, verzuimden de ontvangende bank (ING) tijdig te waarschuwen. Dit onderstreept de zorgplicht voor inter-organisatorische signalering.
- **Vishing & AiTM:** Microsoft en Okta waarschuwen voor phishingkits die in real-time interageren met vishing-gesprekken. Aanvallers praten slachtoffers door nummer-matching MFA heen, terwijl ze de phishingpagina live aanpassen aan de status van het gesprek.

5. Emerging Threats: Schaduw-IT, AI-Agents en Fileless Malware

De snelle adoptie van AI en cloud zonder adequate governance creëert een schaduwlandschap dat door aanvallers actief wordt ontgonnen.

Dreigingsmatrix

Vector	Beschrijving	Strategische Analyse
Onveilige Training Apps	Publieke instances van apps zoals DVWA en Hackazon in Fortune 500 clouds.	20% van de onderzochte instances bevatten actieve **XMRig cryptominers**. Te ruime IAM-rollen geven aanvallers vaak direct 'AdministratorAccess'.
AI-Framework Lekken	*ChainLeak* (Chainlit) en *BodySnatcher* (ServiceNow AI-agents).	Mogelijkheid tot volledige systeemovername door het misbruiken van hardcoded geheimen in AI-infrastructuren.
Fileless Persistentie	**PDFSIDER** en **PixelCode** (YouTube).	PDFSIDER misbruikt DLL side-loading (valse `cryptbase.dll` in `PDF24.exe`). PixelCode decodeert YouTube-videoframes via een Python-stager direct naar een executable in het geheugen.

Strategische Implicaties Het grootschalig misbruik van legitieme infrastructuur (Archive.org, YouTube, Google Ads) maakt domein-gebaseerde blokkades nagenoeg waardeloos. Wanneer de payload afkomstig is van een vertrouwde bron, falen traditionele netwerkfilters.

6. Conclusie en Handelingsperspectief voor Professionals

Het dreigingsbeeld van 2026 dwingt ons tot een 'Assume Breach' mentaliteit. De browser is het nieuwe endpoint en de helpdesk is de nieuwe firewall.

Strategische Aanbevelingen

1. Technisch: Monitoring & Hardening

- Implementeer **phishing-resistente MFA** (FIDO2/Passkeys) om AiTM-aanvallen te neutraliseren.
- Monitor specifiek op ongebruikelijke activiteit van legitieme binaries zoals **`finger.exe`** en **`colorcpl.exe`** (vaak misbruikt als dekmantel voor Remcos/ModeloRAT).
- Blokkeer uitvoering van applicaties uit user-writable locaties (zoals `%LocalAppData%`) via strikte AppLocker-policies.

2. Proces: Verificatie & Signaleringsketen

- Verscherp helpdeskprocedures: **geen MFA-resets** enkel op basis van telefonisch contact. Gebruik out-of-band verificatie die niet afhankelijk is van door de gebruiker verstrekte data.
- Implementeer **Inter-provider Signaling**: werk samen met partners en banken om verdachte transacties of accountwijzigingen direct in de keten te blokkeren (naar aanleiding van de Kifid/SNS-casus).

3. Detectie: Gedragsgebaseerde Analyse

- Zet in op **behavior-based sandboxing** (zoals ANY.RUN) om de volledige keten van AI-gestuurde phishing te ontleden. Statische analyse faalt tegen in-memory reconstructie van payloads (PixelCode).

Digitale Soevereiniteit De afhankelijkheid van kwetsbare Big Tech-infrastructuren blijft het grootste strategische risico. Organisaties moeten actief bijdragen aan de Europese dialoog over digitale autonomie. In 2026 is robuuste beveiliging niet langer een IT-streefdoel, maar een fundament van onze maatschappelijke soevereiniteit en weerbaarheid tegen geopolitieke invloeden.